

INTRODUCTION CYBER FORENSICS

Unit Structure

1.0 Objectives

1.1 Introduction

1.2 An Overview

1.2.1 Types of computer forensics

1.2.2 Advantages of computer forensics

1.2.3 Disadvantages of computer forensics

1.3 Present Scenario

1.3.1 Need of computer forensics

1.3.2 Computer Forensics Versus Other Related Disciplines

1.4 The Investigation Process

1.4.1 Policy and Procedure Development

1.4.2 Evidence Assessment

1.4.3 Evidence Acquisition

1.4.4 Evidence Examination

1.4.5 Documenting and Reporting

1.0 OBJECTIVES

This chapter would cause you to understand the subsequent concepts:

- To define computer forensic.
- To understand the role of forensic investigator.
- To guide you toward becoming a talented computer forensics investigator.
- To understand the investigation process in computer forensic.

- Understand a way to Investigate the cyber forensics with standard operating procedures.

1.1 INTRODUCTION

From a technical standpoint, the most goal of computer forensics is to spot, collect, preserve, and analyse data in a very way that preserves the integrity of the evidence collected so it are often used effectively in an exceedingly legal case.

Computer forensic objectives is to recover, analyse and present computer-based material in such the way that it's useable as evidence in an exceedingly court of law. Computer forensic priorities are primarily forensic procedures, rues of maintaining evidence, and following the legal processes. Secondly it's concerned with computers.

Computer evidence can be useful in criminal cases, civil disputes, and human resources or employment proceedings. Computer crime has forced the computer and law enforcement profession to develop new area of expertise and avenues of collecting and analysing evidence. The process of acquiring, examining and applying digital evidence is crucial to the success of prosecuting a cyber-criminal. A computer crime is a person can sit in the comfort of his home or a remote site and hack into a bank and transfer millions of dollars to a fictitious account is called "Computer crime".

Forensic sciences defined as an application of physical sciences to law in the search for truth in civil, criminal and social behavioural matters to the end that injustice shall not be done to any member of the society. Forensic sciences aim in determining the evidential value of the crime scene and related evidence.

1.2 AN OVERVIEW

1.2.1 Types of computer forensics

Computer forensic involves performing a structured investigation while maintaining a documented chain of evidence to seek out exactly what happened on a computer and who was answerable for it. Figure 1.1 describes the types computer forensics.

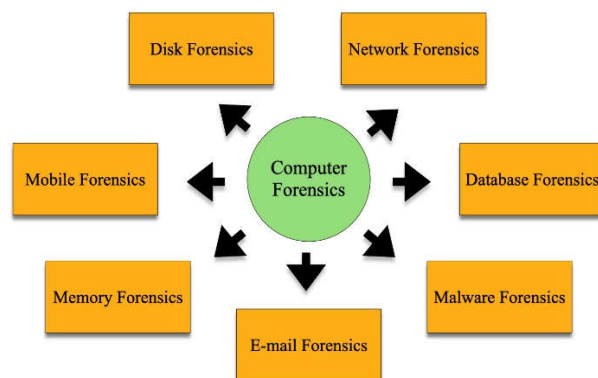


Figure 1: Computer Forensics types

1. **Disk Forensics:** It deals with extracting data from primary or auxiliary storage of the device by searching active, modified, or deleted files.
2. **Network Forensics:** it's a sub-branch of Computer Forensics which involves monitoring and analysing the systems network traffic.
3. **Database Forensics:** It deals with the study and examination of databases and their related metadata.
4. **Malware Forensics:** It deals with the identification of suspicious code and studying viruses, worms, etc.
5. **Email Forensics:** It deals with emails and its recovery and analysis, including deleted emails, calendars, and contacts.
6. **Memory Forensics:** Deals with collecting data from system memory (system registers, cache, RAM) in raw form and then analysing it for further investigation.
7. **Mobile Phone Forensics:** It mainly deals with the examination and analysis of phones and smart phones and helps to retrieve contacts, call logs, incoming, and outgoing SMS, etc. and other data present in it.

1.2.2 Advantages of Computer Forensics

- To produce evidence within the court, which might cause the punishment of the culprit.
- It helps the businesses to gather important information on their computer systems or networks potentially being compromised.
- Efficiently tracks down cyber criminals from anywhere within the world.
- Helps to protect the organization's money and valuable time.
- Allows to extract, process, and interpret the factual evidence, so it proves the cyber criminal actions within the court.

1.2.3 Disadvantages of Computer Forensics

- Before the digital evidence is accepted into court it must be proved that it is not tampered with.
- Producing and keeping the electronic records safe are expensive.
- Legal practitioners must have extensive computer knowledge.
- Need to produce authentic and convincing evidence.
- If the tool used for digital forensic is not according to specified standards, then in the court of law, the evidence can be disapproved by justice.
- Lack of technical knowledge by the investigating officer might not offer the desired result.

1.3 THE PRESENT SCENARIO

1.3.1 Need for Computer Forensics

Adding the flexibility to practice sound computer forensics will facilitate your make sure the overall integrity and survivability of your network infrastructure. One can help your organization if you consider on computer forensics as a replacement basic element in what's called an approach to network and computer security. For example, understanding the legal and technical aspects of computer forensics will facilitate you to capture vital information if your network is compromised and can facilitate your prosecute the case if the intruder is caught What happens if you ignore computer forensics or practice it badly? You risk destroying vital evidence or having forensic evidence ruled inadmissible in an exceedingly court of law. Also, you or your organization may transgress of latest laws that mandate regulatory compliance and assign liability if certain styles of data don't seem to be adequately protected. Recent legislation makes it possible to carry organizations liable in civil or court if they fail to guard customer data.

Computer forensics is additionally important because it can save your organization money. International Data Corporation (IDC) reported that the marketplace for intrusion-detection and vulnerability-assessment software will reach 1.45 billion dollars in 2006. In increasing numbers, organizations are deploying network security devices like intrusion detection systems (IDS), firewalls, proxies, and therefore the like, which all report on the protection status of networks. From a technical standpoint, the most goal of computer forensics is to spot, collect, preserve, and analyse data in a very way that preserves the integrity of the evidence collected so it is often used effectively in an exceedingly legal case.

In general, computer forensics investigates data that may be retrieved from a computer's drive or other storage media. Like an archaeologist excavating a site, computer investigators retrieve information from a computer or its component parts. The information you retrieve might already air the drive, but it would not be easy to seek out or decipher. In contrast, network forensics yields information about how a perpetrator or an attacker gained access to a network.

The Network forensics investigators use log files to work out when users logged on and determine which URLs users accessed, how they logged on to the network, and from what location. However, that network forensics also tries to see what tracks or new files were left behind on a victim's computer and what changes were made.

1.4 THE INVESTIGATION PROCESS

When conducting public computer investigations, you need to understand city, county, state and federal or national crime laws related to computer, considering standard legal processes and the way to make a criminal case. In case of criminal cases the suspect is tried for a criminal offense, like burglary, murder, molestation, or fraud. To work out whether there was a computer crime, an investigator asks some set of questions like the following: What was the tool accustomed commit the crime? Was it a straightforward trespass? Was it a theft, a burglary, or vandalism? Did the perpetrator infringe on someone else's rights by cyber stalking or e-mail harassment? Computers are involved in many serious crimes. the foremost notorious are those involving sexual exploitation of minors. Digital images are stored on hard disks, Zip disks, floppy disks, USB drives, removable hard drives, and other storage media and circulated on the net. Other computer crimes concern missing children and adults because information about missing people is commonly found on computers. Drug dealers often keep information about transactions on their computers or personal digital assistants (PDAs).

This information is very useful because it helps enforcement officers convict the person they arrested and locate drug suppliers and other dealers. Additionally digital photos, deleted e-mail and other evidence stored on a computer can help to solve a case. As an investigator you can track digital activity to attach it for cyber communications and can consider digitally-stored information as a physical evidence of criminal activity; computer forensics also allows investigators to uncover premeditated criminal intent and should aid within the prevention of future cybercrimes. There are five critical steps in computer forensics, all of which contribute to an intensive and revealing investigation are as follows:

1. Policy and Procedure Development
2. Evidence Assessment
3. Evidence Acquisition

4. Evidence Examination

5. Documenting and Reporting

1.4.1 Policy and Procedure Development:

If it's related with malicious cyber activity, the digital evidence are always delicate and sensitive. Cybersecurity professionals understand the value of this information and respect the particular undeniable fact that it are often easily compromised if not properly handled and guarded. For this reason, it's critical to determine and follow strict guidelines and procedures for activities associated with computer forensic investigations. Such procedures like this can include detailed instructions about when computer forensics investigators are authorized to recover potential digital evidence, the way to properly prepare systems for evidence retrieval, where to store any retrieved evidence, and the way to document these activities to assist make sure the authenticity of the info.

1.4.2 Evidence Assessment

In order to effectively investigate potential evidence, procedures must be in situ for retrieving, copying, and storing evidence within appropriate databases. Investigators typically examine data from designated archives, employing a style of methods and approaches to analyse information; these could include utilizing analysis software to go looking massive archives of knowledge for specific keywords or file types, further as procedures for retrieving files that are recently deleted. Data tagged with times and dates is especially useful to investigators, as are suspicious files or programs that are encrypted or intentionally hidden. This may also add reverse order, as file names usually indicate the directory that houses them. Files located online or on other systems often point to the particular server and computer from which they were uploaded, providing investigators with clues on where the system is located; matching online filenames to a directory on a suspect's disc drive is a method of verifying digital evidence. At this stage, computer forensic investigators add close collaboration with criminal investigators, lawyers, and other qualified personnel to confirm an intensive understanding of the nuances of the case, permissible investigative actions, and what sorts of information can function evidence.

1.4.3 Evidence Acquisition

Perhaps the foremost critical facet of successful computer forensic investigation could be a rigorous, detailed plan for acquiring evidence. Extensive documentation is required before, during, and after the acquisition process; detailed information must be recorded and preserved, including all hardware and software specifications, any systems employed in the investigation process, and therefore the systems being investigated. This step is where policies associated with preserving the integrity of potential evidence are most applicable. General guidelines for preserving evidence include the physical removal of such a storage devices, to retrieve sensitive data and ensure functionality, and taking appropriate

steps to repeat and transfer evidence to the investigator's system. Acquiring evidence must be accomplished in an exceedingly manner both deliberate and legal.

1.4.4 Evidence Examination:

For investigate potential evidence, procedures must be in place for retrieving, copying, and storing evidence within appropriate databases. Investigators typically examine data from designated archives, employing a form of methods and approaches to research information; these could include utilizing analysis software to travel looking massive archives of data for specific keywords or file types, additionally as procedures for retrieving files that are recently deleted. When the data is tagged with times and dates it is actually very useful to investigators, as sometimes suspicious files or programs that are encrypted or intentionally hidden. this might also add reverse order, as file names usually indicate the directory that houses them. Files located online or on other systems often point to the actual server and computer from which they were uploaded, providing investigators with clues on where the system is located; matching online filenames to a directory on a suspect's drive may be a technique of verifying digital evidence. At this stage, computer forensic investigators add close collaboration with criminal investigators, lawyers, and other qualified personnel to substantiate a radical understanding of the nuances of the case, permissible investigative actions, and what varieties of information can function evidence.

1.4.5 Documenting and Reporting:

In addition to totally documenting information associated with hardware and software specs, computer forensic investigators must keep an accurate record of all activity associated with the investigation, including all methods used for testing system functionality and retrieving, copying, and storing data, additionally as all actions taken to accumulate, examine and assess evidence. It also ensures proper policies and procedures are adhered to by all parties. Because the purpose of the whole process is to accumulate data that may be presented as evidence in an exceedingly court of law, an investigator's failure to accurately document his or her process could compromise the validity of that evidence and ultimately, the case itself. For computer forensic investigators, selected case should be accounted for in an exceedingly digital format and saved in properly designated archives. This helps in the authenticity of any findings by allowing these cybersecurity experts to indicate exactly when, where, and the way evidence was recovered. It also allows gives the information about the evidence by matching the investigator's digitally recorded documentation to dates and times when this data was accessed by potential suspects via external sources.



COMPUTERS- SEARCHING AND SEIZING

Unit Structure

2.0 Computers – Searching and Seizing

2.1 Electronic Evidence

2.1.1 Removable Media

2.1.2 Removable Storage Media

2.1.3 Cell phones

2.2 Procedures to be followed by the first responder

2.2.1 The Forensic Process

2.2.2 The First respondent role

2.3 Let us Sum Up

2.4 List of References

2.5 Bibliography

2.6 Unit End Exercises

2.0 INTRODUCTION TO COMPUTERS- SEARCHING AND SEIZING

Computers became a principal means for storing both personal and business information for big numbers of individuals. additionally, with the increasing use of the net and e-mail many of us use computers as a method of accessing information and communicating with others both in personal and business contexts. People increasingly store and manipulate accounting and business records with computer systems. At the identical time, commercially available computerized accounting software has dropped significantly in price and has become increasingly easy to use.

At just one occasion, maintaining a close and accurate set of accounting records was beyond the power of virtually well trained and experienced professionals. Today, however, persons with little or no accounting or business background are able competently to keep up their business and accounting records. The trend is one amongst greater availability and constantly dropping prices. As this trend continues, we are going to see an increased use of computers by all sectors of the population. together with the employment of computerized record keeping and communication in

legitimate enterprise has come the employment of the identical technology by criminal enterprises in closing their activities.

As a results of this trend, storage or memory devices have increasingly become the targets of presidency investigations of criminal activity. Here the govt has used evidence gathered from computers countless times in criminal prosecutions. The methods by which organization seek to assemble evidence from computers couple with the boundaries placed on the state by the us Constitution, and also the courts raise critical problems with personal privacy for all citizens who use computers in their daily lives.

This will discuss legal issues associated with seizure and search of computers and define the trend that the law is taking within the emerging area of inquiry. The government's interest can not be placed so high that everyone areas of one's personal life becomes the topic of governmental scrutiny.

2.1 ELECTRONIC EVIDENCE

Digital forensics could be a rapidly evolving field of forensic study. Its techniques are often utilized in criminal proceedings, civil, administrative so as to validate, identify, collect, validate, analyze, interpret, document and present digital evidence. An information derived from devices during a way that enables it to be employed in a proceeding is called as Digital evidence. So as to be admissible in a very court of law, digital evidence must follow a group of rules.

Electronic evidence is additionally called as “Digital evidence”, is employed to store data, within electronic devices or systems, that may be recovered by forensic experts and may be used as admissible evidence in court. The number of information generated from the devices like smartphones and computers is vast.

As such, requirement of any investigation is to spot digital evidence. The electronic evidence can prove crucial to the result of criminal, civil and company investigations. Electronic evidences are Computers, laptops and tablets, transportable data, HDD, RAID and SSD hard drives, USB memory sticks and SD cards, Social media information, Whatsapp messages, Cloud storage data, Digital photographs, CCTV etc. Data recovered from these devices and applications are considered as electronic evidence. However, this can be only admissible if recovered employing a forensic methodology by an authorized expert.

Examples of digital evidence are :

2.1.1 Removable Media:

If legally permissible (like a warrant), we wish to go looking anywhere that might contain a bit of storage media. Considering today's “stamp-sized” memory cards, this piece of evidence may be hidden almost anywhere like in books, wallets, hat bands, etc. Despite their small size,

memory cards can hold a lot of potential evidence like kiddie porn or stolen master card numbers. A fast check of Amazon.com shows that you just can purchase a 64-gigabyte memory card for around \$120. Gigabytes (GB) are pretty abstract for many people. Rather than employing a standard unit of knowledge storage.

2.1.2 Removable Storage Media

Removable storage media such as external hard drives, DVDs, thumb drives, and memory cards. Other than the devices and storage media at the scene, the surrounding area and items are also worth a look in the investigation process. For example, books and manuals can be useful to investigators to find the target and what kind of technology they may be up against. Perhaps the biggest payoff is an alert to the possible use of encryption. Discarded packaging in the trash could also be helpful. According to any forensic examiner avoiding encryption is definitely worth the trouble.

2.1.3 Cell phones:

These days almost everyone has a cell phone and they often contain some very valuable evidence. E-mail, call logs, contacts and text messages are examples of what you can recover. Items like call logs, contacts can be used to determine the last person to come in contact with a murder victim to determine approximate locations. Like electronic devices, it is important to make no changes to the device or its storage media. Therefore, interacting with the phone should be avoided unless very important. Cell phones can be wiped by the cell provider or even by the owner themselves so they are vulnerable. This functionality is intended to protect your data should you lose your phone or have it stolen. Apple's "Find My Phone" app is one notable example. We must address this concern by isolating or shielding the phone as soon as possible.

After securing the evidence, a survey of the scene will give investigators an accurate sense of what's ahead. Several questions need to be answered:

- What kinds of devices are present?
- How many devices are we dealing with?
- Are any of the devices running?
- What tools will be needed?
- Do we have the necessary expertise on hand?

Once these questions are answered, the real work begins.

2.2 PROCEDURES TO BE FOLLOWED BY THE FIRST RESPONDER

Imagine if we could return in time and examine a number of the foremost famous crimes. If only we could freeze time to the moment those crimes came about, we might be able to examine each case with near perfect evidence. Within the world of computer forensics investigation, we almost have that luxury. The primary response is that the most crucial part of a computer crime investigation. If done correctly with forensically sound practices, it's a solid building block to any investigation.

2.2.1 The Forensic Process:

Every incident should be treated as if it will end up in court. This is why the forensics process should be followed for every incident. The forensics process includes and is not limited to preparation, collection, examination, analysis, and reporting (see Figure 15.5). Each phase feeds the next phase in the process. The first responder is an integral part of the collection phase.

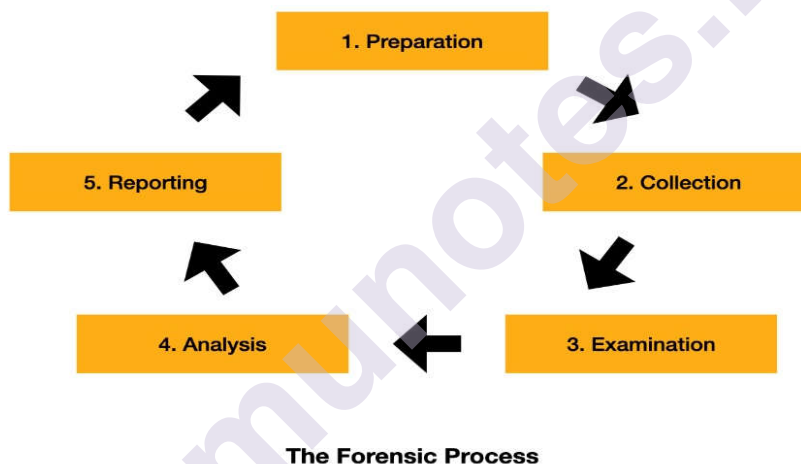


Figure 2The forensic process

1. Preparation:

Prior planning and preparation prevent poor performance. An organization come up with policies and procedures to support forensics process. Software licensing may be a major consideration, because enforcement cannot use evidence collected with pirated software. There should be an organized life cycle supported emerging technologies and personnel working the gathering, examination, analysis, and reporting. This ensures that organization forensics practice is scalable for emerging issues and technology.

2. Collection

The collection phase of forensics is the very first phase. In this phase first responders are handling incidents. As mentioned before, the collection

phase is critical to any investigation. The first responder should minimize any loss of electronic evidence (it can see the Damage & Defence sidebar for a definition of electronic evidence). The procedures which are required need to be completed by the first responder. The complete data should be verified and hashed for integrity. Although it is impossible to list all forms of electronic devices that may hold evidence, Table 1 lists several types of devices and media and the evidence that each of these devices contains. Responders must be careful because of the volatile nature of electronic devices, in order to maintain the integrity of the evidence.

Device or Media	Potential Evidence
Computer System	Computer files, video, audio, e-mail, images,
Network	Traffic Sniffers Binary log captures
Switches	MAC address, security violation logs
Firewalls	Logs, ACLs, configuration information
Servers	Computer files
Routers	Logs, ACLs, routing tables
MP3	Players Computer files, video and audio record
Digital Video Recorders (DVR)	Computer files, video, audio
Smart	Cards Identification, credentials, access information
Smart Phones	Computer files, video, audio, e-mail, images, notes, contacts
Memory Cards	Computer files, video, audio

Table 1 Devices and Media

3. Examination

During the examination phase, forensics practitioners perform a holistic examination of the evidence collected by the primary responders. Contrary to popular belief, the forensics practitioner's function is to require an impartial take a look at the evidence provided to them. The examiner tries to detect hidden, obscured, and encrypted data. The forensics practitioner should provide an unbiased examination report.

4. Analysis

The analysis phase is employed to see the who, what, when, and where of a happening. The evidence is scrutinized to see its value to a case. At this stage, it's going to be determined that there's nothing of evidentiary value.

5. Reporting

The examination report should contain only relevant information for the requested services. All procedures used and notes taken during the examination are preserved for discovery and testimony. The examiner must articulate the findings.

2.2.2 First Responder Roles

Identifying and understanding the roles of First Responders are crucial steps within the development of a happening Response Program. The primary responders are just that, the primary members to spot and address an occurrence. More often than not, they're system and network administrators that don't seem to be trained in forensics. This can be why it's crucial for a company to possess policies and procedures in situ, so that they have a written guideline to follow for every style of incident, they know what to not do, and that they know whom to contact before contaminating evidence. The team should include representatives from legal counsel and Human Resources. They ought to be consulted on all policies and procedures before implementation. Additionally, their expertise are invaluable once the information is collected and examined. These could also be considered liaison roles in some organizations (e.g., legal counsel wouldn't likely be member of the forensic incident response team; however, they're a necessary component of the complete process.)

1. System Administrator:

System Administrators are giving more importance to any computer crime investigation. It's the computer user that discovers anomalies during their daily operations. Most of the time system administrators are concerned more with system availability than forensic practices. It's important that each one organizations and agencies indoctrinate their supervisor on incident response procedures. During a response, the computer user can provide system configuration, configuration, logs, and other critical information.

2. Forensics Personnel:

Forensics personnel are ideal personnel to reply to a suspected incident. Forensics personnel are basically trained to preserve and collect electronic evidence from crime investigation. They sometimes have a variety of tools and software to network administrators who suspect their systems are compromised. The role of forensics personnel is to supply an unbiased forensic analysis to see the evidentiary value of electronic evidence.

3. Non-forensics Personnel:

Since computers are a part of everyone's home and work environment, this raises the possibility that anyone can be a first responder. Organizational management should take steps to ensure that all personnel are aware of what steps to take should an incident occur. Training should begin informing all non-forensics personnel on policy to ensure that

incidents can be processed with forensics practice. Figure 15.8 shows the FCC's Computer Security Incident Form. This type of form should be available to all organizations to record accurate and detailed information of computer systems incidents.

FCC COMPUTER SYSTEM INCIDENT REPORT FORM			
This form is based upon the FedCIRC Incident Report Form, which Federal Agencies and Departments are requested to use when reporting an incident. An automated FedCIRC version of this form can be found on line at http://www.fedcirc.gov/reportform.html . For urgent assistance, call the toll free FedCIRC Hotline at (888) 282-0870.			
1. Contact Information for this Incident:			
Name:	Organization:	Title:	
Address:			
Office Phone:	Cell Phone/Pager:	Fax Number:	
2. Physical Location of Affected Computer/Network:			
(Include building number, room number, and barcode information, if available):			
3. Date and Time Incident Occurred:			
Date (mm/dd/yy):		Time (hh:mm:ss am/pm/Time Zone):	
4. Type of Incident (check all that apply):			
<input type="checkbox"/> Intrusion <input type="checkbox"/> Denial of Service <input type="checkbox"/> Virus / Malicious Code <input type="checkbox"/> System Misuse <input type="checkbox"/> Social Engineering <input type="checkbox"/> Technical Vulnerability		<input type="checkbox"/> Root Compromise <input type="checkbox"/> Web Site Defacement <input type="checkbox"/> User Account Compromise <input type="checkbox"/> Hoax <input type="checkbox"/> Network Scanning / Probing <input type="checkbox"/> Other (Specify):	
4a. If a Virus, Provide the name(s) of the virus(es): Provide any URL with information specific to this virus: Provide a synopsis of the incident: Actions taken to disinfect and prevent further infection:			
4b. If a Technical Vulnerability, Describe the nature and effect of the vulnerability in general terms: Describe the conditions under which the vulnerability occurred: Describe the specific impact of the weakness or design deficiency: Indicate whether or not the applicable vendor has been notified:			
5. Information on Affected System:			
IP Address:	Computer/Host Name:	Operating System (incl. release number):	Other Applications:
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____

1-2

(include hardware/software, version or release numbers):	
7. How Many Host(s) are Affected:	
<input type="checkbox"/> 1 to 100 <input type="checkbox"/> 100 to 1000 <input type="checkbox"/> More than 1000	
8. IP Address of Apparent or Suspected Source:	
Source IP address:	Other information available:
_____	_____
_____	_____
9. Incident Assessment:	
Is this incident a threat to life, limb, or a critical agency service? <input type="checkbox"/> Yes <input type="checkbox"/> No If yes, please elaborate:	
Sensitivity of the data residing on system:	
Damage or observations resulting from incident:	
10. Information Sharing:	
Has the Public Information Officer been notified? <input type="checkbox"/> Yes <input type="checkbox"/> No	If yes, provide name and date of notification:
Consider with whom this information may be shared outside of the FCC (do not leave blank and check all that apply):	
<input type="checkbox"/> NIPC <input type="checkbox"/> NSIRC (NSA) <input type="checkbox"/> JTF-CNO (DoD)	<input type="checkbox"/> Other Government Response Teams <input type="checkbox"/> Other (Specify): <input type="checkbox"/> No Sharing is Authorized
Note: FedCIRC typically shares information with other government entities in a general sanitized form so as not to implicate a specific agency or department. The sharing is for statistical analysis and trend projection. However, any sharing authorized above may include agency specific information for further analytical and/or investigative purposes. Incidents must be reported to FedCIRC and your respective OIG. Reporting to the NIPC is strongly encouraged.	
11. Additional Information:	
(If this incident is related to a previously reported incident, include any previously assigned incident number for reference.):	
Return this Form to: Computer Security Officer, Room 1-A325 445 12th Street, SW, Washington, DC 20554	
Form A-XXX January 2002	

1-3

Figure 3 FCC Computer System Incident Report Form

4. Securing Electronic Crime Scene:

The number one rule of incident response is to preserve the maximum amount evidence as possible. It is important to quickly establish a cordial relationship to achieve maximum cooperation from personnel, especially management, within the response environment. Management typically assigns someone because the DAA who will work with the incident responder on making decisions affecting the organization's assets. The responder should work efficiently and the things which are necessary it is required to document all events that occur. The responder should immediately start taking notes with dates and times employing a known experience source, like a cellular phone. All of your actions, including your notes, are subject to discovery in a very criminal case.

Initially the responder should take steps to secure the protection of all personnel present. Generally, no personnel should be ready to take materials off from the crime scene. It's important to treat other areas outside the proximity of a workstation as against the law scene. Once the realm is secured from all personnel, the responder can proceed with collection. If you're responding to an unfamiliar environment, as is that the case with many enforcement and company investigators, you may need some help.

5. Health and Safety Personnel:

In incident response, it is important to remember the safety of every individual is involved and should be on first priority. In some cases due to some high-pressure situation this is forgotten but it should not. Due to the nature of "electronic" evidence, to take care of this evidence is important. In this case there are natural causes for concern. It is in everyone's best interest to preserve personnel as well as electronic evidence. Some safety items to consider are:

- Unplug the power before working on internal components
- Some equipment may hold an electric charge after unplugging
- Liquids and electricity
- Beware of dangerous radio waves (i.e., microwave transmissions)
- Lasers components on equipment could damage eyesight

6. Collecting and Preserving Evidence:

In a business environment, first responders must locate system administrators or other personnel with knowledge of the PC and network setup. Once the computers involved within the incident are identified, the responder should take an initial examine the workstation to verify if any destructive activity is going on. In many of the cases the suspect may try and cover their tracks purposely by executing utilities which will destroy electronic evidence. If a happening responder notices such behaviour, they must immediately pull the plug on the equipment.

7. Identifying Potential Evidence

The responder should rummage around for all identifying markings on the system. The simplest information to get may be a serial number. If a serial number isn't present, the responder should record all possible identifying properties of the equipment. When seizing computers, all connections are labelled for reassembly at a forensics lab. All of the cables and also the corresponding ports should be labelled.

8. Collecting Volatile Data

When the primary responder arrives, they will try to collect volatile data from the powered-on machine. Volatile data is information that's only present when the machine is turned on. If a network intrusion has

occurred, the attacker should have connections established. Many organizations have their own trusted toolset and they use it for collecting volatile data. Once you have got collected volatile data, you ought to hash the files and record the hash values in your notes. All collected data must be placed on forensically clean media. The netcat tool is usually accustomed collect volatile data over a network.

9. The Initial Interview

First responders must utilize the initial interview to get information that will not be available within the future. System Administrators and potential suspects could also be willing to offer up more information in an initial interview. If information is stored in notes, it may be retrieved for later testimony and examination. the subsequent is a few of the knowledge you ought to try and collect during an initial interview:

- Signed statements
- Owner information
- All users
- Contact information
- Passwords
- Encryption keys
- Internet aliases
- E-mail addresses
- Internet Service Provider (ISP)
- Purpose of the system
- Remote backups or storage
- Media storage
- Removable media

10. Documenting the Electronic Crime Scene

Documenting the crime scene must be done meticulously. This process creates a chronicle of the crime scene. Each crime scene tells a story. When first responders document a criminal offense scene, they ought to take 360-degree pictures of the whole room and any rooms associated with the crime. If a video camera is out there, it should be utilized yet. Pictures of the active programs should be taken to assist profile the user.

11. Evidence Collection Tools and Equipment

As a part of the preparation phase, organizations should have a toolkit ready for action. In short, first responders must be prepared for any

situation. With the vast amount of equipment available today, it's best to plan for versatility. rather than taking four different card readers for non-volatile storage imaging, take one multi-card reader. A number of the tools within the following list should be included within the responses.

12. Chain of Custody

To ensure the integrity of electronic evidence, a sequence of custody should be established. The chain of custody should be documented in writing to incorporate all handlers from seizure, transfer, storage, examination, analysis, and disposition of electronic evidence, and must be wiped out with corporate, local, state, national, and international jurisdictions and may be the other policies. Once the evidence is collected, it must be accounted for in documents literally during every stage of the investigation. Evidence is thrown out at court if it not handled properly. this kind covers the key needs of most chain of custody cases. Each organization should create forms and chain-of-custody procedures specific to that. the standard chain-of-custody form should include the case number, evidence details, handler names, signatures, dates, and relevant location information.

13. Transporting Electronic Evidence

The delicate nature of equipment requires extra attention. When leaving a scene, electronic evidence must always be packed and labelled together with the chain of custody forms. Ideally, electronic media should be placed in an anti-static bag then wrapped in anti-static wrap or bubble wrap. First responders should transport the fabric in sturdy boxes or cases until arriving at a delegated evidence room. Once the fabric arrives safely to the evidence room, the chain of custody documents are often appropriately documented and turned over to the evidence custodian. If acceptable by your organization, you'll be able to use mail services to move evidence. it's important to think about the environment during which the devices are placed. Electronic evidence is at risk of damage by extreme cold or heat. If you're transporting evidence by vehicle or air delivery, you ought to consider the extremities of every environment.

2.3 LET US SUM UP

The objectives of computer forensic is to identify the evidence quickly and estimate the potential impact of the malicious activity on the victim and assess the intent and identity of the perpetrator. Adding the pliability to practice sound computer forensics will facilitate you ensure the integrity and survivability of your network infrastructure. Additionally, to establishing strict procedures for forensic processes, cyber security divisions must also set forth rules of governance for all other digital activity within a company. this will be essential to protecting the data infrastructure of enforcement agencies similarly as other organizations.

2.4 LIST OF REFERENCES

- The Official CHFI Study Guide (Exam 312-49) by Dave Kleiman, Craig Wright, Jesse (z-lib.org)
- Littlejohn Shinder, Michael Cross, in Scene of the Cybercrime (Second Edition), 2008
- <https://online.norwich.edu/academic-programs/resources/5-steps-for-conducting-computer-forensics-investigations>
- <https://cyfor.co.uk/the-importance-of-electronic-evidence/>
- <https://resources.infosecinstitute.com/topic/computer-forensics-digital-evidence/>

2.5 BIBLIOGRAPHY

- Digital Forensics: Advancing Solutions for Today's Escalating Cybercrime, Software Engineering Institute, Carnegie Mellon University
- Basics of Digital Forensics_ The Primer for Getting Started in Digital Forensics, The - John Sammons
- Forensics Information from CERT <http://www.cert.org/forensics/>
- <https://us-cert.cisa.gov/sites/default/files/publications/forensics.pdf>
- <https://online.norwich.edu/academic-programs/resources/5-steps-for-conducting-computer-forensics-investigations>

2.6 UNIT END EXERCISES

1. The _____ is a debugger and exploration tool.
 - a. backtrack
 - b. Netcat
 - c. tcpdump
 - d. Netdog

2. The _____ can be any information stored or transmitted in digital form.
 - a. Chain of custody
 - b. Digital evidence
 - c. Forensic evidence
 - d. Pendrive

3. Computer forensic evidence is also considered as _____.
 - a. Data
 - b. Hearsay
 - c. Chain of custody
 - d. Information

4. Metadata is a _____.
 - a. Data about record
 - b. Information/data about data
 - c. Information stored in record
 - d. Information itself

SETTING UP A COMPUTER FORENSICS LAB

Unit Structure

- 3.0 Objectives
- 3.1 Introduction
- 3.2 Setting up a lab for Computer Forensics
 - 3.2.1 Computer Forensic Lab
 - 3.2.2 Laboratory Strategic Planning for Business
 - 3.2.3 Elements of facilities build-out
 - 3.2.4 Electrical and Power Plant Considerations
 - 3.2.5 Essential Laboratory Tools
- 3.3 Hard Disks and File Systems
 - 3.3.1 Overview of a Hard disk
 - 3.3.2 Hard Disk Interfaces
 - 3.3.3 Filesystems
- 3.4 Let us SumUp
- 3.5 List ofReferences
- 3.6 Bibliography
- 3.7 Unit EndExercises

3.0 OBJECTIVES

After studying this unit, it will help you to:

- understand and evaluate a plan for setting up a cyber forensic laboratory.
- classify the different factors to be considered for performing digital forensics.
- state and explain the different types of files and hard disk drive.

3.1 INTRODUCTION

To perform digital forensics by collecting evidence and processing them, thereby maintaining integrity, that is, without letting the original data getting tampered is a major concern. Hence before the forensic investigation of any scenario certain criteria fulfillments need to be ensured such as Computer forensic laboratories with physical as well as virtual security, the systems to be provisioned with appropriate application software's and tools, the configuration of appropriate hard disks and file systems for evidence collection without modification.

3.2 SETTING UP A LAB FOR COMPUTER FORENSICS

3.2.1 Computer forensic Lab

The entire field of data analysis and investigation has evolved in case of malicious intents in the digital realm. Technologies including laptops, desktops, cell phones, and the internet have certainly increased individual productivity and creativity, simultaneously it is also being used for violation of law or causing harm to an organization. Thus, such scenarios need to be evaluated by corporate investigators and law enforcement officers based on the phases of identifying, recovering, analyzing, and reporting onto the digital facts. There is an increase in the requirement of expert forensic examiners as well as forensic investigation facilities.

3.2.2 Laboratory Strategic Planning for Business

Factors to be considered for strategic planning of laboratory for business may include:

a. Philosophy of Operation

- Each data forensic implementation involves four core modes of operation, that is, the operating philosophies of forensic implementations will be similar in the case of the individual practitioner or a government-based investigative arm.
- The four core areas of operations include business operations, technology venue, scientific practice, and the artistic expression domain.
- A computer forensic initiative should pursue business practices, function through high technologies, and must foster a creative vision while technologically solving the investigation case.

b. Core Mission and Services

- During the design plan consideration of a forensic facility, it is important to consider the type of services and the level of scope or scale at which the services are to be provided.

- Determining the core mission and the scope of the service at the prospective laboratory will help analyze the aspects of building, operating the forensic facility, selecting the annual budget for the equipment or the furniture ergonomics.
- Depending on the service scope, a laboratory can be designed within a single room or an entire building with experts executing their multiple domain-specific tasks in each of several geographic regions.
- There exists a law enforcement agency to focus upon the violations of criminal statutes, a governmental agency to focus on civil litigation, a commercial venture to define service package details, and a market that packages to multiple audiences.

c. Revenue Definition

- Effectively addressing the five w's (who, what, when, where, why) of a business plan determines the plan completeness from conceptual theory to execution.
- Implement a minimum of the five-year strategic plan for successful growth based on the realistic environment where the facility resides and to which the facility will respond.
- Defining milestones to achieve as well as follow a growth track. Ultimately, the implemented budget needs to serve the facility's needs in the strategic vision of both actual operation and realization.
- Every forensic facility initiative requires funds to work whether for law enforcement, corporate or for-profit.

d. SOP

- -Policy and procedure execution, whether applied at the strategic, daily operations, or process-specific level, will eventually be the measure of operational excellence by which a data forensic laboratory's (and the product the laboratory generates) caliber is defined.
- A SOP should be determined and defined during the planning stages of the laboratory design so that valid and objective electronic evidence will be presented in a law court.
- The laboratory should function at a highly professional standard, along with the employees abiding professionally as well as ethically and the execution of tasks done by the employees should be systematic. Thus, a testable, repeatable procedure that generates predictable and accurate results should be considered.
- Evidence integrity must be maintained against attacks such as data spoliation attacks.
- Thus, robust policies need to be determined for procedure implementation. The phases of data analysis, that is, Digital

Investigations Standard Operating Procedure (SOP) are as follows:

Setting up a Computer
Forensics Lab

- Request for Services
- Initial Analysis
- Data Collection
- Data Analysis
- Data Reporting

e. Human Talent

A forensic examination environment as well as a good hardware purchasing plan will not suffice and will require human intervention. Factors such as experience gathering, knowledge sharing, continual education and investment in human resources development are mandatory for a successful data forensic laboratory.

3.2.3 Elements of Facilities Build-out

- Elements of facilities build-out denotes budget for constructing and operating, provisioning of normal operations as well as based on adverse events or disaster recovery along with provisioning for future modifications, expansions, and growth. A facility's complexity can be determined based on the scale of implementation and the budget constraint.

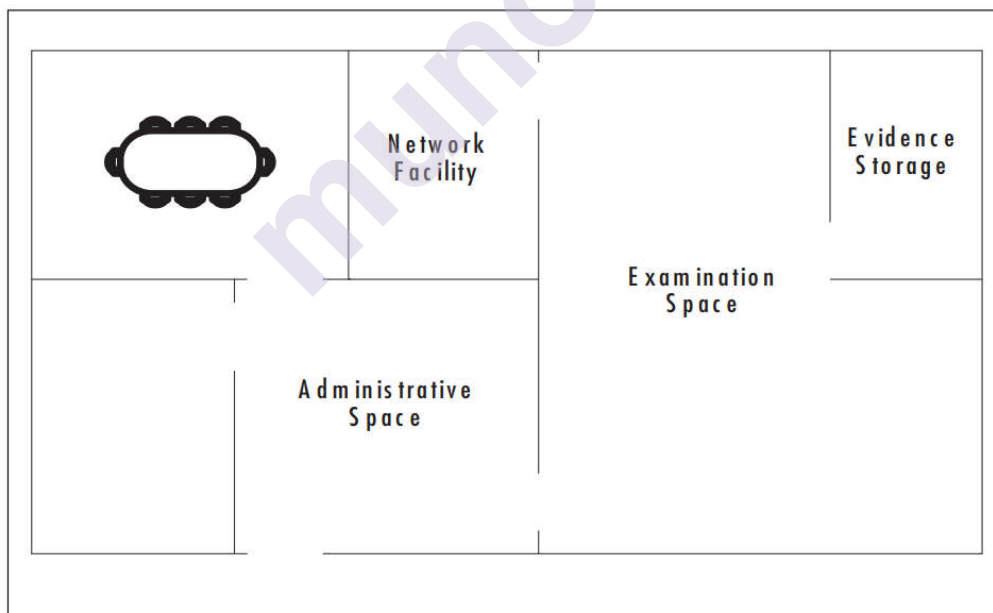


Figure 3.1: Simple model of a facilities plan.

I. Space Planning Considerations

- For designing the overall layout of a forensic laboratory, the following minimum functional areas should be considered:

a. Administrative area

- Consists of office space for personnel involved with the forensic team consisting of project management, executive staff, investigators, as well as for a meet space amongst internal personnel and clients or private guest areas.
- Designed to provide enough space with a comfortable environment for customer-based or team meetings.
- It can be considered as a private space for confidential calls or conversations, engaging in corporate communication.

b. Examination space

- Entire space which is dedicated to technical and investigative aspects of the forensic examination process. Technical staff members spend most of the time working on technical equipment required for the respective examination process.
- Access to this space should be restricted to relevant personnel and details of every person entering or exiting the lab space should be logged.
- Requires plenty of surface area with dedicated footage per investigator and ample square footage for forensic equipment location.

c. Evidence storage

- Dedicated storage space for storing digital evidence and other evidence items. Should be the most secure environment to access, the most controlled area for any kind of activity or entry within this space of a forensic build-out.
- Evidence locker should be designed to restrict forced or unauthorized entry so that its contents survive any environmental events. Access should be limited to key personnel, that is, a single Custodian of Evidence.
- Automated security systems should be used to challenge all accessors and logging into accesses.
- A robust audit methodology should be deployed for the complete accuracy of data being maintained.
- This facility also ensures every piece of evidence and its details are known and well documented.

d. Network Facilities

- Space where the data network, security, and telecommunication equipment provisioning services to laboratory space resides.

- This space is equally important as evidence storage space and should be protected. Physical elements of data networking and security, sending or accessing evidence, or examination work product should be dedicated and stand-alone infrastructure, that is, servers, switches, routers, data cables, and other physical elements serving the forensic space.
- Inbound or outbound facing day-to-day business protocols such as corporate, e-mail, telephony, internet access, etc. should be provisioned across a different physical network architecture.

II. Fire Protection/Suppression

- A forensic laboratory requires a well-designed fire protection plan, based on the standards and ordinances mentioned by the local fire marshal. Fires can be classified based on the material which led to the fire.
- The plan will be determined based on the cost constraints, personnel habitation zones, and technology venue residing in the space as well as its impact on the other aspects of the build-out. The ideal fire suppression methods for any forensic facility can be deployed after the data center or disaster recovery plan designs.

- Five globally accepted classes of fire include:

Class A: Common (solid) combustibles

Class B: Liquids and gases

Class C: Fires involving electricity

Class D: Combustible metals

Class K: Cooking fluids/oils

In the case of a forensic laboratory environment, the most common fire classes mostly are Class A (infrastructure materials) and Class C (electrical wires involving powered-up technology).

To resolve class A/C hazards, few options for suppression systems include:

- **Water dispersion systems (air-pressurized water systems)**
 - Water pipe Systems
 - Employs a piping scheme for maintaining a constant water load. It is one of the most cost-effective and low-maintenance of all fire-protection options as they are easy to repair and maintain with a faster recovery window after activation.
 - Also has drawbacks, accidental failure or impactful damage could lead to water leaks, whether, small or large.

- Dry pipe System
 - Employs a piping scheme to maintain pressurized air load, where the pressurized air holds back the liquid flow under normal circumstances.
 - Deployment head events trigger gas release and allow water to flow into pipes as the gas leaves the same.
 - Are expensive compared to wet pipe systems, though dry pipes also offer the same drawbacks as water pipe systems, in addition to maintenance complexities and higher maintenance costs. Though dry pipe system offers protection from pipes bursting in cold environments.
- Preaction systems
 - -Acts as the second level of fire protection implementation to be considered in a facility build-out. It is a modified dry pipe arrangement, advantage of a preaction system is the use of two triggers to release the liquid suppressant.
 - An electronic valve acts as the release inhibitor, where water is not held back by gas pressurization. The valve is controlled by a discrete fire sensor, wherein if the valve releases, the pipes get filled with liquid while the system behaves like a wet pipe. Another event must occur at the delivery heads level to release the water in the surrounding.
 - Pipe impact damage and head failures offer lesser threat to the surrounding environment, as the pipes are in a no-load state under normal circumstances.
 - The potential time delay between valve sensor engagement and sprinkler engagement may also benefit the environment, assuming some interruption can resolve a sensor-perceived threat before head discharge.
 - The cost factor increases from wet pipe to preaction pipe in proportion to the planned facility size increase, along with an increased complexity level and maintenance disadvantages of dry pipe, in preaction systems.
- Water Damage
 - Wet pipe, dry pipe, and preaction systems mostly use water as the liquid suppressant.
 - In environments with specialized electronics, computer equipment, evidentiary electronic devices, consideration should be given to the probabilities of water damage to the evidence or technology during any event.

- Waterproofing for certain fixtures should be done in an environment where water dispersion is used for fire control such as waterproof fire-rated safe inside the evidencelocker for storing evidence is a good preventive measure against the use of water-based firesuppression systems.

- **Gaseous suppression (clean agents)**

Gaseous suppression systems are also called gas/clean agents or total flooding systems, which provide a high-end option for laboratory fire control. These suppressants function in one of the two ways: one group removes heat faster than its generation during combustion, thus surpassing combustion, while the second group depletes oxygen for deprivation of oxygen fuels while combustion.

Gas agent suppression systems are permeable as compared to water-based systems and do not leave chemical residues while lowering the business recovery costs as compared to chemical suppression systems. An important characteristic of these materials is that they are non-conductive, that is, they do not have any conductive material left behind, making them suitable for electronics-based areas. They are costly for implementation and their maintenance tends to be higher. Two main classes of gas agent suppression systems exist, they are:

i. Inert Gas Suppressors

- Includes several blend gases such as carbon dioxide, argon, and nitrogen. Inert gas suppressors are oxygen reducers as they displace oxygen and prevent fuel combustion via fuel deprivation.
- Pure CO₂ suppression should never be utilized for laboratory fire suppression as it deoxygenates the air and can prove fatal for people.
- Inergen and Pro-inert are branded suppressants which are argon/nitrogen blends sold with proprietary delivery system deployments. They decompose into natural atmospheric gases and can be used in populated environments. They are also environmentally friendly.

ii. Fluorine compound Suppressors

- Fluorine compound suppressors are used as Halon replacements whenever halon systems are upgraded. Fluorine compound suppressors act as combustion inhibitors, thereby filtering heat at a very high rate.
- Examples of suppressors include branded suppressants such as Novec, FM-200, and FE-227, which can be used in populated environments and are environment friendly.

- **Chemical suppression: Foam, Dry chemicals**

- Apart from water dispersion and clean agent systems, several options for chemical suppression exist, where most chemical suppression methods require facility investment and increased costs in various areas of build-out.
- Example: Airtight sealed environments may be required for the chemical suppression systems in few areas when used.
- Both classes, that is, foam and dry chemical suppression systems are available, but tend to be insufficient for a populated environment. Thus, such systems cannot be used in a data center facility.

3.2.4 Electrical and Power Plant Considerations

A high-tech facility will require an above-average power demand to run, cool, and stay stable. Thus, the cost of provisioning in a forensic facility will be more as compared to a regular corporate environment. Standard power provision plan would involve factors such as dedicated water provision and stand-alone power generation facilities along with stand-by fuel resources, HVAC, and site security. Three main categories of requirements need to be assessed in the laboratory build-out:

- i. Facility build-out based on the facility load: Electrical demand of all general infrastructure-level technologies such as lighting, emergency lighting, HVAC, security systems, automatic doors/windows, audio/visual implementations, communication systems, corporate equipment, etc.
- ii. LAN/WAN Load: Any data center or forensic laboratory setting should have independent consideration from a power perspective. Server rooms with LAN provisions need to be implemented to avoid external network issues
- iii. Examination local workspace load: Applies to individual examiner's workspace as well as the overall examination space with a requirement of per capita that the forensic team demands.

a. LAN/WAN Planning

- The examination environment network components need to be separated from the general corporate network, apart from functional separation there is a need for absolute physical boundaries.
- If corporate and examination hardware are present in the same server room, then a divider wall or door should be built around the examination architecture with an extreme limit to human access levels in the physical space.
- All the examination traffic should be routed through dedicated examinations and servers. Whenever data storage is planned within the laboratory facility, facilities such as disaster recovery, redundancy, and sustainability concepts and support for large data

volumes should be considered. Deployment of physical segregations needs to be optimized.

- A medium-sized laboratory can encounter tens to hundreds of terabytes of data, leading to significant space requirements within the server room, associated with other high-footprint items such as near-line storage solutions, large tape backup jukeboxes, and others.

b. HVAC

- Huge number of computers may lead to massive amounts of BTU generation (British Thermal Units, a standard measure of heat generation). Conservative calculations need to be performed to determine the tons of AC required in spaces where heat-generating equipments reside.
- Planning for hardware growth and their future purchases since the beginning. Entire redundant units in areas cool the examination environment technology to provide the entire cooling burden whenever required.
- Ventilation requirements should be provisioned for spaces being cooled. An active exhaust system can be provided to recover the environment in case a fire event has been suppressed.
- HVAC units when placed above the lab space, add security against physical compromise but could also lead to risk in the form of water line breakage or leakage, hence it is important to consider pipes and pump systems to be deployed with a failover system as a countermeasure to any risk.
- HVAC concerns the environment which should also be managed, example an AC unit placed above examination space could create noise pollution in different scenarios.

i. Abatements

In the forensic laboratory, few factors need to be reviewed and monitored during the planning phase as well as after the completion of build-out.

1. Temperature

Every equipment has a desired operating temperature range. A data center maintains a temperature of around 68-70 degrees F. Hence, it requires temperature stability within the desired ranges during equipment failures as well. Devices such as a portable cooling device can be placed but within a particular optimized range, as temperatures at a low point could lead to electrostatic buildup and further discharge in air.

2. Humidity

A humidity management system should be deployed so that the humidity can be measured and controlled within +/-1 percent. Humidity control

plays a key role in reducing electrostatic buildup and discharge. During maintenance, various factors such as tolerance of the equipment to be used in the environment along with its geographic location, elevation, and so on should be determined.

ii. Static Electricity

Since temperature and humidity are considered as two key environmental factors to avoid static electricity issues. Workspace elements include antistatic flooring drawer linings and actively dissipative counter surfaces along with grounding of all metal furniture's to earth. Provision of anti-static mats, gloves, and sprays should be done for any operation or in case of any employee wearing charge-generating fabrics.

iii. Electromagnetic interference

The electrical plant needs to be planned carefully to reduce the electromagnetic field generation in any storage/handling areas. Main power plant components such as transformers whenever required to be guarded. Evidence locker should be shielded well, examination laboratory should also be taken into consideration for electromagnetic interference (EMI) shielding. A gauss meter or a series of them should be maintained in the functional laboratory space with regular anomaly checks. EMI regulation should communicate to ISO planning and competency levels for any operation which focuses on electronic data handling.

iv. Acoustic Balancing

Multiple workspaces purposely put white noise into their environments to generate acoustic masking for privacy reasons and to avoid a silent environment. A forensic laboratory may have acoustically reflective surfaces, make it mandatory for surface texture applications, baffling, or any other acoustically absorptive abatements.

c. Security

Security is an important concern for any forensic operation. Protocols must be applied to campus-level, environment-level, and object-level access. Video and live surveillance is strongly required. The entire facility should be provisioned with a minimum two-challenge system such that each entrant will have to surpass a minimum of one validator at checkpoint such as biometric, card swipe, etc., while the other could be an independent manual or automatic validator such as sign-in security desk or internal security card swipes, etc.

Higher-level access control should be applied especially to examination environments where access should be challenged through dual point authentication (two-factor identification methodology) while the access points should be constantly monitored. A physical sign-in or sign-out log needs to be maintained despite dual-authentication protocol being implemented, as an ink-signature trail could prove useful for independent security audit and review phases.

d. Evidence Locker Security

A locked, fire-rate safe in a locked room along with hand-written access logs could be sufficient security for a minimal environment. A shelf-and-cage methodology with a single portal of entry that is key-locked and monitored for access is implemented for evidence storage environments. The build-out of an evidence locker could be expensive and complex, depending on the facility needs and various other factors such as level of national security.

The evidence storage environment has the highest and most restrictive levels of access control, where only a single custodian of evidence will be granted the master access who can

execute the chain of custody check-ins and outs from the locker.

Each access should be logged with 100 percent accuracy. Video surveillance at entry as well as exit view along with the storage space should be deployed. A robust alarm should be configured to capture any unauthorized entry through any location around the space. Air ducts should be of a thinner size to avoid human intervention or invalid objects surpassing through them. No openings or ventilations should be kept open to avoid unwanted entry or evidence tampering activities by any means.

e. General Ambience

The environment of a data forensic laboratory should not have any disruptions, with the lab space being a low-foot-traffic environment so that employees can work without any disruption. Space should be isolated from other environments and should be well-lit with personal comfort and positive support in the common area as well as in personal space.

f. Spatial Ergonomics

A data forensic laboratory functions as a warehouse operation. The computer hard disks being examined, the chassis, monitors, and other products require handling and storage. Other components such as monitors, workstations, servers, and others are very bulky, due to which moving them from evidence lockdown and placing them for work could be difficult, hence this issue needs to be considered during workspace design. Lumbar harnesses or similar safety equipment should be provided to employees responsible for lifting or carrying tasks.

g. Personal Workspace Design

Every lab inhabitant should have an ample amount of operating space, that is, work surface area mostly digital work surface areas such as monitor footprint should be abundant. Electric supplies should be robust and the personal space of every examiner should be considered as a mini-laboratory which should be facilitated with all the hardware and software, to perform the investigative task as well as maintain work product. A dedicated investigation platform, an entire kit of write blockers and accessories, a separate system for corporate or business communications, a

workspace-level data management system, and a library of reference materials are desired elements for an active and personal investigation workspace.

h. Common-Area Considerations

Consider providing many units of technology with multiple sets of write blockers and investigation machines for various parallel tasks to be conducted. Workspaces should be designed with a design template to enable multiple individuals to execute the same tasks at the same time in various workspaces or to allow an individual to switch between different stations thereby managing machine and time-intensive tasks. Maximum tasks execution should be organized with minimal foot traffic.

Shared resources should be deployed for serving the needs of the staff without causing workflow deadlocks.

3.2.5 Essential Laboratory tools

I. Write Blockers

- Write block methodology and devices are mandatory in laboratory or field forensic toolkit.
- Data spoliation, that is, data integrity being tampered with intentionally or accidentally is a major concern for forensic examiners.
- Forensic workproducts should be leveraged spoliation concerns which is considered to be one of the most common attacks while handling digital evidence.
- Whenever an unprotected writable data device is connected to a computer, it leads to change. Volume mounts, computer boot sequences, and other events could modify evidence data store components from explicit write-to events.
- Thus, methodologies and devices should be deployed by forensic examination environment to ensure write block capability.
- Few windows registry edits could protect USB devices from write events, whereas Linux volumes could be modified so that the data stores are made read-only.
- Hardware write block devices, namely blockers, forensic bridges are a major component of the forensic tool kit and have advantages such as portability, ease of use, and function testing. Few common write block tools include Tableau, WiebeTech, and Intelligent Computer Solutions DriveLock.
- Hard-disk technology consists of various multiple interface types such as IDE, SATA, SCSI, etc. wherein different types of interfaces are integrated for different connectivity needs as required by an

investigator. USB and FireWire form are some interface types used to connect external write blockers to examination machines.

- Forensic bridges can also be permanently installed into workstations, though it isn't portable, the internal forensic bridges have the advantage of being space-efficient.
- Write block technology also supports the examination of non-hard disk media.

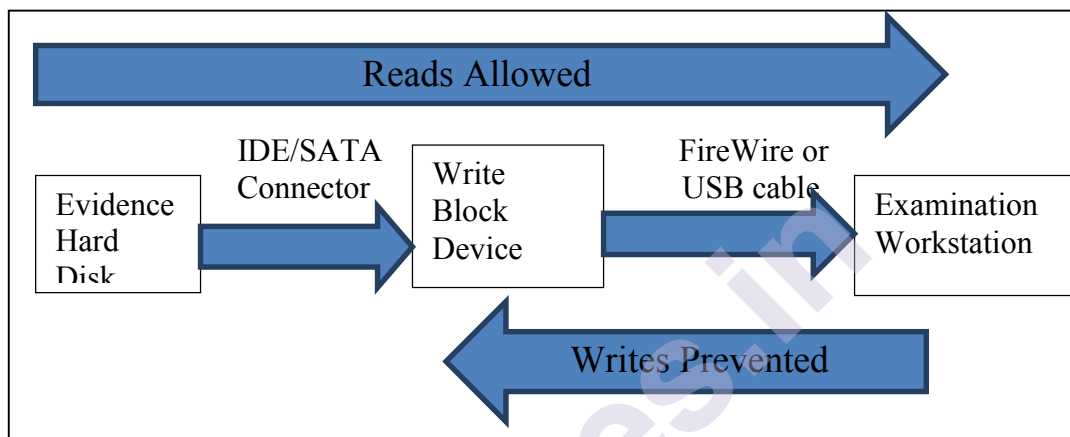


Figure 3.2: Write Blockers

A. Write Block Field Kits

- -Forensic bridge field kits are a part of the forensic laboratory inventory, which can be fully functional on an examiner's laboratory desktop and help reduce inventory purchase costs by minimizing the hardware amount per examiner needed for data acquisition and investigation in diverse environments.
- Field kits are lightweight, designed to be shock-resistant, and meet air transport criteria, packed with device, adapter, and cabling options to address the unknowns of field work.
- Example: Digital Intelligence UltraKit and the Ultimate Forensic Write Protection Kits from Forensic Computers are single-package systems.
- -Field kits mostly supply a basic multifunction hand toolkit, bit/driver set, and a digital camera to support other aspects of field work.
- A good core field kit can be supported by cabling, adapters, extra devices, and so on to create a powerful and economical portable laboratory system.
- Redundant highly used/ fragile components such as multiple AC adapters, power cords, and interface cabling units are mandatory.

- Another level of protection can be added to the examination equipment assembly process thereby protecting it against the damage to evidence media via pilot error, through convenience items like Tableau in-line power switch (T2).
- The write block methodology ensures on original media protection from any modification during examination and duplication. Example: Some field investigation practices require data acquisition through a forensic duplicate of original evidentiary materials for transport of evidence to the laboratory environment for analysis. The requirement for write blocking can be conjoined to the need for a duplication platform in such cases.

B. Hardware Duplication Platforms

Multiple handhelds and desktop forensic duplication systems are available, wherein the core functionalities they provide are write-blocking the original evidence media, conducting data replication to secondary media, measuring the accuracy/completeness of the duplication process through some measurement criteria such as hash algorithm MD5 or SHA1 or both to ensure that the entire original has been duplicated to a forensic copy, while some devices of this class also involve reporting capability.

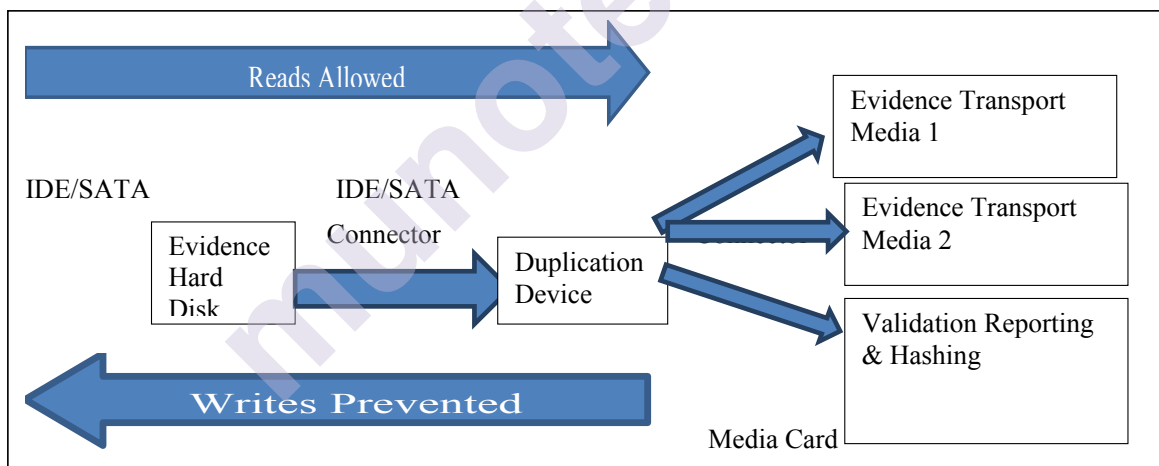


Figure 3.3: Hardware Duplication Devices

Various models are readily available such as the logicube forensic talon, which has a duplication rate of upto 4 GB/minute and provides multiple media adapter kits along with possessing extensive reporting capability. Intelligent computer solutions ImageMASSter Solo-III forensic duplication device handles interface types and is capable of writing to output hard drives concurrently.

Voom technologies hardcopy II provision a simple interface and handle IDE hard-disk duplication, voom technologies also produce a SCSI HardCopy for SCSI platform acquisitions. Multiple hardware duplication

devices and accessories can be packaged into a field kit such as the DIBS RAID: Rapid Action Imaging Device. Many devices also support output options of bit-by-bit duplication, one or more forensic image format acquisitions, and transport media sterilization. Data transcription rates of hardware-based duplication platforms are much faster as compared to software-based duplication options.

Duplication hardware is considered to be an important addition to the examiner's toolbox, but duplication tools do not provide any environment in which an examiner could investigate the data that is being duplicated. An examiner is provisioned with an investigation environment by portable forensic computer systems which expands the examiner's field capability.

C. Portable Forensic Systems

- In case of requirement to take the entire investigation process into the field, a forensic examiner should have access to the protective and duplication tools as well as completely interactive examination environments.
- A specialized portable forensic computing system provisions a highly mobile, equipment-intensive, and methodology-sound platform to the forensic examiner. The examiner duplicates digital evidence and analyzes it on a robust platform through complete field examination.
- 'Bye-hand transport' level portable forensic systems will contain feature-packed laptops or custom suitcase-style workstations along with the second tier having a class of machines and mini networks which are ruggedized for mobility but are not recommended for day-to-day high mobility. These investigation systems have faster processor capability, ample amount of memory, and high-volume data storage space which are optimized for specific forensic software packages.
- Multiple operating systems can be implemented on one workstation. Each examiner requires a personal field kit inventory making it easier to manage it into vehicles and for air travel. High-mobility portable systems rely on external field kits like the write blocker field kit, supplemental cable, and adapter solutions to make the core system compact and easier to transport.
- Suitcase-style workstations consist of detachable monitor, keyboard and mouse set which could be utilized to work with evidence workstations for boot-up procedures like BIOS checks and verifying proper suspect system reassembly.

D. Portable Enterprise Systems

- Sometimes field portability addresses the requirement of a robust, temporary laboratory facility at an examination location. Forensic portability could be extended to network-in-a-box solutions wherein these needs can be fulfilled by half-rack solutions.

- The core components that a portable enterprise system can offer include an examination system along with integrated write block bridges and robust examination hard-disk storage space with add-on hardware such as monitors, KVM, and so on.
- This portable environment is mostly highly durable but with low mobility, quite heavy, and transported as crated and packed, that is, the setup time and breakdown time as opposed to the plug and play high mobility equipment.

E. Laboratory Enterprise Systems

- The high-mobility equipment used by the field examiner can also be used on the desktop.
- Facilities that support a permanent lab installation of desktop investigative gear along with field support equipment, many non-portable investigative systems are available.
- These systems offer various field hardware solutions in portable kits for write blocking and hard-disk management combined into a single desktop chassis.
- All-in-one devices like Tableau T35i Combination Bridge and Tableau T335 Drive Bay Controller can be economical options that implement multiple write-block and multiple hard-disk solutions in a single chassis.
- Prebuilt desktop forensic systems have the best computing power available at the purchase time.
- When selecting the specifications for a desktop laboratory processing system, factors such as faster processing, largest memory allocation, and largest possible hard-disk drive volume as per budget should be targeted.
- Based on the process-intensive needs of most forensic software application suites, a faster, powerful, and a larger amount of RAM are important. Hence, maximizing the storage space and considering the relatively shorter span of any volume's sufficient during the allocation of resources for acquiring forensic computing equipment.
- Evaluation of hardware-level redundancies and robust backup systems for data volume management. The viewable area of the computer monitors on which they work can have an impact on the investigation speed and efficiency.
- Many forensic systems are sold with dual-head video cards in a way that two to four monitors can be attached to a single system. Large flat-panel monitors are considered space-efficient, readily available, and cost-effective.

- Multiple OS are desirable as they will support various investigation tools. Powerfulprebuilt forensic systems can provide four or more bootable operating systems.

II. Media Sterilization Systems

- Spoliation challenges, that is, causing harm to evidence integrity, that is, to the duplicate evidence copy. Thus, a solid policy should be determined during any forensic practice for work product media sterilization.
- A hard drive to be used as a substrate for the duplication of evidence should be sterilized before use and should be documented as sterile, that is, totally clean and then it can be validated by some post-sterilization procedure.
- Sterilization can be done by some hardware and software duplication tools along with data acquisition by using hash-validation to written sectors and zeroing out all the other writable space. The acquired evidence data stream will be validated via hash methodology and then wipe any remaining writable data space to a random or zero value through data overwrite methods.
- Software's such as Guidance Software's EnCase forensic examination suite involves the capability to sterilize and validate the hard disk media, products such as White Canyon Software's WipeDrivedestroys data as per several data overwrite patterns.
- Hardware sterilization devices can bulk-overwrite the hard disk media. Sterilization followed by a validation process can be used to destroy sensitive data after its value expires.
- A forensic laboratory must have a data destruction tool to address the real needs of that facility. Thus environments, where data destruction practices are conducted, should have consideration of bulk data wiping hardware devices for a new media preparation as well as a degauss chamber or a physical destruction device for any disposal sterilization requirements.

III. Data Management (Backup, Retention, Preservation)

- Whenever considering a forensic environment implementation, there arises a need for data storage and preservation. Requirement of high volumes of digital workspace with examination workstations having terabytes of onboard storage, wherein high-volume data may be transacted across the environment.
- Networked storage has data content that requires preservation for a longer duration, a rapid workflow turnaround to archive, or an extended presence in online storage.
- A forensic facility might require more stringent policy and procedure for auditing and report on data management activities. Both per-

machine, as well as enterprise level data management solutions, guarantee options for data handling, minimizing workflow-based bottlenecks.

- A forensic environment should be designed to manage the need for constant, rapid, and high-volume data management. Components for data management might include data storage and movement-based hardware and software solutions.
- Systems of tape backup deployed at a per-machine or enterprise-level may provide the ability to backup and store large volumes of product through the clone-validate-delete methodology. Offline storage such as tape, optical disk, and offline hard disk arrays, etc. allow multiple options for long-time preservation.
- External devices or hot-swappable devices provision additional value to the data management proposition through instant access or instant storage methodology for data repository refreshes along with fast data offlining.
- Several magnetic tapes and DVD formats are readily available along with being cost-effective for evidence preservation. High storage solutions can be provided by magnetic storage such as hard disk or tape when the environmental factors are tightly controlled, both formats are subject to limitations of data degradation over time and are magnetic.
- Tamper resistance adds or deletes the data resulting in physical signs (splicing) or electronic signs (readability/non-readability) as an advantage of magnetic tape.
- Disadvantages of tape could include tape readability being impacted from backup software versioning changes along with media degradation after a certain period and little recourse for restoration when tape span media tapes fail. Tape hardware is expensive, especially at the enterprise level wherein installing and licensing for backup software at an enterprise-level could be costly.
- Although, tape systems as high-end hardware rotary jukeboxes and advanced library software systems are more cost-effective as compared to full hardware storage dependencies such as parallel storage area networks (SANs).

i. CD/DVD Hardware Solutions

- Optical media such as CD or DVD are used for long-term evidence preservation and storage needs and are very inexpensive along with being readily available. CD and DVD
 - media can be used as backup evidence storage.
- High-grade optical media has a life span measured in decades, which could prove as an ideal for preserving long-term evidence. For

example, an image file set can be created in a specific format and size, while the default image segment file sizes reflect the anticipated use of CD as the ultimate storage unit.

- The special needs of the forensic environment can be handled by data and media duplication hardware. Example: Fernico FAR system is a technology-based on CDR/DVD burning technology from Primera technology and is made greater by specialized forensic data archiving software developed by Fernico.
- Combined system provisions the forensic examiner with robust data management and archival tool which provides several services which are explicit to the evidence management requirements.
- The FAR system burns DVDs or CDRs, labels the media, manages the spanning of data across disks and applies forensically desired validators like robust hashing options to the data burned onto the disk.
- Device is network-capable, automating activities to utilize a calendar and job-based scheduling system, which is designed to archive data to disk and restore data from disk archive libraries.
- A FAR system can be used to replicate CD/DVD original evidence media. Each FAR system caters to a specific scope of media capacity and disk production. An optical media production platform could act as an addition to the Forensic laboratory tool set.
- Forensic laboratories need to be prepared to process old storage technologies, such as floppy diskettes are a feasible medium to duplicate evidence for media that can be automated by bulk duplication machines.
- Ashby and CopyPro are vendors which provide floppy diskette duplication systems which auto-feed the bulk diskette media and bit-for-bit validate copies.

IV. Portable Device Forensics: Some Basic Tools

- Portable device forensics embraces configuration uses of the Faraday enclosure for data integrity preservation or to prevent a data transmission.
- A Faraday enclosure is capable of blocking electromagnetic fields and energy waveforms and is composed of conductive materials such as wire mesh layers, which allow the occurrence of electrical induction across the material surface when energy is applied to it.
- When a penetrating electromagnetic field or a waveform of a particular frequency or range of frequencies are introduced to a Faraday enclosure, they won't penetrate the enclosure surface instead they will travel across the conductive surfaces of the enclosure.

- In case the faraday enclosure consists of a signal generator within itself then that signal can be kept inside the box. In case a signal receiver is kept inside a Faraday enclosure, it can prevent the receiver from hearing the signal.

V. Portable Devices and Data Storage

Portable devices can store data in many ways such as SIM cards along with other card media types, chip-based storage while modern portable devices might have more than one way of storage mechanisms. The form factor predisposes either the static data, that is, phone numbers stored on a SIM card, or volatile data storage such as recently dialed phone numbers stored in battery-powered, chip-based memory, as the storage form multiplies.

a. Power

The primary rule for securing portables for forensic examination is the device should be kept off but the battery should be fully charged, in case the device is on, it should be ensured that the device stays on unless the entire examination is completed. To manage power and limited time to respond to portable device research, multiple tools can be added to the examiner's tool kit.

Multipurpose power devices such as Paraben's Remote Charger and Handheld First Responder Kit supply power to a device to extend its data preservation window, which gives ample time to the examiner for transporting the device to a laboratory environment for detailed analysis. To document a live review process in a lab or field, the Project-A-Phone device analysis platform and the Fernico ZRT Mobile Device Screen Capture Tool helps examiners perform rapid examination and preservation of power-on screenstates, menu system and other live-system processes whose recovery is difficult by a data export process or document for examination and future presentation purposes.

b. Readers

Many of the card types to cell phone technology such as SIM are proprietary, to differentiate SIM contents, leads to the requirement of custom forensic software/hardware packages. A 15-in-1 card reader could act as a good tool to add to the tool kit for the common data storage card types such as PDSs, cameras, cell phones, etc. with formats like SD, MMC, and CF. Forensically sound card media readers are distributed across by forensic vendors such as digital intelligence.

c. Cables

Many portable device power and data cables are included in a good portable device forensic tool kit. Multiple all-in-one forensic cell phone and PDA examination suites provide an extensive cable selection for powering as well as linking to the many data interface formats found on the portable devices. Don't discount the retail cell phone outlets, electronic

stores, websites for supplemental cables, and adapters to increase the mobile device field kit. Adapters are also included in a good tool kit along with cables.

VI. Forensic Software

The domain of forensic software selection is extremely vast, a forensic examiner will require various types of applications to address the different investigative scenarios faced during the business course. None of the tools are all-inclusive, thus, utilization of multiple tools is required. Though tools may have similar features which help validation of processes and methods, every tool has its unique strength also which helps in the investigative process being thoroughly conducted with the diverse investigation. Whenever software services are provisioned to an investigative team, the following areas need to be considered:

i. Operating Systems

Operating systems are software that performs operation control of a computer and processing of programs, that is, input, output, assigning storage space functions. While considering a forensic laboratory, a need for a software library with many OS including the available version levels of each OS can be retained. Multiple OS can be leveraged as a production environment, where the forensic examiner can conduct an investigation. Leveraging multiple OS permits an examiner to access software applications written for specific OS platforms, wherein the ability to work with multiple OS versions needs to be standard. Example: Some features which are required in an older version of software may require the use of an older version of OS. Thus, strategically it needs to be decided which version of OS will be required for the examination. An investigation may require examination of NTFS (New Technology File System) format a hard disk from a Windows OS of the suspect's computer while working on an examination system configured with Linux OS, which may lead to evidence spoliation. Thus, the forensic examiner may need to work on diverse OS depending on the OS configured by the suspects of different investigations. Thus, the advantage of having an installable OS library allows the investigator to reconstruct events in the same software universe as the suspect computer by creating a test environment.

ii. File systems

To examine file systems of a specific type it may require a compatible OS as different OS support different file systems, wherein a file system represents the way data is organized and stored in a medium. File system in computer forensics denotes the organization of data stored on computer media such as hard disks, floppy disks, thumb drives, optical disks, etc. A forensic examiner may require access to multiple OS, hardware devices, and software applications to work with different file systems.

iii. Main investigative platform

Multiple software applications act as the main investigative software platform for a forensic examiner, where the common characteristics of the main investigative tool suite involve the capability to create an 'image file set or bit for bit clone' copy of suspect media, analyze live or imaged data streams, search and obtain suspect data content, develop reports on contents and findings, as well as export required data for subsequent use external to the software. Investigative software suites are available for multiple OS (Windows, Linux, and Mac), where some investigative software's are restricted to law enforcement (iLook) and other applications are accessible to the general public (in the form of EnCase Forensic, Forensic Tool Kit, S.M.A.R.T., and MacForensicsLab).

During an investigation, forensic examiners often possess several software suits and leverage more than one investigative suite. Every investigative suite has some strengths. Encase forensic of Guidance software has a robust scripting language that strengthens custom investigation. Forensic Tool Kit of AccessData has an intuitive user interface as well as the capability to integrate password-breaking software from the same vendor. MacForensicsLab is the only forensic investigative suite developed for the Apple OS X system. S.M.A.R.T. is a robust tool developed for the Linux OS. ProDiscover Forensic by Techpathways can perform examinations on Sun Solaris UFS media.

iv. Special focus tools

To conduct specific data analysis, multiple software packages have been developed.

Several tools such as E-mail analysis, password-breaking, decryption, portable hardware analysis, artifact-specific identification, and analysis tools, and other types of data identification, conversion, and analysis tools have been developed, which may prove valuable to the forensic data examiner. AccessData's password recovery toolkit executes password breaking and decryption tasks, whereas Windows Registry examinations are enabled by Access Data Registry Viewer. Product-specific e-mail analysis is provided by Hot Pepper Technology's EMail Detective AOL e-mail analysis. Specific realm analysis capability can be provided by Paraben's Chat Examiner, Email Examiner, and Device Seizure. Steganographic investigation capability can be provided by Wetstone's Stego Suite, whereas malware detection is provisioned by Wetstone's Gargoyle Investigator. These specialty tools could supplement an investigator's digital toolbox.

VII. Tools in the Enterprise

The forensic examination could be executed against LAN or WAN resources in the enterprise. Investigative tools were developed to deal with forensic-grade in widely distributed environments, that is, enterprise forensic tools can investigate live systems remotely and can also analyze volatile memory contents, network metrics as well as local machine activities.

Guidance Software's EnCase Enterprise Edition allows various functional aspects such as data collection, analysis, and reporting to be driven across networked resources through local application connector clients and centralized investigative resources. It is intended for the corporate implementation, a special version known as Field Intelligence Model (FIM) is available to law enforcement only for ad hoc investigation. Live wire, an agentless investigation tool designed for permanent installation in a corporate network or ad hoc investigation, pushes its application software packet across network resources into the memory space of suspect systems.

VIII. Ad Hoc Scripts and Programs

Despite several prebuilt tools, there may be a need for a custom solution that might need to be created for addressing the investigative requirements. Additionally, code writing, scripting, and resource fabrication skills are also available within forensic examiner's toolbox. Any ad hoc implementation requires complete validation and testing of mechanical and process which guarantees the tool performs as per expectation and preserves the evidence integrity.

IX. Software Licensing

The entire software environment which consists of the OS as well as the applications should be licensed for an examiner, thus the use of any unlicensed software, that is, software piracy is illegal. Software licensing is considered as one of the main cost factors for laboratory scope of service provision, initial space targets as well as ongoing laboratory operations.

The laboratory SOP needs to be integrated with maintaining, auditing, documenting, and demonstrating license compliance.

X. Tool Validation

One of the mandatory and constantly ongoing processes for the forensic examiner and the laboratory is tool testing. Testing of both hardware and software is needed, consistent repetitive testing ensures methods and leads to maintenance of the integrity of the equipment. It is important to demonstrate as well as document the proof of any tool's ability to preserve the integrity of any data which is under examination. Testing and documentation of test methodology, results, and theory that surrounds the test design help provide forensic defensibility that the evidence hasn't been tampered with by the tool. Testing must be performed specifically and exhaustively to prove the tool functionality valid. Example: Examiners can create a specific test script for their respective write block devices, create standard test media, and perform procedures such as an attempt to write, delete or access media to and from media, to demonstrate function integrity.

3.3 HARD DISKS AND FILE SYSTEMS

3.3.1 Overview of a Hard disk

Hard disks are non-volatile storage devices which can store and fetch data quickly, that is, it reserves data even after the system is shut down thereby making it suitable for permanent data storage. A hard disk drive (HDD) is installed within the computer making it easier to access the data and process it as compared to floppy disks or any removable media. It writes digital data into magnetic patterns onto the disks.

The data is organized and can be located on a hard disk through file systems, which is responsible for controlling how the storage of directories(folders) and files in an organized way can be done on physical media.

There are two placement of disk drives:

- a. **Fixed storage drives**, to be installed within the system.
- b. **External storage drives** attached explicitly to the system.

The hard disk can be placed in either of the two roles:

- a. **Primary hard disk:** The computer accesses it during boot up (starting) of the system as they generally consist of the operating system to be loaded.
- b. **Secondary hard disk:** Generally used for data storage or as the location for additional software to be installed.

Components of a Hard disk: Internal

i. Disk Platter: May consists of one or many platters which are flat and round disks. Made of a rigid material such as aluminum, alloy, glass, or glass composite and coated with a magnetic substance.

ii. Spindle: Runs through a hole in the middle of every platter, multiple platters are placed one above another. Spins the platters at a faster speed, with some spinning at thousands of revolutions per minute (RPM).

iii. Motor: Rotates the platter and is attached to the spindle.

iv. Electromagnetic Heads: Writes the information in the form of magnetic impulses on the disks and also reads the information that was recorded from them. Read/Write head moves over the platter and reads or writes data over the platter. In the case of more than one platter on a hard disk, each platter has a read/write head on either of its sides. Smaller platters save space as well as improve the seek time, that is, disk performance as the movement of heads at a far space is not required.

v. Tracks: Concentric circles are further divided into sectors where data is stored on the magnetic surface of the platter. Data resides within a specific sector of a specific track on a particular platter. When the platter is

spinning, the part under the read/write head is known as a track. Tracks and sectors are defined physically through the process of low-level formatting (LLF), which designates the location of tracks and sectors on every disk.

Tracks are numbered for reference to the computer during the read/write operation of data. The numbering ranges from zero to the highest-numbered track (mostly 1023) starting from the outermost edge, which is the first track of the disk to the track which is nearest to the platter center, that is, the highest-numbered platter close to the center.

vi. Sectors: Divided as segments in a track, they are the smallest physical storage unit on a disk. The size of sectors is 512 bytes (0.5 KB) in size. Whenever a low-level format is performed, a number is assigned to the sector before the contents. The number in the header helps identify the sector address on the disk. A computer can locate the physical location of the data on the disk through the tracking number and specific sector address.

- **Bad Sectors**

Sectors that cannot store data due to some accidental damage or manufacturing defect are known as bad sectors. In case of sectors getting damaged, those specific areas become unusable but it does not impact the other areas of the disk. Since damage to sectors denotes damage at the disk surface, it cannot be repaired, thereby leading to irreversible loss of data, if any, in that section of the hard disk. Such sectors are marked as bad to avoid attempt of data being written in those areas by an operating system or any software.

Windows supports programs such as ScanDisk and CheckDisk, while Linux allows the use of the Badblock tool to detect sectors that are damaged and to tag them as bad sectors.

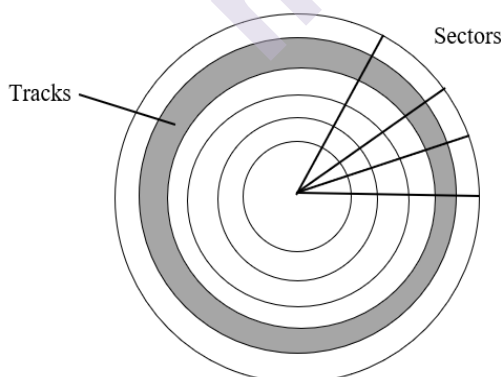


Figure 3.4: Tracks and Sectors on a hard disk

Disk Capacity

Disk Capacity is the capability of the hard disk in terms of the amount it can store. Measurement of disk capacity is done in bytes (7 or 8 bits), where a bit is the smallest measurement unit of data. A bit consists of

binary values, either 1 or 0, indicating on or off. A bit is abbreviated as b, while a byte is denoted by B. A kilobyte (KB) equals 1,024 bytes, instead of 1000 bytes since it is calculated using binary (base 2) instead of decimal (base 10).

Disk capacity in terms of different units are as follows:

- Kilobyte (KB) = 1,024 bytes
- Megabyte (MB) = 1,024 KB = 1,048,576 bytes
- Gigabyte (GB) = 1,024 MB = 1,073,741,824 bytes
- Terabyte (TB) = 1,024 GB = 1,099,511,627,776 bytes
- Petabyte (PB) = 1,024 TB = 1,125,899,906,842,624 bytes
- Exabyte (EB) = 1,024 PB = 1,152,921,504,606,846,976 bytes
- Zettabyte (ZB) = 1,024EB = 1,180,591,620,717,411,303,424 bytes
- Yottabyte (YB) = 1,024ZB = 1,208,925,819,614,629,174,706,176 bytes

Calculating Disk Capacity

Hard disk capacity can be determined based on the elements of the disk, including the number of tracks, sectors and surfaces on which various amounts of data can be accessed or written.

Formula: Capacity = (bytes/sector) * (sectors/track) * (tracks/surface) * # of surfaces

Example: To calculate the disk capacity of the drive, considering the following factors:

Bytes per sector 256

Total tracks: 21,576

Total cylinders: 7,192

Sectors/track (avg): 213

Number of heads: 3

Following specification of the actual hard disk, does not contain tracks/surface, but the values for the total tracks and the number of physical heads is provided. Since each head reads the disk surface, it helps find the total number of surfaces on the disk.

To obtain the tracks/surface, the total tracks can be divided by the number of heads, that is, (21,576/3). Thus, the formula can be written as:

$$\text{Capacity} = (\text{bytes/sector}) * (\text{sectors/track}) * \text{total tracks}$$

The capacity of the above-mentioned specification can be calculated as:

$$\begin{aligned}\text{Capacity} &= 256 \text{ bytes/sector} * 213 \text{ sectors/track} * 21,576 \text{ total tracks} \\ &= 1176496128 \text{ or } 1.1\text{GB}\end{aligned}$$

3.3.2 Hard Disk Interfaces

It is an interface which connects a hard disk to the computer for data access from the disk, thus it is one of the standard technologies which acts as a communication channel through which data flows between the HDD and the computer. An interface helps connect the hard disk to a disk controller, which is mounted directly on the computer's motherboard. Few commonly used hard disk interfaces include:

i. IDE/EIDE/ATA

- IDE stands for Integrated Drive Electronics since the disk controller is integrated with the disk drive's logic board, while EIDE is an acronym for Enhanced IDE.
- IDE is also known as ATA (Advanced Technology Attachment) which is a standard of the ANSI (American National Standards Institute).
- Mostly all modern PC motherboards consist of two EIDE connectors. Maximum two ATA devices (HDD or CD) can be connected to each connector, in a primary/secondary configuration, where the primary drive responds to the probes or signals on an interrupt (signal from any device or program to its OS that causes a pause to determine next task to be done) and shares it with the secondary drive which shares the same cable. Users can configure settings where drives can be considered as primary, secondary or cable-controlled.

ii. SCSI

- SCSI (Small Computer System Interface) is an ANSI standard with faster data transfer than IDE/EIDE. SCSI connectors and controllers are in-built within some motherboards, while SCSI disks can be added by installing a SCSI Controller card in one of the expansion slots.
- Devices are chained on a SCSI bus, each with a different SCSI ID number.
- Either eight or sixteen SCSI IDs can be attached to one controller depending on the SCSI version, wherein controller uses one ID while allowing seven or fifteen SCSI peripherals.

iii. USB

- USB is an acronym for Universal Serial Bus, which is used for various peripherals, such as keyboards, mouse, and other devices, that previously required serial and parallel ports, and several newer

technologies including digital cameras and digital audio devices.

- Since these devices are based on a bus topology, they can be daisy-chained together or connected to a USB hub, allowing up to 127 devices to connect to the computer at the same time.
- USB also provides an interface for external hard disks, where disk which provide USB connection can be mounted by plugging into a USB port of the computer.
- Current standard for USB is USB 2.0, backward-compatible to earlier 1.0, 1.1 standards and supports bandwidths of 1.5Mbps (megabits per second), 12.5Mbps, and 480Mbps, 12.5Mbps, and 480Mbps respectively.
- USB 2.0 supported external USB hard disk provides faster exchange of data between the computer and the HDD.

iv. Fibre Channel

- It is another ANSI standard which provisions faster data transfer and uses optical fiber for connecting devices.
- Various standards are applicable to fiber channels, but Fiber Channel Arbitrated Loop (FC-AL) primarily applies to storage, that is, it is designed for mass storage devices and for Storage Area Networks (SANs) where a SAN is a network architecture where computers attach to remote mass storage devices such as disk arrays, tape libraries, etc.
- Since optical fiber connects devices, FC-AL supports transfer rates of 100 Mbps, and may replace SCSI for network storage systems.

3.3.3 File Systems

File management systems or file systems are used by the operating system to organize and locate the data stored on a hard disk. File systems manage storage media such as hard disks along with controlling sectors on those drives, it also keeps track of sectors occupied for storage of data and vacant sectors, available for storage.

Network file systems provision client's access to data on a remote server. Hierarchical systems involve organization of data in a tree structure.

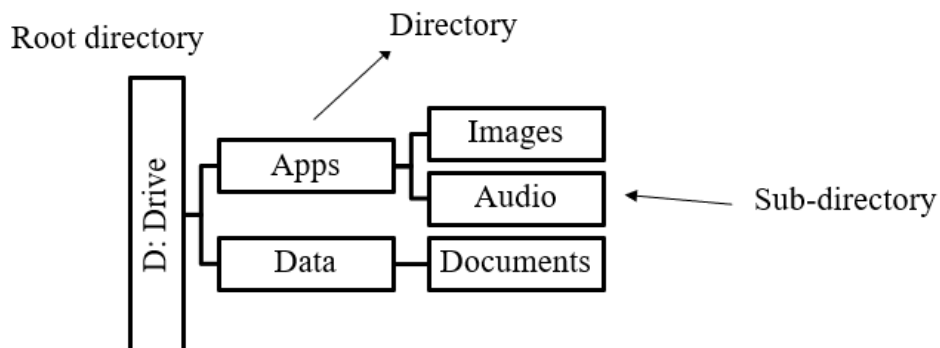


Figure 3.5: Hierarchical Directory Structure

As seen in Figure 3.5., a hierarchical file system looks like an inverted tree.

In figure 3.5., the base of the structure is a root directory, and directories(folders) branch from the root. These directories are containers which store files or other directories. Directories which are present in other directories are also known as subdirectories (subfolders).

A. Microsoft File Systems

Different operating systems use different file systems, while some OS support multiple file system. Few file systems which are commonly used by Microsoft OS include:

i. FAT12

- FAT (File Allocation Table) file system was developed by the DOS operating systems.
- The first version of FAT used a 12-digit binary number(12 bits) for cluster information, hence it was called as FAT12.
- It was useful for the smaller hard disks that came with the original IBM PC (less than 16MB in size) and were also used to format floppy diskettes.

ii. FAT16

- FAT16 was a standard file system for formatting hard disks for a long time, it was developed for disks greater larger than 16MB.
- Uses 16-bit allocation table entries and is supported by all Microsoft operating systems, from MS-DOS to Windows XP along with some non-Microsoft operating systems, such as OS/2 and Linux. Thus, it was the most universally compatible file system.
- Some drawbacks of FAT16 included its inability to scale well to large disks since the cluster size increases as disk partition increases, lot of space was wasted when a large disk greater than 2GB was formatted with FAT16. It doesn't support file-level security, that is, individual level permissions to files and directories) and also does not support file-level compression, as the entire drive needs to be compressed.

iii. VFAT

- Virtual FAT or VFAT, is a file system driver introduced in Windows for Workgroups 3.11 and was supported by Windows 95.
- It works in protected mode and allows usage of long filenames with FAT16.
- VFAT is a program extension and not a file system, which handles filenames over the 8.3 limitations imposed by the original FAT16.

iv. FAT32

- FAT32 uses a 32-bit allocation table and was first supported by the OSR 2 version of Windows 95 (95b).
- Advantages of FAT32 over FAT16 included:
- Efficient use of space with larger hard disks through small cluster sizes
- Support for larger partitions, up to 2TB in size, theoretically (Practically supports up to 32GB)
- Better reliability, as includes backup copy of information in the boot record.
- Disadvantages of FAT32 was that it is incompatible with several versions of Windows such as MS-DOS, Windows 3.x, Windows 95a, Windows NT, and some non-Microsoft operating systems (although FAT32 drivers were available from third-party vendors for Windows 95, NT, and even non-Microsoft operating systems such as Linux). Additionally, the overhead used by FAT32 can also slow performance slightly.

B. NTFS

- NTFS (New Technology File System) is the most secure file system for computers running Microsoft Windows operating systems. NTFS was released in 1993 as a replacement to FAT file system on Windows NT OS, followed by successive releases in Windows 2000, 2003 Server, XP and Vista.
- It was more robust and secure as compared to other Microsoft file systems. NTFS handles partitions, where partitions are logical sections of a hard disk which operate as a separate drive. Example: A hard disk could be partitioned as C: , D: or E: drive on the computer.
- NTFS supports very large partition sizes (up to 16EB theoretically) and permits creation of volumes that can span two or more partitions.
- It is more reliable since it supports hot fixing feature, wherein the OS detects a bad sector on the disk and relocates the data from that sector to a good sector, and marks the bad sector so that the system does not

use it. It happens in the background which does not require any user intervention.

i. Metadata and the Master File Table (MFT)

- Metadata is the information about a specific set of data, which contains information such as author of the file, its size, and other technical information hidden from the common user, that is, it is data about data.
- It describes a file, its format, its creation time, and other details.
- NTFS stores additional files which are hidden in the system and contain information about users, files and other details.
- Whenever a disk is formatted to use NTFS, the files are created with their locations being stored in these files, known as Master File Table (MFT) to keep track of each file on the volume.
- FAT file system keeps track of files using a File Allocation Table, NTFS performs similar complex functions using a Master File Table.

ii. NTFS Attributes

- -A record stored in the MFT works with NTFS attributes, every file and directory are viewed as a set of file attributes containing information such as name, data, and security information by NTFS.
- The data which defines a file, and is used by the OS and other software's to decide how a file is accessed and used is called as attribute.
- Every attribute has a code and might contain information on attribute's name and description in MFT.
- Two different kinds of attributes can be used in NTFS:
- Resident attributes: Can fit in an MFT record. The name of the file and its timestamp are always included as resident attributes.
- Non-resident attributes: Are allocated on the disk to one or more clusters elsewhere. These attributes are useful when the information about any file is too large to fit in the MFT.

iii. NTFS Compressed Files

- - NTFS permits compression of files, entire NTFS volumes or file-by-file basis to save space. It compresses individual folders, files or anything on the drive using the NTFS file system.
- The file gets automatically decompressed when being read and compressed whenever the file is saved or closed. Whenever the data is compressed on an NTFS drive it can only be read by the file system, if a program attempts to open a compressed file, then the file should be decompressed by the file system's compression drive before providing access to it.

- Compressing data does not need additional software for compression and decompression thereby saving disk space and archive folders.

iv. NTFS Encrypting File Systems (EFS)

- Encryption involves the process of file encoding to make it unreadable for any unauthorized person to open, copy, view, or rename the data, file, or folder.
- Encryption can be performed on a disk as well as on a single file, where disk encryption refers to encrypting all the contents on the diskette, hard disk or removable disk and file encryption refer to encrypting the data on a disk through file-by-file basis.
- Disk or file encryption can be built onto an OS or file system. EFS cannot protect data on floppy diskettes as they cannot format in NTFS format, but can encrypt files/folders.
- EFS is integrated with the OS, where the encryption and decryption processes are invisible to the user. EFS relies on public key cryptography and digital certificate, wherein public key cryptography consists of public key and private key to be used together and digital certificate helps identify the person logged into the system, and credentials to verify authorized person uses digital certificates associated with the user account.
- While public key cryptography is time-consuming, digital certificates could cause issues in case the user has left the system logged in and unattended leading to unauthorized access.

C. Linux File Systems

- Linux is an open-source OS based on UNIX OS. Use of a Virtual File System (VFS), supports multiple file systems where VFS acts as an abstract layer between kernel and lower-level file systems. Linux can support multiple file systems using VFS, such as:
 - i. ext: First version of Extended file system created for Linux. It was the first file system to use VFS added to the Linux kernel, which was replaced by ext2 and xiafs based on the older Minix system (shortcomings such as 14-character file naming limit, 64 MB limitation on partition sizes) and not found in current systems since they are obsolete.
 - ii. ext2: Second extended file system, which offers great performance with file size of upto 2 TB. This file system had implementation of a data structure which includes inodes, storing information about files, directories and other system objects. It stores files as data blocks on the hard disk. The smallest units of data in the file system are called blocks, and a group of blocks that contain information to be utilized by the operating system and is known as a superblock.
 - iii. ext3: Third extended file system, extends ext2. A major advantage of ext3 is a journaled file system, making it easier for recovery where a

journal resembles a transaction log used in databases, where the data is logged before it is written. Journal is updated prior to blocks of data being updated in ext3 and it could be used to restore the file system ensuring that any data which was not written in blocks prior to the crash is resolved. In case of any issue on ext2, a filesystem check (fsck) needs to be resolved with files and metadata on the system.

iv. ext4: Fourth extended file system, has been improvised in terms of performance, which supports volumes of up to 1 EB.

D. Mac OS X File System

- Originally, Macintosh used the Macintosh File System (MFS) used to store data on 400KB floppy disks.
- Files are stored onto hard disks in MFS into two parts: a resource fork which stores structured information and a data fork which stores unstructured data. Thus, the data used in a file will be stored in a data fork, whereas file information such as menus, icons, menu items, etc. will be stored in the resource fork.
- The resource fork enables files to be opened by the appropriate application, without a file extension requirement as well as to store metadata. MFS was further replaced by Hierarchical File System (HFS) which uses multiple forks while storing data and manages the data on both the hard disks or floppy disks.
- HFS supports filenames of 255 characters length. Since MFS works with floppy disks leading to slow down on larger media, while HFS works with hard disks and uses a hierarchical design through a Catalog File which replaces the flat table structure which was used by MFS.
- Apple launched a HFS new version known as HFS Plus, where improvements were made in performance and how HFS plus handled data.
- HFS and HFS Plus store blocks of data on the hard disk, where volumes are divided into logical blocks of size 512 bytes. HFS uses 16-bit block address whereas HFS Plus supports an improvement with 32-bit block addresses being supported.

E. Sun Solaris 10 File System: ZFS

- Sun Solaris is an open-source OS developed by Sun Microsystems, the first ZFS file system was first used in Solaris 10.
- ZFS (Zettabyte File System) handles large amount of data and uses virtual storage pools known as zpools, composed of virtual devices (vdevs). These pools could contain various vdevs, further containing one or more storage devices, along with those using Redundant Array of Inexpensive Disks).

- ZFS is a 128-bit storage system, supporting more data and variable sized blocks of up to 128 KB. It can improve I/O throughput, if the file system compresses data to fit into smaller blocks.

F. Network File Systems and File Sharing Protocols

- Permits users to access and update the files on remote computers as if they are placed on the local computer. File systems on remote machine are irrelevant whenever machine's resources are accessed, this also helps OS such as Windows 9x computer which does not support NTFS to read and write NTFS files stored on a remote computer such as Windows NT, 2000, XP, or Vista. File sharing across a network can be done through the following:

i. Server Message Block (SMB):

Microsoft uses SMB protocol to permit client applications to access as well as write to remote files and request services from server applications on remote systems. SMB is involved in Windows OS. SAMBA is an implementation of SMB and the Common Internet File System (CIFS) which can be installed on UNIX computers to allow Windows clients to access their files as if SMB servers.

ii. Common Internet File System (CIFS):

A protocol proposed as a standard which permits remote files access across the internet. CIFS is an open (nonproprietary) version of SMB. SMB and CIFS run on top of TCP/IP protocol stack.

iii. NetWare Core Protocol (NCP):

NCP is a set of protocol which provide file and printer access between clients and remote servers on NetWare networks. NCP runs over IPX or IP.

iv. Network File System (NFS):

A client-server application which was developed by Sun Microsystems to run on TCP/IP which allows remote file access. NFS uses the Remote Procedure Call (RPC) as the communication method. Used for the remote file access by UNIX/Linux machine, can also be installed on Windows or Macintosh computers.

G. Disk Partition

- To use a hard disk which can be formatted, a file system can be used. Logical division of a hard disk which permits a single hard disk to work as though it is a single or more hard disks on the computer is known as partition.
- Even though multiple partitions are not being used, a partition must be setup so that the OS knows that the entire partition will be considered. A drive letter can be given to the partition and it is formatted to use a file system. When an area of the hard disk is formatted and assigned a drive letter, it is known as a volume.

- Example: On a single volume of Windows computer, C: could be formatted as NTFS and D: could be formatted as FAT32. Similarly, for Linux different drives can be formatted as ext or ext2 respectively. Thus, it provides the advantage of different file systems used on the same computer.
- Two types of partitions exist, namely:
- Primary partition: Partition on which an OS can be installed and is used whenever the computer starts to load the OS.
- Extended partition: Partition which can be divided into additional logical drives. It does not need a drive letter or installation of file system. Instead OS can be used to create more logical drives with extended partitions with drive letters assigned to logical drives.

i. System and BootPartitions

- Amongst multiple partitions, a partition maybe designated as the boot partition, system partition or both. A system partition is responsible for storing files which are used to start or boot start the computer, wherein when a computer is powered on it is known as cold boot and when it is restarted from within the system it is known as warm boot.
- Boot partition is a computer volume which contains the system files which are used to load the OS. System partition is where the OS is installed, whereas the system and boot partition can exist as separate partition on the same computer or else on separate volumes.

ii. Boot Sectors and Master Boot Record

- Many sectors exist but the first sector, that is, sector 0 on a hard disk is considered as boot sector, where the boot sector contains codes which the computers use to boot the machine. The boot sector is also known as the Master Boot Record (MBR), where the MBR consists of a partition table to store the information on which primary partitions need to be created onto the hard disk to start the machine. Using the partition table in the MBR, the computer understands the organization of hard disk before the OS starts interacting within it.
- Once partitions are set up on the machine, they can provide the information to the operating system.

iii. NTFS Partition Boot Sector

Since NTFS uses a Master File Table used to store file system information, location information of the MFT as well as MFT mirror file is stored in the boot sector. A duplicate of the boot sector is stored at the disk's logical center, to prevent the information from getting lost and for recovery.

Clusters and Cluster Size

- A group of two or more consecutive sectors on a hard disk are called clusters, where they are the smallest amount of disk space that can be allocated to store a file.
- A sector is mostly 512 bytes in size but the data stored onto a hard disk is greater, thus data is saved on a greater number of sectors.
- Clusters are logical units of file storage, where a unique number is assigned to every cluster and their respective files can be accessed.
- Cluster size is controlled by the OS, wherein the cluster size is determined by different factors such as the file system being used. During the formatting of a drive, the ability to select the file system in which the disk will be formatted is called allocation unit size.

Slack Space

- Clusters are a fixed size, the entire space will be used by the cluster. Example: Cluster size if 4,096 bytes, but a 20-byte file is stored onto the disk, the entire 4KB cluster would be used even though 4,076 bytes of space will be wasted. This wasted space may be known as Slack Space or File Slack, where it is the space area between end of the file and the last cluster used by that data.
- The cluster size should be smaller, so that the amount of space in the final cluster can be used to store a file with lesser unused space being wasted and lead to effective usage of disk.
- The formula to calculate the amount of wasted space is:

$$(\text{Cluster size}/2) * \text{number of files}$$

It provides a estimate of disk space being wasted on a particular hard disk, instead of the exact amount.

Lost Clusters

- Each cluster is a unique number which is used by the OS to keep track of files that are stored on the hard disk. At equal intervals of time, even though the cluster has not been assigned to a file still the OS will mark the cluster as being used, this concept is known as a lost cluster.
- Lost clusters are called as lost file fragments or lost allocation units. In Linux or UNIX machines clusters are denoted as blocks, while they are referred as lost blocks or orphans.
- Lost clusters do not belong to any specific file, instead they are created from sudden shutting down of computer, closing of application, file not being closed appropriately, etc.
- When such an event occurs, the cluster must have been assigned to the data in the cache, but may not have been written due to unexpected events.

- In case the system was shut down incorrectly, the cluster might also have had data written to it before, this data could be a fragment of the file or any other corrupted data.
- Tools such as ScanDisk and CheckDisk could also be used to detect lost clusters and also to recover the data stored in the cluster.

3.4 LET US SUMUP

This unit helps gain an understanding into the various factors that need to be considered for setting up a cyber forensic laboratory, performing digital forensics on different OS, the different types of file systems and hard disk drive, tools needed for performing digital forensics on a windows-based machine, tools and techniques required for evidence acquisition and data replication.

3.5 LIST OF REFERENCES

[1] The official CHFI Exam 312-49 Study Guide by Dave Kleiman, Syngress Publication, 2007.

3.6 BIBLIOGRAPHY

[1] EC-Council CHFIv10 Study Guide, EC-Council, 2018

3.7 UNIT ENDEXERCISES

1. Which of these is not a space planning factor in the facilities build-out?
 - a. Administrative area
 - b. Examination space
 - c. Domain area
 - d. Evidence storage
2. Write Blockers methodology is deployed for prevention of _____.
 - a. Data Spoliation
 - b. Data Availability
 - c. Data Confidentiality
 - d. Data Repudiation
3. _____ is considered as one of the main cost factors for laboratory scope of service provision, initial space targets as well as ongoing laboratory operations.
 - a. Tool Validation
 - b. Software Licensing
 - c. Software Validation
 - d. System Licensing

4. Whenever a disk is formatted to use NTFS, the files are created with their locations being stored to keep track of each file on the volume. This concept is known as _____ .
- Master File Table
 - Master File
 - Master Table
 - Master Data Table
5. Concentric circles further divided into sectors where data is stored on the magnetic surface of the platter are known as _____.
- Disks
 - System
 - Tracks
 - Drives
6. _____ is a computer volume that contains the system files which are used to load the operating system.
- Last partition
 - Boot partition
 - Data partition
 - Computer partition
7. _____ do not belong to any specific file, instead they are created from sudden shutting down of computer, closing of application, file not being closed appropriately, etc.
- Found cluster
 - Lost cluster
 - dd cluster
 - Slack cluster



WINDOW FORENSICS, DATA ACQUISITION AND DUPLICATION

Unit Structure

4.0 Objectives

4.1 Introduction

4.2 Forensics on Windows Machine

4.2.1 Locating and Gathering Evidence on a Windows Host

4.2.2 Understanding file slack and its Investigation

4.2.3 Interpreting Windows Registry and Memory Dump Information

4.2.4 Investigating Internet Traces

4.2.5 Investigating System State Backups

4.3 Acquire and Duplicate Data

4.3.1 Data Acquisition Tools

4.3.2 Hardware Tools

4.3.3 Backing Up and Duplicating Data

4.3.4 Data Acquisition in Linux

4.4 Let us SumUp

4.5 List ofReferences

4.6 Bibliography

4.7 Unit EndExercises

4.0 OBJECTIVES

After studying this unit, it will help you to:

- Perform digital forensics on a windows-based machine.
- Select appropriate tools for collecting evidence.
- Understand the importance of backups.
- Determine the various tools and mechanisms that can be used for acquiring and replicating the data.

4.1 INTRODUCTION

Certain procedures need to be followed to perform forensic on a Windows machine without tampering the evidence. To fetch or acquire the data and then process it with the help of various forensic tools is a major concern. Usage of those tools for acquiring data and backing them up in case of any requirement for disaster recovery or data loss should be taken into consideration.

4.2 FORENSICS ON WINDOWS MACHINE

4.2.1 Locating and Gathering Evidence on a Windows Host

- Evidence location involves the process of investigating and gathering information of a forensic nature and legal importance. It aids in the investigation of both criminal investigations and civil suits.
- Several locations could act as a rich source of evidence in Windows OS. File attributes and timestamps are also considered as valuable. Perpetrators may try to change a file's attributes so that their tracks can be covered or the data stays hidden within the system.
- Few important sources of electronic evidence on a Windows host could include:

Files, Slack space, Swap files, unallocated clusters, unused partitions, and hidden partitions.

a. Gathering Volatile Evidence

- It is considered one of the most important aspects of digital forensics. During the investigation of a Windows-based OS for the probable evidence or information and facts that are related to the case, it should be ensured that all the relevant volatile data, that is, current data about the system, registry, cache and memory has been collected. If the system is powered down, data may be lost and cannot be recovered.

- In non-volatile memory data isn't lost, after the power is cycled.

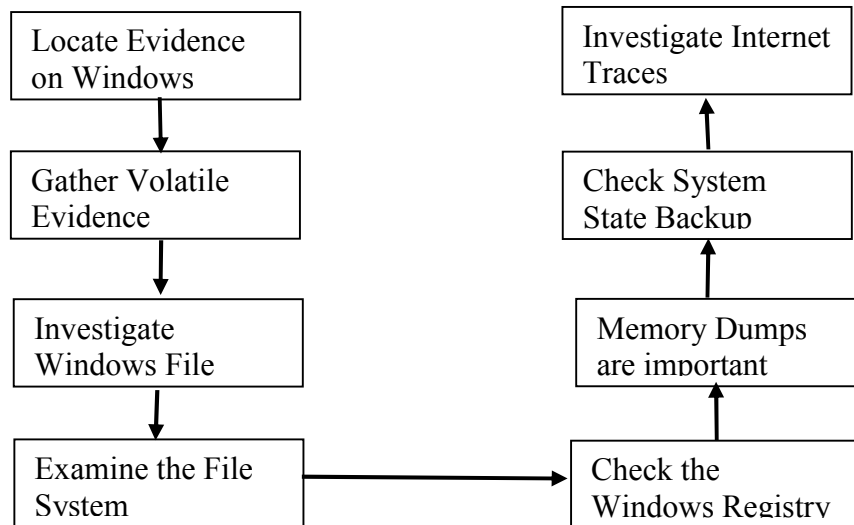


Figure 4.1: Steps for searching data on a windows-based system

- Within the volatile data most crucial areas which could be checked for evidence would include registers, physical and virtual memory, cache, network connections, running processes, and disk.
- Any other external device connected to the system such as floppy disk, tape, CD-ROM, and printers should also be verified for evidence if any.
- All the data captured should be gathered to store in external devices for it to be safely removed and placed offline at another location.
- Capability of a windows forensics tool to gather data on a live Windows system is very important. Offline imaging and searching through disk images are standard fare for a computer forensic analyst. But sometimes it could be infeasible to take a system offline for imaging, especially for larger e-commerce sites where critical infrastructure is a factor to be kept online. Thus, live imaging is an important aspect to be considered.

b.Helix Live on Windows

- Helix runs on Windows to collect evidence from active or live Windows systems which could cause a constant flux, which is constantly changing such as virtual memory.
- Turning off the system could result in evidence destruction. Thus, the Helix tool can be used to collect volatile information and presents a portable forensics environment that may provide access to many windows-based tools.
- Helix Live Response is about the tools wherein the CD contains static binaries for Linux, Solaris, and Windows using GNU utilities and Cygwin tools.

- The Helix.exe graphical application will only operate in a live Windows environment and will vary on each version of OS. Since windows are live, many DLL files are used by Helix and the OS during this process.
- The Helix Windows Live function is a GUI interface to a Windows-based CLI and other tools. A major advantage is that Helix performs the actions to maintain the integrity of the command line so that the built-in Windows tools are not run through the compromised system, thereby risking the data from corruption.
- Windows command-line tools which can be accessed from the Helix.exe application on the CD may include .cab extractors, ipconfig, netstat, kill, etc.
- Tools available from Windows Live side of Helix for forensics may include:
 - Access PassView
 - Astrick Logger
 - Drive Manager
 - FAU
 - Forensic Server Project
 - FTK Imager
 - Galleta
 - HoverSnap
 - IECookiesView
 - IEHistoryView
 - IRCR (The Incident Response Collection Report)
 - Mail PassView
 - MEM Dump
 - Messen Pass
 - Mozilla Cookies View
 - Network Password Recovery
 - Pasco
 - PC Inspector File Recovery
 - PC On/Off Time
 - Process Explorer
 - Protected Storage Pass View
 - Ps Tools Suite
 - Pst Password Viewer

- PT Finder
- PuTTY SSH Client
- Reg Scanner
- Re SysInfo
- Rifiuti
- Rootkit Revealer
- Sec Report
- Win Audit
- Windows Forensic Toolchest (WFT)

c. MD5 Generators

MD5 Generators are used to maintain the integrity of a file, file system, or application. A cryptographic hash of the bit-wise information in the data will be created by the application. This added layer of protection helps maintain the value of the chain of custody as well as to ensure the admissibility of the evidence that the evidence has not been tampered with.

d. Pslist

Displays process, CPU, and thread statistics or memory information for all processes currently running on the system. The process information listed involves process execution time, process execution in kernel and user modes, physical memory that the OS has allocated to the process.

Example:

```
Pslist [-?] [-d] [-x][-t] [-s [n] [-r n] ] [\\computer [-u username] [-p password] ] [name | pid]
```

where,

- d: Displays statistics for all the active threads on the system, grouping the threads with their owning process
- m: Displays memory-oriented information for every process
- x: Displays CPU, memory, and thread data for each process specified
- t: Displays process trees

e. fport

- Displays all the open TCP/IP and UDP ports and maps them to the applications which own the port. It is similar to netstat, except that it maps the ports to the running processes with the PID, process name, and path. The switches may be used through either a / or a – prior to the switch. The command-line switches include:

/? Usage help

/i Sorting by PID

/p Sorting by port

/ap Sorting by application path

/a Sorting by application

f. Psloggedon

- Displays both locally logged on users and users logged through resources for either local or remote computer, it verifies which users are logged in by examining them under the HKEY_USERS keys.
- Psloggedon searches for the corresponding username and displays that particular user name for every key with a name, that is, a user SID (Security Identifier).
- Psloggedon uses NetSessionEnum API to verify who has logged onto a computer through resource shares.

Example: psloggedon [-?] [-l] [-x] [\\compname | username]

- Few common parameters include:
- ? Shows supported options and measurement units for output values.
- l Shows local logon instead of local as well as network resource logons.

4.2.2 Understanding file slack and its Investigation

- A windows disk cluster is a fixed-length data block used to store files. File slack is the gap
- or the space that exists onto the Windows disk between the end of the file and the end of the lastcluster since the sizes of both can never match. System-associated data such as usernames, passwords, and other sensitive data can be found within the slack.
- Storage space is wasted if there is an increase in the slack space due to larger cluster sizes.
- Window OS fills the difference between the end of a file and the end of a cluster with data from its buffers, in case there is no space available. This data is selected randomly from the system's RAM is known as RAM slack since it is obtained from the computer memory.

- RAM slack consists of created, viewed, modified, or copied files, since the last time the system was booted. Encase software provides tools to perform complex digital forensic investigations and manage large volumes of digital evidence along with viewing computer drive contents.

- To examine file systems:
- Built-in Tool: Sigverif.exe
- Can analyze a system as well as report on any unsigned drivers detected. To run the tool:

Click Start | Run, type Sigverif, click OK -> Click Advanced button -> Select Look for others which are digitally unsigned -> Select WINNT | System32 | Drivers folder, click on OK.

- Sigverif displays all the unsigned drivers installed on the system after its process completion.
- List of signed and unsigned drivers detected by Sigverif.exe can be viewed in Sigverif.txt file within the Windir folder, that is, Winnt or Windows folder, while unsigned drivers are marked as Unsigned.

Word Extractor Forensic Tool

- An application which extracts the human-understandable interpretation from the computer binary format and resembles the UNIX command, strings. It includes features such as replacing non-human words with spaces or dots for better visibility, supports wrap text as well as drag and drop, multitasking through response to command and large file processes, saving results as txt or rtf.

4.2.3 Interpreting Windows Registry and Memory Dump Information

- Registry is a component to be examined during the investigation of a Windows system. Selected keys should be verified with significance to supply evidence for what the services have been running for, services presently running and who has logged into the system over a certain span of time. Primary keys to be known include:

a. HKEY_LOCAL_MACHINE

- \Software\Microsoft\Windows\CurrentVersion\Run
- \Software\Microsoft\Windows\CurrentVersion\RunOnce
- \Software\Microsoft\Windows\CurrentVersion\RunOnceEx
- \Software\Microsoft\Windows\CurrentVersion\RunServices
- \Software\Microsoft\Windows\CurrentVersion\RunServicesOnce
- \Software\Microsoft\WindowsNT\CurrentVersion\Winlogon

b. Registry Viewer Tool: Reg Scanner

- The RegScanner is a registry tool from NirSoft provides a search function that can search for any registry value and display the instances of that value in a single view. It allows a selection and jumps function which redirects to that registry key for editing.
- It also helps export results to a REG file for saving or loading into another computer.
- No installation will be required; it can be unpacked from the .zip file into any folder and run. After launching, it provides an option to select which base key to start searching from. The search string could be case sensitive or insensitive along with the match being exact or within certain parameters.
- Example: Matching can be done against data and the values, instead of the key names themselves.
- The application also provisions a search function for Unicode strings in binary values.
- -RegScanner does result reporting in a grid-formatted list, to be saved as REG file or either exported into an HTML format.

c. Microsoft Security ID

Microsoft Security IDs can be obtainable in Windows Registry key:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\ProfileList

The ProfileList key holds the SIDs, selecting the individual ID value entry, along with an associated username is probably feasible. Some specific IDs enclosed under Microsoft Security are as follows: Retrieve MAC Address, Registry Dump, Registry Scan, Registry Dump, Event Logging Utility, etc.

Importance of Memory Dump

- After every crash, Windows generates a memory dump file that contains information that can help in determining why has the system stopped. For memory dump in Windows, the system needs a paging file with a minimum of 2 MB on the boot volume.
- Memory dumps are useful in helping with the system bug diagnosis and for memory content analysis during a program failure. They might contain binary, octal or hexadecimal forms of information.
- When a system runs MS Windows 2000 or later, a new file gets created whenever the system stops suddenly. Microsoft tool, dumpchk.exe can be designed to verify memory dump files for information.

- The systemroot | Minidump folder consists of a small memory dump files list. While conducting an MS Windows system, memory dumps need to be checked and obtained on the system. A memory dump file may contain:
 - Stop message with its parameters
 - Loaded drivers list
 - Processor's context (PRCB) for the processors responsible for stopping the normal operation of Windows
 - Processor information and kernel context (EPROCESSSES) for the processes stopped
 - Process information and kernel context (ETHREAD) for the thread which stopped
 - The kernel-mode call stack for the thread is responsible for stopping the process from execution.

Pagefile.sys and PMDump

Windows XP Professional uses paging file information to generate a memory dump file in the system root directory. This dump file analysis can be done to supply data, that is, the reason for the crash during the offline analysis. Analysis can also be done through tools running on another computer.

PMDump or Post Mortem Dump tool performs the dumping of memory contents relative to any process or a file with its process stopped. It can be used for conducting forensic analysis of a dump file.

What is Virtual Memory?

An imaginary location that is supported by the Windows OS is known as virtual memory, where it is an alternate memory address set that expands the available memory range.

Data that isn't needed often for programs can be store in instructions and data into the virtual memory. Virtual memory is converted into RAM, whenever these memory address locations are called.

An OS divides the virtual memory into pages whenever virtual memory needs to be copied into RAM, where each page consists of a fixed number of addresses stored on disk which are yet to be called by the OS.

When the OS calls the pages, it is copied from disk memory to RAM, which translates virtual addresses to real addresses also called mapping, while the process where virtual pages are copied to main memory is known as paging or swapping.

System Scanner

System scanner acts as a replacement to the task manager, wherein the System scanner fetches more specific information about the processes. The main window in the system scanner consists of the current running processes in the system, number of threads per process as well as the executable path, while the status bar shows the overall number of running processes, which is updated every 5000 milliseconds. The refresh time can be customized along with the colors of the memory regions in the memory map as per requirement.

Integrated Windows Forensics Software: X-Ways Forensics

X-ways forensics is an advanced work environment, based on WinHex for the digital forensic analysis. Its features include forensic sound disk imaging and cloning, complete directory structure examination inside raw image files, native support for various file systems, several data recovery techniques along with file carving, hard disk cleansing for producing forensically sterile media, automated file signature verification etc.

4.4.4 Investigating Internet Traces

Evidence can be searched from different locations in Internet Explorer. Following files and folders can be investigated for analyzing Web browser activity:

- Cookies: Can be found on the following locations in Windows 2000/XP:
 - C:\Documents and Settings\%username%\Cookies
 - C:\Windows\Cookies (in Windows 95/98/ME)
- Typed URLs
- History
- Temporary Internet Files

Internet explorer can store records of sites visited by a user in the History folder, where the URLs of websites are present. C:\ drive also consists of Documents and Settings, further consisting of another folder, that is, Cookie's folder which stores cookies visited by each user based on which individual user folders are created. These files are further stored in the Temp folder, where the temporary internet file's location provides the name and number of sites visited by each user. Thus, temp files contain details of the user's activities in the various TMP files.

a. Traces Viewer

A tool that helps view all images, flash movies, pages, and other media files that are cached by the Internet Explorer browser on a system. It involves a function in which Web traces generated by Internet Explorer

can be removed from a system. Though, it does not wipe the evidence and can be uncovered.

b. IECookiesView

A forensic utility that displays the details of the cookies saved by the Internet Explorer. It provisions the capability to sort the cookies as per the name and their date. Additionally, it provisions a search function that can find a cookie in the list based on the website name. The cookie information can also be copied on the clipboard and using remote login, the cookies of other users of the same or another system can also be displayed.

c. IE History Viewer

Whenever a URL is typed into the address bar or any link is followed in Internet Explorer, it leads to the address being stored in the history index file. IE History Viewer inputs all the history data from the file and prints a list of URLs visited. The list of addresses is stored as text, HTML, or XML files through this application.

d. Cache Monitor

Cache monitor provisions a real-time view of the systems cache's present state as well as can check the configuration of dynamic caches. It can help the forensic analyst verify the cache policies and monitoring of cache statistics. Some other tools also provide the capability to monitor the data flow through cache and the data present in the edge cache. The statistics available through Cache monitor include:

- Cache hits: The match entries with the number of requests onto the edge servers.
- ESI Processors: Number of processes which are configured as edge caches.
- Cache Misses by URL: Cache policy that does not exist on the edge server for the requested template.
- Several Edge Cached Entries: Number of entries that are currently cached across all edge servers and processes.

4.4.5 Investigating System State Backups

A system state backup involves the backup of the entire system so that no data will be lost in case of a system crash or corruption of the driver files. To perform a forensic analysis of the evidence on a Windows system, only backing up the system is not sufficient. Thus, an extended data backup is essential to remain secure against any malfunction.

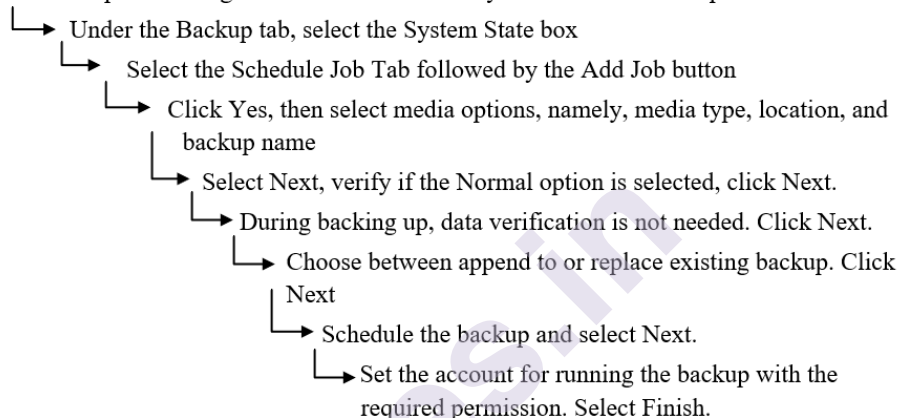
An extended state backup saves the:

- Active directory

- Registry
- Windows boot files
- System volume (SYSVOL)
- IIS Metabase
- COM+ class registration database

- The procedure to create a system state backup is as follows:

Go to Start option-> Programs -> Accessories -> System Tools -> Backup



Investigating ADS Streams

- NTFS consists of a compatibility feature known as Alternate Data Streams (ADS). It could help an attacker with hiding rootkits or hacker tools on a compromised system, which can further get executed without being detected by the system.
- Thus, ADS may be used as a way of hiding the executables or proprietary contents, if any.
- To maintain the integrity of an NTFS partition against unauthorized Alternate Data Streams, a third-party checksum application could be utilized.
- Common DOS commands like type can create ADS, wherein these commands in conjunction with > (redirect) and : (colon) could fork one file in another.
- Example: type c:/maliciousfile.exe > c:\winnt\system32\calculator.exe: maliciousfile.exe

Where, ADS Tool ? LADS (List Alternate Data Streams) :

Syntax: {file name} : {stream name}

Create: type textfile>visible.txt:hidden.txt

View: more <visible.txt:hidden.txt

- **CD-ROM Bootable Creation for Windows XP**

Multiple tools such as Bart's PE Builder and Ultimate Boot CD-ROM could be used to create bootable Windows CD-ROM. These tools could be useful for PC maintenance tasks and yield a complete Win32 environment with network support along with a GUI and NTFS/FAT/CDFS file system support.

- **Bart PE (Bart Preinstalled Environment)**

A Bart Preinstalled Environment (BartPE) bootable Windows CD-ROM or DVD can be created by Bart's PE Builder through the installation/setup CD of Windows XP or Server 2003. It can also restore any DOS-based boot disk. Windows versions that are supported include Windows XP (Home Edition or Professional) and Windows Server 2003 (Web, Standard, or Enterprise Edition).

Ultimate Boot CD-ROM

The execution of floppy-based diagnostic tools from CD-ROM drives onto Intel-compatible machines is permitted by Boot CD-ROM. This tool contains multiple diagnostic utilities which provide sharing of Internet access or web surfing. It does not need a separate OS. With network support, modifying NTFS volumes, recovering the deleted files, scanning the hard drives for viruses, and creating NTFS volumes are possible. It includes multiple CPU tests, memory tests, and peripheral tools.

4.3 ACQUIRE AND DUPLICATE DATA

4.3.1 Data Acquisition Tools

While selecting the tools to use, it needs to be ensured that data does not get modified. The validity of tools needs to be acceptable in court. Example: Tools such as Encase would lead to lesser chance of it being mostly scrutinized. Although tool validation is still required but using tools could make the process easier comparatively. Below mentioned data acquisition tools may consist of software to duplicate data, creating image files which may be mounted and analyzed later or hardware solutions which can acquire data from a suspect's machine.

a. FTK Imager

- Forensic Tool Kit (FTK) is a fully integrated forensic data acquisition and analysis program which was developed by AccessData. FTK provides features like full-text indexing image files without extracting them to a hard disk as well as include a file viewer to preview the files.

- FTK also has an imaging component for collecting data from CDs and DVDs with commonly supported file systems. FTK Imager is an imaging tool to preview data and assess the potential evidence on a machine.
- A forensic image of the data, duplication on the machine using the tool, so that modification of original data does not take place. FTK Imager reads image files with ICS and SafeBack as well as uncompressed images created with Ghost.
- FTK Imager will read or write image files in different formats such as Encase, dd Raw, SMART, and FTK. The major advantage is that even if the image files are created by another organization in any format, they can be read easily.
- FTK Imager has an easy-to-use interface wherein once the evidence file is opened, the folder structure can be viewed in the Evidence tree located in the upper left lane.

b. SafeBack

- One of the earliest DOS-based tools developed by NTI for acquiring evidence sector by sector from a computer. It can boot from a floppy disk, make a duplicate image of everything on the hard disk, thereby preserving its integrity and analyzing evidence without it getting modified.
- Capable of replicating individual partitions or entire disks of any size virtually with the image files being transferred to SCSI tape units, etc. An audit trail of the software's operations is maintained through the product's CRC function which checks the integrity of the copies, its data, and timestamps.
- Despite being a DOS tool, it can copy DOS, Windows, and Unix disks onto Intel-compatible systems and the images can be stored as multiple files on CDs or any small capacity media. No compressions or translations take place during the creation of the image.

c. DriveSpy

- It is a DOS-based data acquisition tool that was developed by Digital Intelligence Forensic Solutions. Despite being DOS-based, it can acquire evidence from partitions using FAT, non-DOS, and hidden DOS partitions, that is, visible files to the file system, deleted files, exists in slack space, and unallocated space on the disk.
- Performs data acquisition from hard drives greater than 8.4 GB and floppy disks as well as other storage media. DriveSpy is also responsible for providing a built-in sector and cluster Hex Viewer to view the data, it also can create and restore compressed partition forensic images.

- A major advantage is its logging capabilities, such as logging each keystroke that was made, which are then written on a log file and can be logged into a report of procedures that were followed to acquire the evidence.

d. Mount Image Pro

- A tool developed by GetData Software Development that mounts and view forensic image files created by EnCase, Unix, and Linux DD images, SMART and ISO images of CDs and DVDs.
- When an image is mapped to a drive letter, data acquired can be explored through the image and use third-party tools.
- It can mount different types of forensic image files and does not need additional copies of software or dongles such as EnCase software to view evidence acquired from the image. It can save a considerable amount of money because image analyzer machines don't require the original software to acquire the evidence.
- EnCase image file can be opened without knowing the password despite being password protected.

e. DriveLook

- A free forensic search tool designed for indexing all of the text written to a hard disk or other media, was developed by Runtime software. Searched drives can be physical, logical, or remote drives, which can be connected using a serial cable or network connection using TCP/IP.
- It can also be used with image files created with Runtime's DiskExplorer or GetBackData, which helps search for words stored on a suspect machine. Once the words are indexed on the media and saved to a table, the search can be done through keywords or browsing the table to view the location of the stored words.

f. DiskExplorer

- A tool that helps browse the hard disk contents and was developed by Runtime software with two main versions, namely, DiskExplorer for NTFS and DiskExplorer for FAT.
- They are disk editors, which help browse NTFS and FAT file systems along with recovery of data stored on a disk as well as view the contents of a physical, logical drive or image files.
- When the information on the disk is being viewed, analysis of partition table, MFT, boot record, and index buffers can be done.
- DiskExplorer also involves search capabilities which will allow searching for text, viewing the files and their properties, identifying the cluster to which the file belongs. Sectors of the disk can be edited and lost or deleted files can be recovered using this tool.

- It can also create an image file to duplicate the data on a hard drive. Once the image is created it can be preserved on the disk for further analysis or can be used to restore data on another machine.

g. SnapBackDatArrest

- Snapback developed a suite of data duplication and forensic tools known as DatArrest, where data can be acquired using a program on a bootable floppy from a machine.
- Images also contain the deleted, encrypted files or those which are present in the slack space on the disk apart from the files that can be seen by the filesystem.
- CMOS settings used by the computer are also captured as a part of the image. Data can be acquired and images can be created to and from hard disks, removable media, and magnetic tapes with the help of the modules and utilities included in the project.

h. SCSIPAK

- Suite of tools developed by Vagon, which provides data recovery and conversion between Windows NT4 or 2000 and other systems such as DEC, ICL, and IBM Mainframe.
- SCSIPAK extends the abilities of the Windows tape drive to make the data readable.
- Data from tapes or optical discs can be downloaded and written up to seven drives at the same time. Thus, tapes can be copied, data can be transferred from Windows NT or 2000, or can also be transferred between disk, tape, or optical disc using SCSIPAK.

i. IBM DFSMSdss

- Data Set Services (DFSMSdss) is an IBM-developed utility that was designed for disaster recovery and data management.
- It was developed as a part of the Data Facility Storage Management Subsystem (DFSMS), DFSMdss can be used to move or copy data between various types of storage media so that storage on different servers can be managed.
- Permits backup, restore data and copy backups to another storage media irrespective of the type of media.

4.3.2 Hardware Tools

Tools for duplicating data can be used in a forensic lab or the field, wherein forensic images can be created which can be analyzed later for potential evidence. These tools act as portable forensic labs, which allow acquisition and analysis before the computer is removed from the crime scene. The majority of these tools store data on a hard disk within the

device, thus providing the ability to transfer image files from a device to another system in a forensic lab, and can then wipe the device's drive to make it sterile forensically.

a. ImageMASSter Solo-3 Forensic

- It is a hardware tool that is portable and hand-held device which can acquire data from the suspect's machine at a speed exceeding 4 GB/minute. It was developed by Intelligent Computer Solutions.
- Since the hard disks is directly connected to the machine using a drive-to-drive interface or external Firewire/USB interface, a duplicate copy of data can be created from one or two drives at the same time without letting the speed get reduced. Can acquire data from hard drives such as IDE, SATA and SCSI.

b. LinkMASSter-2 Forensic

- It is a hardware tool developed by Intelligent Computer Solutions where the device connects to a computer through a USB port or Firewire and create an image of any data on the machine.
- A software permits access and data acquisition using Firewire or USB ports, after booting the machine and connecting to the LinkMASSter.
- The write-block feature protects the data during acquisition on the original machine.

c. ImageMASSter 6007SAS

- It is a powerful tool for generating data images from the suspect machines and duplicating IDE, SAS, SATA, and IDE hard drives.
- Was developed by Intelligent Computer Solutions and can migrate the server data from SCSI to SAS/SATA. It can acquire data from multiple disks as well as store multiple images on a single hard drive.
- It is the only tool to support SAS (Serial Attach SCSI) hard drive and copies multiple drives at the same time with a faster speed.
- The system provides a window XP-based interface that allows copying data from Windows, Macintosh, and Unix file systems.

d. RoadMASSter-3

- It is a data acquisition and analysis tool developed by Intelligent Computer Solutions to create an image and also to analyze the data acquired from the suspect's hard drive.
- Can connect to an unopened computer using Firewire and USB ports. Can also connect directly to IDE, SATA, SAS, and SCSI hard drives.
- Capable of acquiring data from multiple drives to a single target drive which makes the acquisition faster. It analyzes the data quickly.

- Designed with a 15-inch color display inside its case which helps view data stored in the image file to enable it to determine if any evidence exists on the machine.

e. Disk Jockey IT

- It is a portable, hand-held hardware tool by Diskology and is the smallest write-blocking and disk copy device for computer forensics.
- Can be used as a write-blocking device for acquiring data using Firewire and USB connections to a suspect computer.
- Device can then be connected to a Windows or Macintosh system through write-protect mode to analyze the data without altering it.

4.3.3 Backing Up and Duplicating Data

Many tools can be used to backup data so the restoration of systems can be done in case of any virus or malicious software, failure of a hard disk, intrusion, or any other event which could lead to loss, corruption, or deletion of the data. During mass deployment of a system, images are made of systems. Example: Since mostly all the workstations will have similar OS and software configurations, hence making a single image of a system could be utilized to restore that image on others computers with a slight change in the system's name, IP address, etc. This restoration helps save time and money in setting machines that were being deployed in the network. Backups and Duplicate data minimize the impact of losing a system as a replacement system can be immediately deployed.

a. R-Drive Image

It is a data duplication tool developed by r-Tools technology and is designed for backup and duplication data, as well as creates a byte-by-byte data copy on hard drives, partitions, and logical disks. These files are stored on another hard disk, network drive, or storage media and restored as needed.

b. Save-N-Sync

- Save-N-Sync tool was designed by Peer software to synchronize the data stored in a directory on a laptop or system with the data stored on another location like a network server. Data can be backed up on a location or can synchronize the changes on either the source or target folder to be reflected in both the directories which will help for restoration in case any problem occurs.
- A single directory can be chosen to synchronize with another directory in the standard version of the tool, while the corporate version permits 15 directories for synchronization.

c. QuickCopy

- It is a tape duplication system developed by Shaffstall Corporation which is designed to make tape-by-tape backup copies. When the data on the server or any other computer is backed up on magnetic tape, copies are required for offsite storage.
- Whenever a nightly backup is done, QuickCopy duplicates this data, thereby providing a backup of the backup tape.
- Duplicates of tapes can be used for the analysis of potential evidence. QuickCopy checks the data byte-for-byte along with the capability to copy a single tape to an image file which can be stored on a hard disk.

4.3.4Acquiring Data in Linux

Apart from data recovery and forensic tools run on Linux, UNIX, and other Posix OS, specific commands can be used on OS to copy data on a machine and transfer it across a network. Other versions of similar tools can be used for Windows OS. Commands are:

i. dd: Convert and Copy Command

- dd is used in Linux to convert and copy the data, along with a version of it that runs on windows. Allows copying a hard disk to another disk drive, magnetic tape, or vice-versa. Data is transferred byte-for-byte, thus generating an exact mirror image.

Syntax: dd <options>

- The command can be used in various ways,for example: to copy contents of a disk to another, use the command with if (input file) and of (output file) options:

dd if=/dev/hda of=/dev/hdy

Example: To backup the disk into an image on the hard disk,

dd if=/dev/hda of=/path/to/image

Option	Description
if=inputfile	Specifies where to input data from (file or device)
of=outputfile	Specifies where to output data (file or device)
ibs=bytes	Number of bytes to read at a time
obs=bytes	Number of bytes to write at a time
bs=bytes	Several bytes to read and write. This is used instead of ibs and obs, and it specifies the same number of bytes to use for both input and output.
bs=bytes	Number of bytes to convert at a time

skip=blocks	Specifies to skip blocks in the input file before copying
seek=blocks	Specifies to skip blocks in the output file before copying
count=blocks	Copy blocks from the input file, instead of everything at the end of the file
conv=conversion	<p>Specifies to convert the input file before copying to an output file. Conversion methods include</p> <ul style="list-style-type: none"> ■ ascii, which converts EBCDIC to ASCII ■ ebcdic, which converts ASCII to EBCDIC ■ ibm, which converts ASCII to alternate EBCDIC ■ block, which replaces the input newline with padding of spaces to fit the size of cbs ■ unblock, which replaces trailing space characters in datasets of size cbs with newline characters ■ lcase, which converts uppercase characters to lowercase ■ ucase, which converts lowercase characters to uppercase ■ swab, which swaps every pair of input bytes ■ noerror, which ignores read errors ■ notrunc, which specifies not to truncate the output file ■ sync, which pads every input block to the size of ibs with null bytes if its shorter than the specified size

Table 4.1: dd options

- MBR can be extracted from a disk using the dd command. Since MBR and partition table are present in the first bytes of the disk, by specifying first few data bytes from the disk, a backup of data can be acquired. Example: To acquire file from the disk, use the command:

```
dd if=/dev/hda of=/path/to/img count=1 bs=512
```

- To restore data to the disk, incase of any problem, the input and output value needs to be interchanged:

```
dd if=/path/to/img of=/dev/hda
```

ii. Netcat: Transfer data and for other functions

- Netcat tool is available on all Posix OS such as UNIX and Linux, which uses Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) to transfer data across a network. A Netcat version can be used on systems running Windows 9x, NT, ME, 2000, and XP OS.

- A partition image can be created and transferred files between remote computers or send to a machine. It supports port scanning and the ability to connect through Telnet.
- Netcat runs in server mode on one machine and client on another for communication between them. Server mode Netcat listens on a port specified and transmits data to the client connected to that port number.
- Following syntax is used for Netcat to run from the server: `nc -l <-options><port number>`

where the port number is the port on which the server should listen and that clients connect to:

`nc -l <-options><port number>`

- Following syntax would be used by the client:

`nc -l <-options><server ip-address><port number>`

Netcat has additional options which can be used for listening on a network and connecting to computers.

Option	Description
-d	Background mode. Detach from console
-e program	Inbound program to execute
-g	Source routing flags
-h	Help
-i seconds	Delay interval for lines sent, ports scanned
-l	Listen for inbound connections
-n	Numeric only IP addresses (no DNS)
-o	Hex dump of traffic to a file
-p	Local TCP/IP port to listen to. Used with -l in server mode
-r	Random local and remote ports
-s addr	Local source address
-t	Answer TELNET negotiation
-u	Use UDP to listen on a port. Used with -l in server mode
-v	Verbose. -v-v will put it into an ultra-verbose mode
-w seconds	Connects and final net reads timeouts before Netcat will automatically quit
-z	No, I/O mode. Used for scanning ports

Table 4.2: Netcat Options

- Netcat can be used with other tools to generate a compressed image of the disk and permit others to download a file. In the below-mentioned example, the dd command creates an image of a disk, with gzip to compress it. Netcat listens to the port number, making the file available:

```
Dd if=/dev/hdb | gzip-9 | nc -l 4321
```

4.4 LET US SUMUP

This unit helps gain an understanding of the various factors that need to be considered for performing digital forensics on Windows OS, the tools needed for performing it and techniques required for evidence acquisition and data replication.

4.5 LIST OF REFERENCES

[1] The official CHFI Exam 312-49 Study Guide by Dave Kleiman, Syngress Publication, 2007.

4.6 BIBLIOGRAPHY

[1] EC-Council CHFIv10 Study Guide, EC-Council, 2018

4.7 UNIT END EXERCISES

1. _____ is a tape duplication system developed by Shaffstall Corporation which is designed to make tape-by-tape backup copies.
 - a. SCSI
 - b. SCSIPAK
 - c. ScanCopy
 - d. QuickCopy
2. _____ are disk editors, which help browse NTFS and FAT file systems along with recovery of data stored on a disk as well as view the contents of a physical, logical drive or image files.
 - a. DExplorer
 - b. DiskExplorer
 - c. DiskScan
 - d. PCScan
3. _____ is a powerful tool for generating data images from the suspect machines and duplicating IDE, SAS, SATA, and IDE hard drives.
 - a. ScanCopy
 - b. ImageMASS
 - c. QuickCopy
 - d. ImageMASSter 6007SAS

4. The space area between the end of the file and the last cluster is known as _____.

- a. Space Gap
- b. Gap
- c. Slack Space
- d. Slack data

5. _____ is used in Linux to convert and copy the data, along with a version of it that runs on windows.

- a. dsd
- b. dd
- c. sdd
- d. dss

6. _____ tool is available on all Posix OS such as UNIX and Linux, which uses Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) to transfer data across a network.

- a. Disk Explorer
- b. Quick Copy
- c. Net cat
- d. Image MASS

7. _____ is a set of protocol which provide file and printer access between clients and remote servers on NetWare networks. NCP runs over IPX or IP.

- a. Common Internet File System
- b. Network File System
- c. NetWare Core Protocol
- d. Server Message Block



RECOVERY OF DELETED FILES AND PARTITIONS, USING ACCESS DATA FTK AND ENCASE FOR FORENSIC INVESTIGATION

Unit Structure

- 5.0 Objectives
- 5.1 Introduction
- 5.2 Recovery of deleted files and partitions
 - 5.2.1 Recycle bin
 - 5.2.2 Deleted File Recovery tools
 - 5.2.3 Recover the deleted files using Recuva
 - 5.2.4 Recovering deleted partitions
 - 5.2.5 Methods and tools to recover the deleted partitions
- 5.3 Using Access data FTK and EnCase for Investigation
 - 5.3.1 Forensic Tool Kit(FTK)
 - 5.3.2 Investigation using FTK
 - 5.3.3 En Case
 - 5.3.4 Investigation using EnCase
- 5.4 Let us Sum Up
- 5.5 List of References
- 5.6 Bibliography
- 5.7 Unit End Exercises

5.0 OBJECTIVES

After studying this unit, you will be able to know:

- Recycle bin
- What are the deleted files
- How to recover the deleted file

5.1 INTRODUCTION

Investigator performs digital forensics by collecting and correlating and analyzing evidence to know the process and motive behind the crime and to identify criminal, but hidden or deleted data are major concern before forensic investigator, various tools and techniques will help the digital forensic investigator in every phase of the digital forensic process. Hence Computer forensic investigators should know those tools and techniques, their functions.

Recovery of Deleted Files and
Partitions, Using Access Data
Ftk and Encase for Forensic
Investigation

5.2 RECOVERY OF DELETED FILES AND PARTITIONS

5.2.1 Recycle bin

Recycle bin is a temporary storage place on windows desktop for deleted files where those deleted files are temporarily stored if not deleted permanently. Recycle bin will not store deleted Files from removable storage media like floppy disk, USB pen drive, or network drive, and even if a deleted file is too large will not get a place in recycle bin.

Users can delete a file from a hard disk in the Windows operating system by right-clicking on that file and selecting the delete option to send a file to recycle bin. Even users can restore an individual deleted file or all deleted files by selecting the restore option.

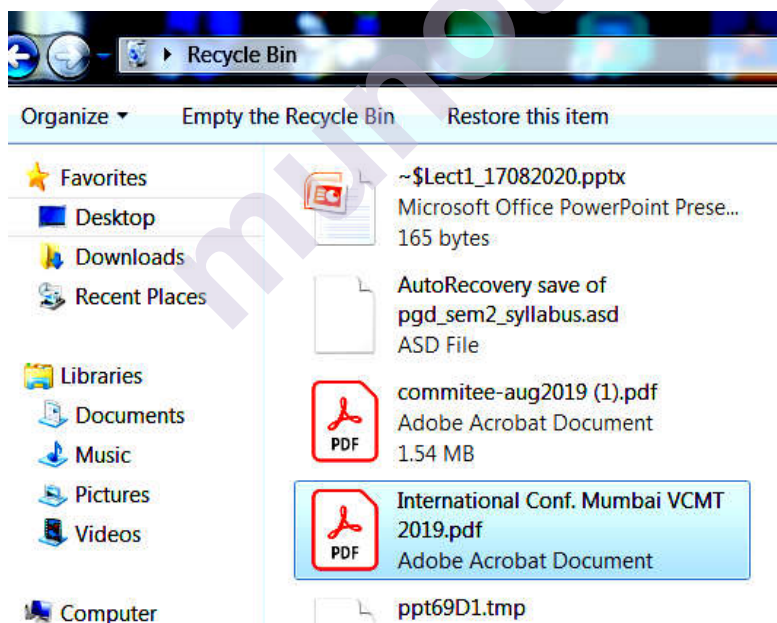


Table shows Location and Storage size Limit of Recycle bin

File System	Operating System	Location on drive	Size Limit
FAT	Win 98 and prior	Drive:\RECYCLED	3.99 GB
NTFS	Windows 2000/Win XP	Drive:\RECYCLER	3.99 GB
NTFS	Windows Vista and later	Drive:\$Recycle_Bin	No Limit

When user deletes a file from computer actually it won't delete it physically only the entries of those files are deleted from MFT (Master file table) but file remains there on hard disk and OS replace first letter with E5h hex byte code to indicate that the file has been deleted

5.2.2 Deleted File Recovery tools:

Various Tools are designed to recover/restore deleted or corrupted data/files from hard disks, USB pen drives, Memory cards, and other storage devices.

Tools available for recover deleted data/files:

- Recover My Files : (www.recovermyfiles.com)
 - It recovers deleted files from a hard drive, memory card, USB, ZIP, floppy disk.
 - It also recovers deleted files emptied from the windows recycle bin,
 - It recovers deleted files from a formatted or corrupted hard disk.
 - It also recovers documents, photos, videos, and audio files.
- EaseUS data recovery wizards :
- Diskdigger :
- Handy recovery
- Quick recovery
- Stellar Phonix Windows Data Recovery
- Total Recall
- Advanced Disk recovery
- Window data recovery software
- R-Studio

- Orion File Recovery Software
- Data Rescue PC
- Smart Undelete
- DDR Professional Recovery Software
- Data Recovery Pro
- Undelete Plus
- File Scavenger
- VirtualLab
- Active UNDELETE
- WinUndelete
- R-UnDelete
- Recover4all Professional
- Recuva
- Active File Recovery
- Disk Drill
- PhotoRec

5.2.3 Recovering the deleted files using Recuva

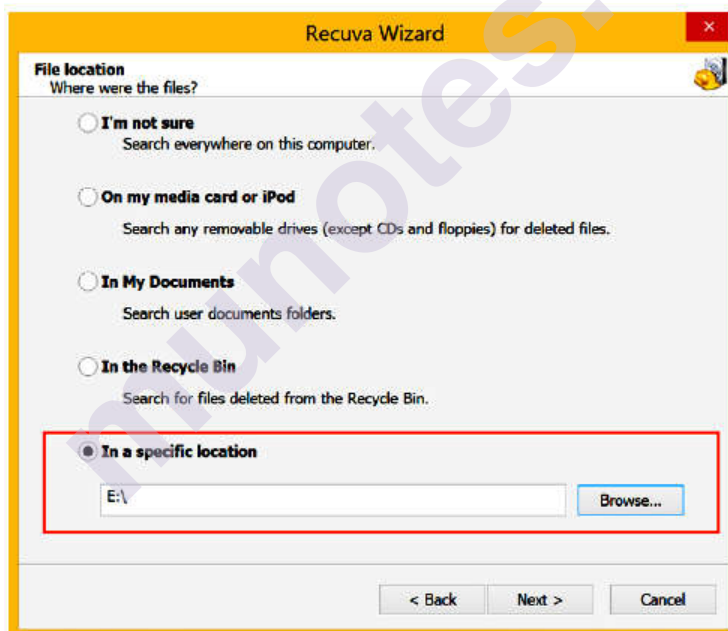
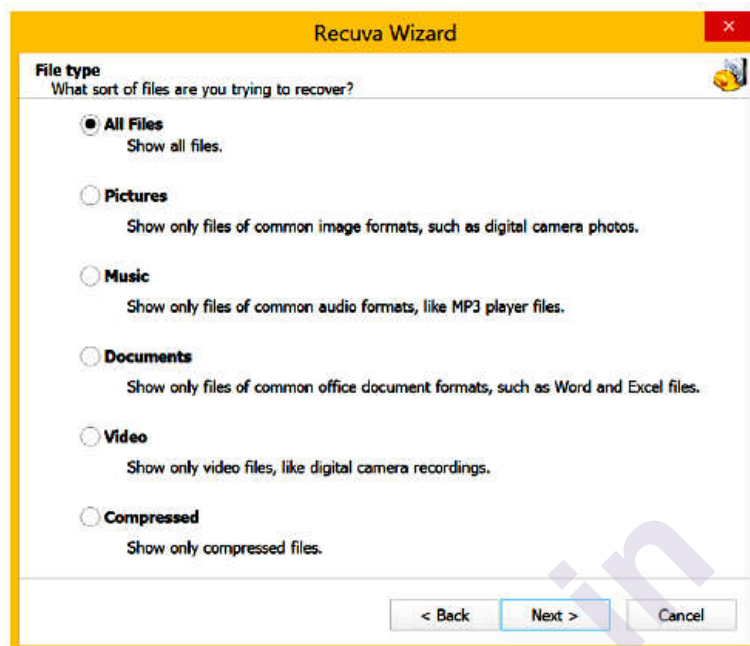
Recuva is one of the tools used for file recovery. It can recover deleted files from a hard disk, USB pen drive, memory card, etc. (<http://www.ccleaner.com/recuva>). Its feature includes

- Superior file recovery
- Recovery from the damaged disks
- Deep scan for buried files
- Securely deleted files

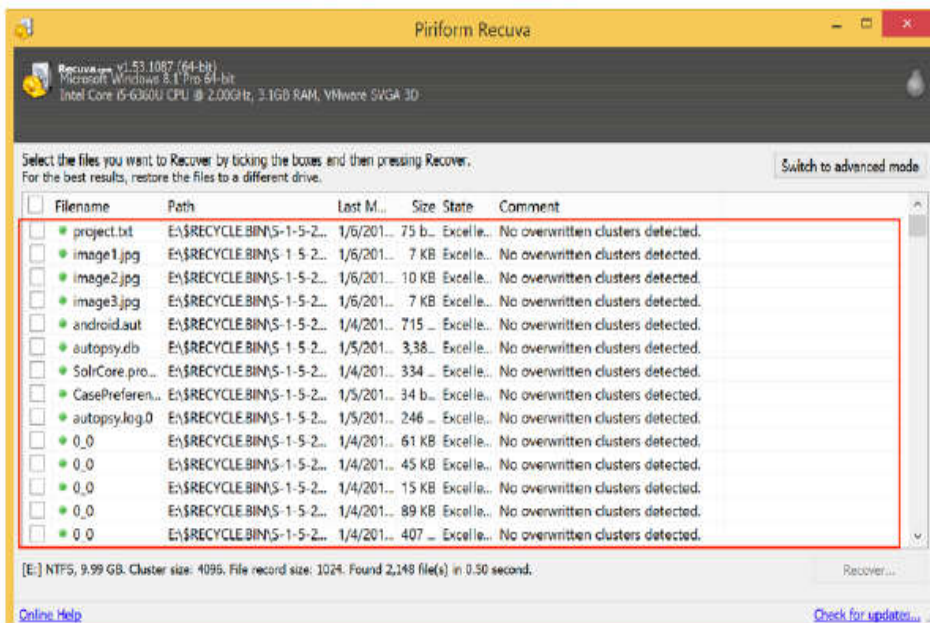
Steps to recover deleted files using Recuva:

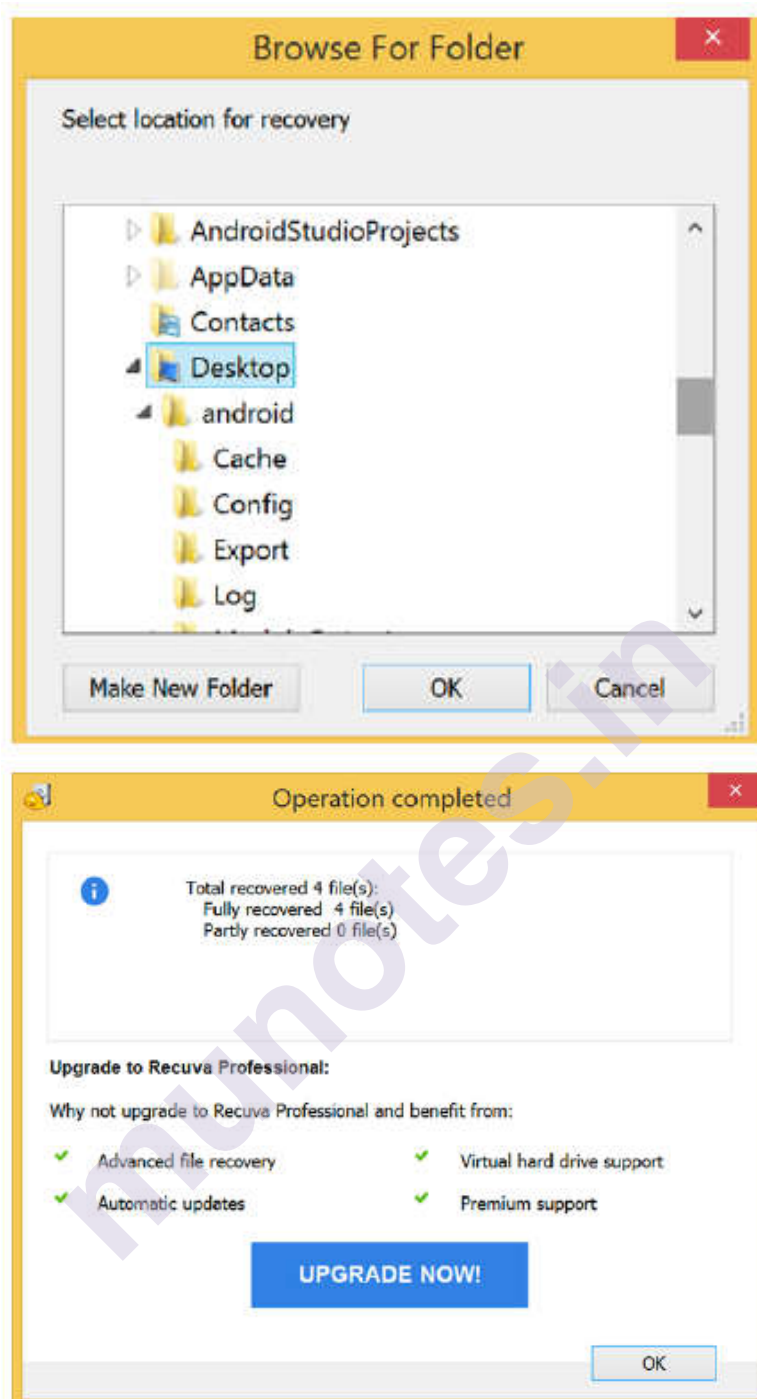
1. First Start the tool
2. Then select which type of files you want to recover (All files)
3. Now specify the location of the source drive to recover files. (E:)
4. Now select the list of files you want to recover

5. Select destination folder/drive where you want to store recover files (Desktop)



Recovery of Deleted Files and Partitions, Using Access Data Ftk and Encase for Forensic Investigation





5.2.4 Recovering the Deleted Partitions

Partitions are created by logically dividing the hard disk into volumes (Drive) and those volumes/drives are identified by letters like C or D or E etc. Those logical drives can be formatted separately and each drive can use a different file system like NTFS or FAT etc

When partitions are deleted knowingly or accidentally, all data will be lost. The system does not delete anything but erases the parameters which define partition set up size and location.

By using software that can reestablish those parameters can recover deleted partitions. Deleting primary partitions results in empty space referred to as unallocated disk space and deleting logical partitions within extended partition results in empty space referred to as free space.

An automated task performed by **partition recovery tools** to locate and recover data

- By allowing a user to select another partition after determining the error on disk and then making that partition active.
- By attempting to reconstruct the partition table entry after scanning the disk for a partition boot sector or damaged partition information.
- By attempting to reconstruct the partition table entry after scanning the disk for a partition boot sector or data from deleted partition information.

5.2.5 Methods and tools to recover deleted partitions:

Method one:

- Restart the systems with windows install DVD in the system
- Select the key listed on the screen to go to BIOS
- Select the menu name boot priority or boot order to set DVD as the first boot device then restart the system and start the installation process
- Then while installation select repair instead of install
- And type exboot on DOS screen
- Restart the system to check whether the deleted partition is restored.

Method two:

- Remove the HARD DRIVE after shutting down the system
- Install hard drive as slave on another system
- Now attempt to recover deleted partition

Method three:

- By using third party partition recovery software to recover the drive
- Follow instructions to recover partition after running the partition recovery program

Tools to recover partitions:

- Active Partition for windows
 - Allows recovering deleted and damaged logical drives and partitions within Windows, WinPE, Linux environments.
 - Will detect deleted but non-formatted partitions.
 - Allows fixing damaged Partition table, Master Boot Record (MBR), GUID partition table.
 - Can restore data from raw, compressed, and VMWare Disk image.
 - Will create disk image - backup for data recovery.
 - Can trace reformatted and damaged partitions.
 - Will recovers volumes lost due to accidental disk formatting
- Acronics Recovery Expert
- Power data recovery
- EaseUS Partition recovery
- Disk Internals partition recovery
- GetDataBack
- Advanced Disk Recovery
- NTFS Partition data recovery

5.3 USING ACCESS DATA FTK AND ENCASE FOR INVESTIGATION

5.3.1 Forensic Tool Kit (FTK)

- Forensic Tool Kit (FTK) is a commercial software suite from Access Data.
- It is a Complete Computer Forensics Solution.
- It Comes with FTK Imager used for imaging and image analysis and also to recover the file.
- It can perform Email Analysis, File Decryption, Data Carving, and Data Visualization.
- It has features such as registry viewer, in-depth easy to read logging, standalone disk imager.
- Can generate the report in different types of format.

Access Data's FTK Imager is a Windows software platform that performs a variety of Imaging tasks, including acquiring the running memory of a system.

Recovery of Deleted Files and Partitions, Using Access Data Ftk and Encase for Forensic Investigation

The software can be downloaded at www.accessdata.com/product-download

5.3.2 Investigation using FTK

Creating New Case:

Following steps must be completed to start a new case

1. Enter basic case information.
2. Check what you want to be included in the case log.
3. Check the processes that you want to run on the evidence.
4. Select the criteria for adding evidence to the case.
5. Select the criteria for creating the index.
6. Add the evidence.
7. Review your case selections.
8. Complete the wizard to launch the processing of evidence.

Click on **File** then Select **New Case** and Specify case name, case number, name of the Investigator name and select case path to store evidence then click on Next button.

Note: Case folder based on case name and case path field.

New Case

AccessData's
Forensic Toolkit®-FTK™
The Complete Analysis Tool

Wizard for Creating a New Case

Investigator Name:

Case Information

Case Number:

Case Name:

Case Path:

Case Folder:

Case Description:

The next screen will appear to enter information about Examiner like Examiner Name, Agency Name, Address, Phone No, Email Id, etc.

The next Screen is of **Case Log option** Form for selecting events FTK to log for the current case such as Bookmarking items, searches and error messages for each case. The case log file name ftk.log will get created automatically; this log file can be used as a part of the report.

Case Log Options

The case log is a text file named FTKlog in the case folder. It gets created automatically by FTK and contains a record of events that occur during the course of the case. You can choose which type of events you would like to be logged.

You can also add your own comments to the log file at any time by selecting "Add Case Log Entry..." under the "Tools" menu item, and you can view the log file by selecting "View Case Log" under the "Tools" menu item.

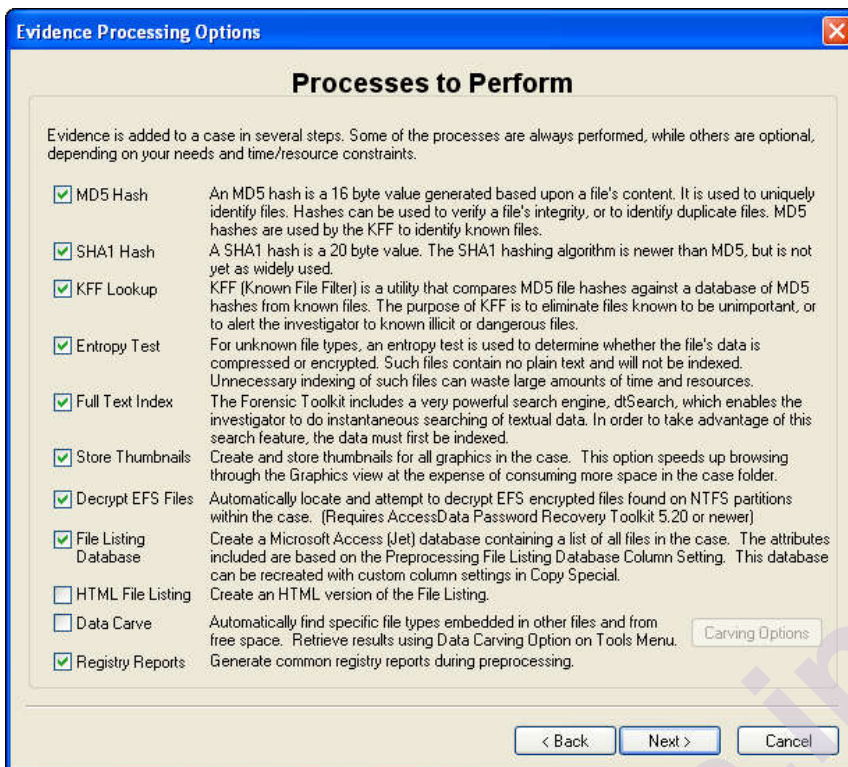
Events to go in the Case Log

<input checked="" type="checkbox"/> Case and evidence events	Events related to the addition and processing of file items when evidence is added or when using Analysis Tools later in the case.
<input checked="" type="checkbox"/> Error messages	Events related to any error conditions encountered during the case.
<input checked="" type="checkbox"/> Bookmarking events	Events related to the addition and modification of bookmarks.
<input checked="" type="checkbox"/> Searching events	Events related to searching. All search queries and resulting hit counts will be recorded.
<input checked="" type="checkbox"/> Data carving / Internet searches	Events related to special data carving or internet keyword searches that are performed during the case.
<input checked="" type="checkbox"/> Other events	Other events not related to the above, such as copying, viewing, and ignoring files.

< Back Next > Cancel

Select what event you wanted in the case log and Click on the **Next** button.

The next **Evidence processing Options** form will appear allowing you to which process to perform on evidence like full index, data carving, hashing (MD5, SHA1), etc. for example for a large image file if we don't want to create an index which will take more time then don't select Full-text index option.



Recovery of Deleted Files and Partitions, Using Access Data Ftk and Encase for Forensic Investigation

Process	Description
MD5 Hash	<p>Creates a digital fingerprint based on the contents of the file. This fingerprint can be used to verify file integrity and to identify duplicate files.</p> <p>For more information about MD5 hashes, see "Message Digest 5" on page 344.</p>
Registry Reports	<p>Generates common registry reports.</p> <p>For more information about Registry Report Summaries, see "Creating Registry Summary Reports" on page 208.</p>
SHA-1 Hash	<p>Creates a digital fingerprint based on the contents of the file. This fingerprint can be used to verify file integrity and to identify duplicate files.</p> <p>This is the only process not checked by default. If you want FTK to create SHA-1 hashes, you must check the box.</p> <p>For more information about SHA-1 hashes, see "Secure Hash Algorithm" on page 344.</p>
Store Thumbnails	<p>Creates and stores thumbnails for all graphics in the case.</p> <p>This process speeds up the browsing of graphics in the Graphics window.</p> <p>Each thumbnail is about 4 KB per graphic file.</p>

Process	Description
Data Carve	Carves data immediately after pre-processing. Select Carving Options and then select the file types you want to carve immediately. For more information on Data Carving, see "Data Carving" on page 181.
Decrypt EFS Files	Automatically locates and attempts to decrypt EFS encrypted files found on NTFS partitions with the case (requires Password Recovery Toolkit 5.20 or later). For more information on EFS, see "Decrypting EFS" on page 217.
Entropy Test	Determines if the data in unknown file types is compressed or encrypted. The compressed and encrypted files identified in the entropy test are not indexed.
File Listing Database	Creates a Microsoft Access (Jet) database containing a list of all files in the case. The attributes included are based on the Default File List Column Setting. This database can be recreated with custom column setting in Copy, and then Special.
Full Text Index	Indexes all keyboard-related characters in the case evidence. This process is the most time-consuming step in starting a new case. However, the index is required for data carving and Internet keyword searches. It also makes searching much more efficient. For more information about indexing, including disk space requirements, see "Conducting an Indexed Search" on page 154.
HTML File Listing	Creates an HTML version of the File Listing database.
KFF Lookup	Using a database of hashes from known files, this option eliminates ignorable files, checks for duplicate files, and alerts you to known illicit or dangerous files.

Select the process on the evidence and click on the **Next** button.

The next Screen is of **Refine case** will appear to exclude certain data from the case.

FTK contains five default exclusion templates:

- **Include All Items**
- **Optimal Settings**
- **Email Emphasis**
- **Text Emphasis**
- **Graphics Emphasis**

Select default template you wanted to use and click on the **Next** button.

The next screen for **Refine index** to specify data to index

Here select the type of file you want index and click on the **Next** button.

Add Evidence File:

This option will allow you to add evidence, remove evidence, edit evidence or refine evidence.

Add Evidence

Any number of evidence items can be added to the case. There are several types of evidence items:

- Acquired image of drive: Several formats supported; can be an image of a logical or physical drive
- Local drive: Can be a logical or physical drive
- Folder: Adds all files in the specified folder, including contents of subfolders
- Individual File: Adds a single file. NOTE: Disk image files should be added as acquired images.

The default refinement options, set previously, can be overridden independently for each evidence item, and additional types of refinements can also be made. These refinements can include the exclusion of date/size ranges, as well as specific folders. To make these further refinements, highlight an evidence item in the list and press Refine Evidence - Advanced...

Buttons: Add Evidence..., Edit Evidence..., Remove Evidence, Refine Evidence - Advanced...

Display Name	Source	Name/Num...	Type	Refined	Time Zone	Comment
Monster Image\ZIP-100-F...	C:\Program Fil...	001	FAT16	N	America/D...	

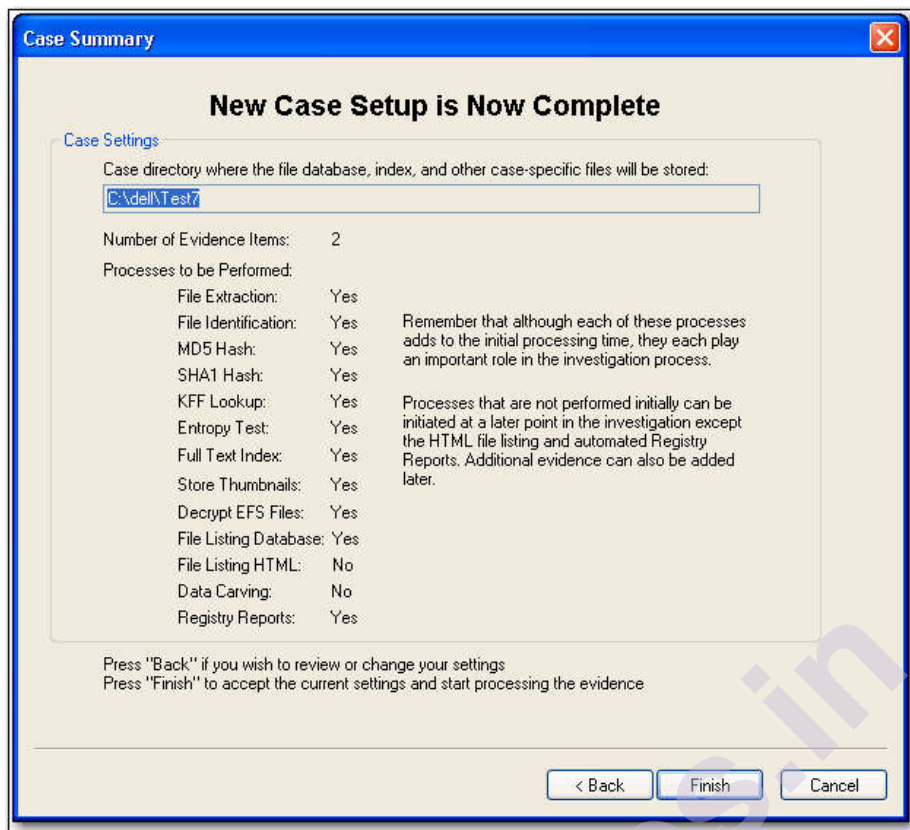
Buttons: < Back, Next >, Cancel

From add evidence case form click on **Add Evidence** and select one of the options.

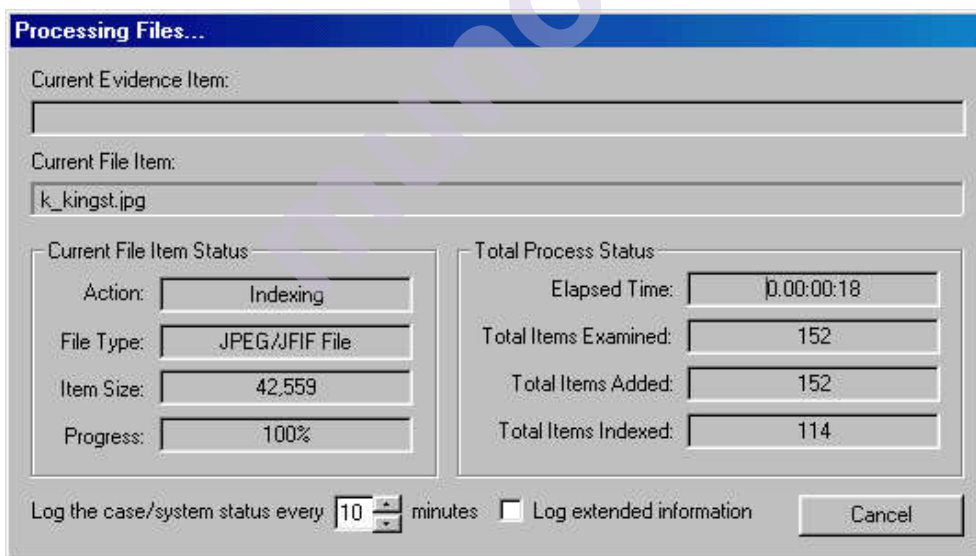
- **Acquired Image(s) of Drive:** Select this type to add a Forensic Image of a logical or physical drive.
- **Local Drive:** Select this to add a logical drive (C or D drive) or physical drive (full hard disk).
- **Contents of a Folder:** Select this type to add all files in a specific folder.
- **Individual File(s):** Select this to add a single file (.docx, .pdf, .jpg, and so on).

And after selecting the evidence option from the above list, click on the **Next** button.

The next **Case Summary** form will appear which allows you to review the evidence directory, number of evidence items, and evidence processes that you selected during the New Case Wizard.



After you click **Finish**, the Processing Files form appears and displays the status of the processes you selected in the wizard.



Search the Case:

Investigator can efficiently Search through suspected media by adding relevant keywords to determine if certain words, expressions or strings exists in files documents or emails or not.

There are two types of searching: Live search and index search.

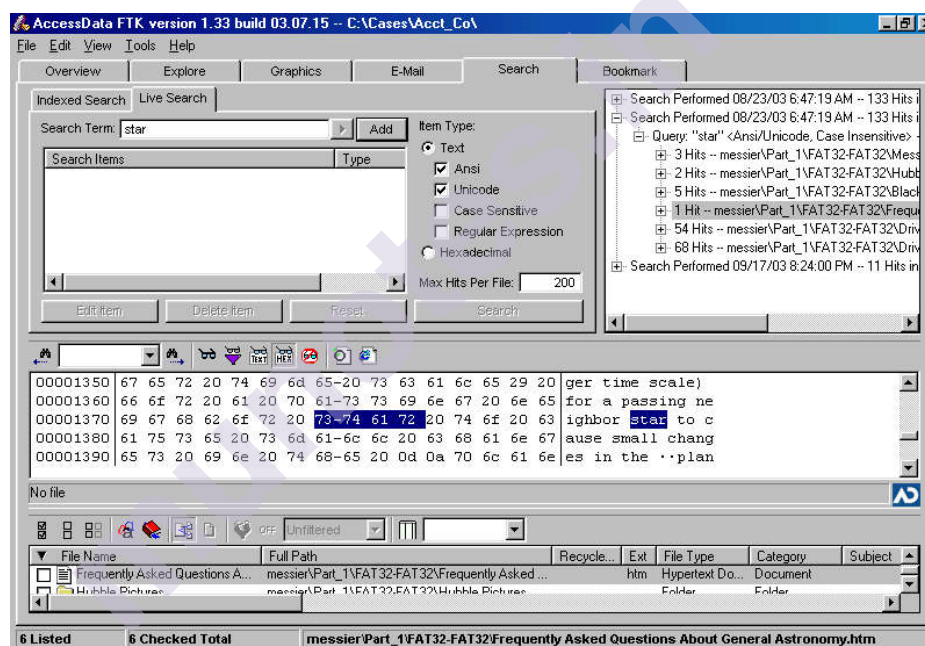
Index search uses index files to search. Live search is an alternative to index search if you don't have time for index searching. Live search is a time-consuming process because it will perform an item-by-item comparison with search terms.

To perform Live Search:

Click on **Live Search** in search window and enter the term in **Search Term Field** and in **Item Type** select either **Text** or **Hexadecimal**.

In **Item Type Text** you can select **ANSI**, **Unicode**, **Regular expression** or **Case Sensitive**.

You can add many Search term by clicking on **Add** button, ,modify using **Edit Item**, remove by using **Delete Item**, clear the search list by using **Reset** button



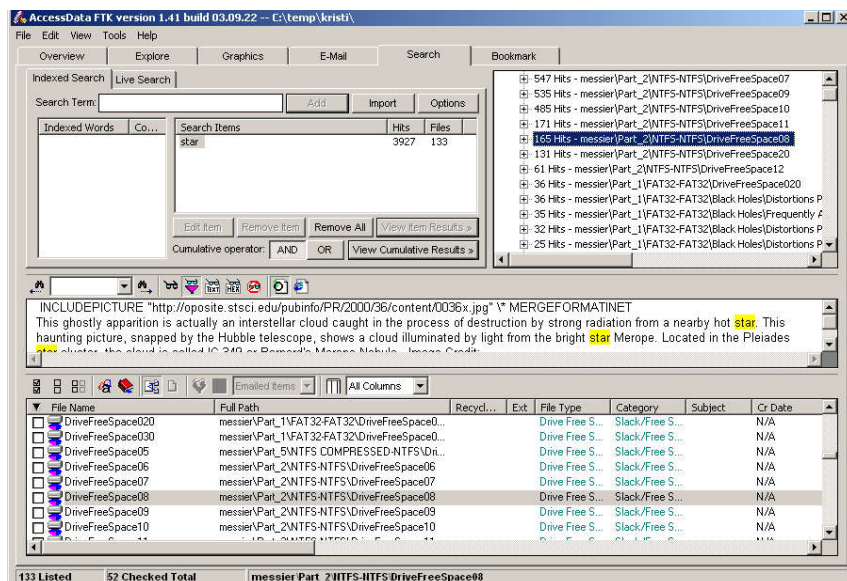
At last click on **Search** button, after finishing result will appear in search result list.

To perform Indexed Search:

Click on **Live Search** in the search window and enter the term in **Search Term** Field and **Item Type** select either **Text** or **Hexadecimal**.

In **Item Type**, **Text** select **ANSI**, **Unicode**, **Regular expression**, or **Case Sensitive**.

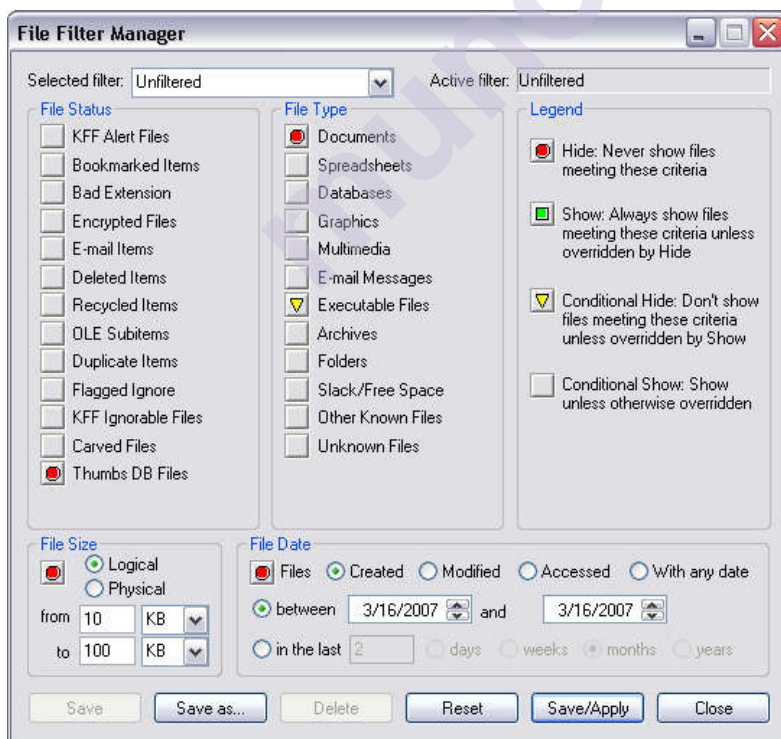
You can add many Search terms by clicking on **Add** button, modify using **Edit Item**, remove by using **Delete Item**, clear the search list by using the **Reset** button.



Using Filter:

To minimize the number of evidence items to examine, you can apply an existing filter or create a customized filter to exclude unwanted items. Forensic Toolkit (FTK) allows you to filter your case evidence by file status, type, size, and date parameters.

Select **View** and then **File Filter Manager** or Click on **File Filter Manager** icon, then **File Filter Manager** form appears has various options under **File Status**, **File Type**, and **Legend**.



File Status:

- E-mailed Items: Shows e-mail items such as e-mail messages, archive files, and attachments.
- Encrypted Files: This shows encrypted files that are possibly in all file types.
- Graphic Files: Only shows graphic files.
- KFF Alert Files: This Shows KFF alert files that are possibly in all file types.
- No Deleted: Hides deleted items.
- No Duplicates: Hides duplicate items.
- No Ignorable: Hides duplicate items, KFF ignorable files, and files that were flagged ignorable.
- No OLE: Hides items or pieces of information embedded in a file, such as text, graphics, or an entire file.
- Unfiltered: Displays all items in the case.

Legend:

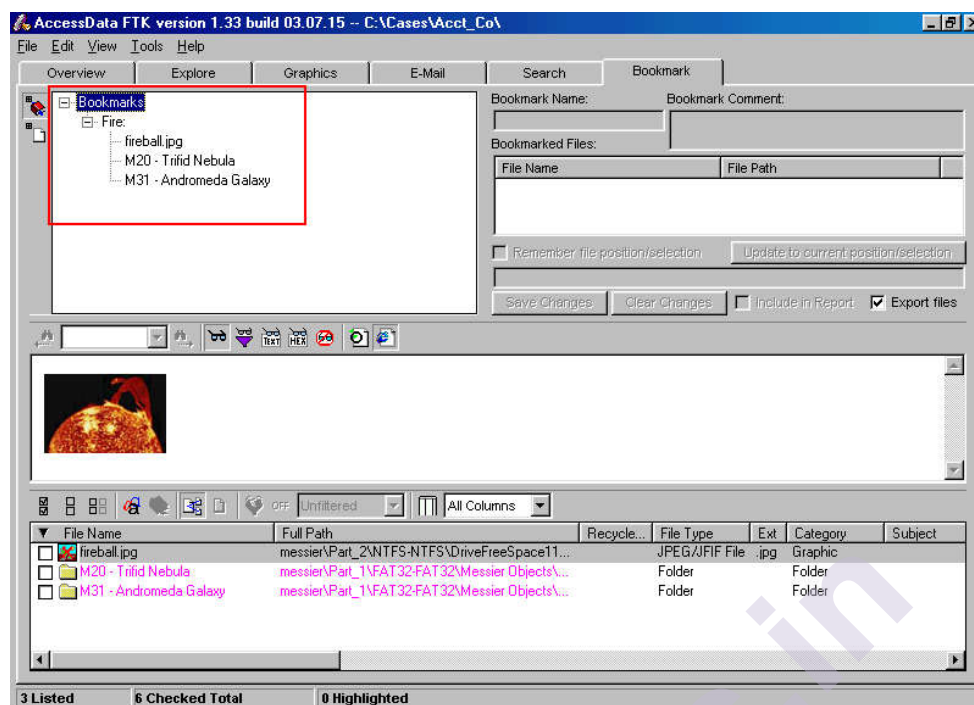
- Hide: Never shows files meeting selected criteria. If you click this icon in the Legend column, all file statuses and types are marked Hide.
- Show: Always shows files meeting selected criteria unless overridden by hiding. If you click this icon in the Legend column, all file statuses and types are marked, Show.
- Conditional Hide: Doesn't show files meeting selected criteria unless overridden by Show. If you click this icon in the Legend column, all file statuses and types are marked Conditional Hide.
- Conditional Show: Shows selected criteria unless otherwise overridden. If you click this icon in the Legend column, all file statuses and types are marked, Conditional Show.

To create a new filter, in the **Selected Filter** down down box enter the name of the new filter.

To modify the filter, in the **Selected Filter** drop-down box, select the filter to modify.

Creating Bookmark:

A bookmark helps to group related and similar files like bookmarks of graphics that contain similar image files.



Bookmarks can be created by selecting **Tools** then **Create Bookmarks** and then enter information about the bookmarks like bookmark name, Bookmark comment. Then specify the files to add to the bookmark. Select **the Include in Report** to include the bookmark and **Export** in the report

Reporting the case:

Reporting is the final stage of Forensic analysis phase. Reports are about the relevant information of investigation. The report can be generated in HTML or PDF or other formats.

To generate Reports

- Click on the **File** then **Report**

In Case Information form enters basic case information, such as the investigator and the organization that analyzed the case.

- Then select the information that will be used for the generation of the report such as Bookmarks. In the **Report Folder** field, set the path to output your report.
- Select a language to use on the report.
- Select the output file format. Click on **OK** to generate a final report.

5.3.3 EnCase

Features of EnCase:

- EnCase software is developed by 'Guidance Software'.
- It is a reliable and widely used tool.
- There are multiple packages in a single software.
- It supports all popular operating systems.
- Users can write a script for automated tasks.
- It can also perform file signature analysis.
- It has an MD5 database to crack encrypted files with passwords.
- It supports the Windows platform but it can analyze any operating system.
- The software goes through an entire file system, file registry, temporary files, and virtual memory.
- A specific term can be searched by using regular expressions.
- It makes many complicated jobs easy.
- It has a built-in imager with a software write blocker.
- It is always suggested to use a hardware write blocker as a precaution.
- EnCase provides another independent tool for live acquisition which is very useful in incident response.
- EnCase gives very good results for Disk imaging, Volume image, memory, logical files.

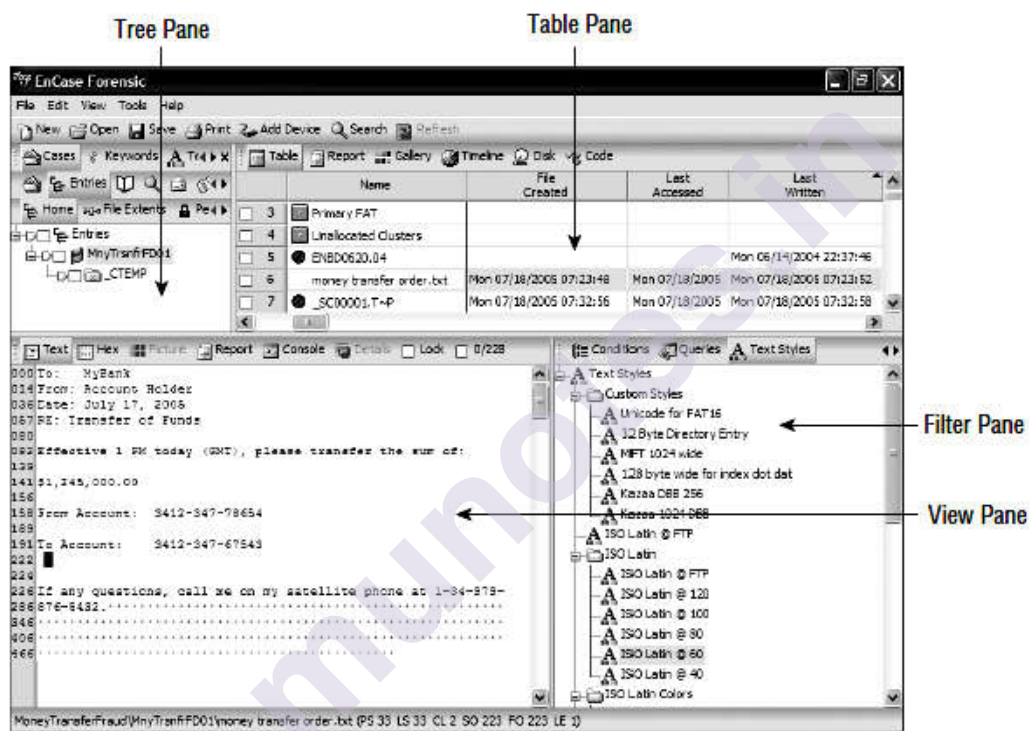
5.3.4 Investigation using Encase

Steps to Create a Case in EnCase:

1. Create case – Ensure that you have all relevant information – custodians, clients, case name, etc.
2. Change storage paths as appropriate. It set everything to go to a volume or folder dedicated to the case.
3. Save All.
4. Add evidence – E01, LEFs, loose files, etc. Each time you add evidence, you should consider rerunning several of the following steps.

1. Confirm disk geometry, sector count, partitions. You're checking to see if everything is accounted for. There may be hidden partitions.
5. Run Partition Finder if indicated
6. Run Recover Deleted Folders
7. Search case – hash and signature analysis. You will probably repeat this each time you add new evidence.
8. Search case – hash and signature analysis.

EnCase Forensic Main Pain is divided into four Panes from where various tabs are accessible.



Tree Pane: Cases, Home, Entries, Bookmarks, Search Hits, Email, History, Web Cache, Devices, Secure Storage, and Keywords tabs can be accessed from the Tree pane which is the top left pane in EnCase.

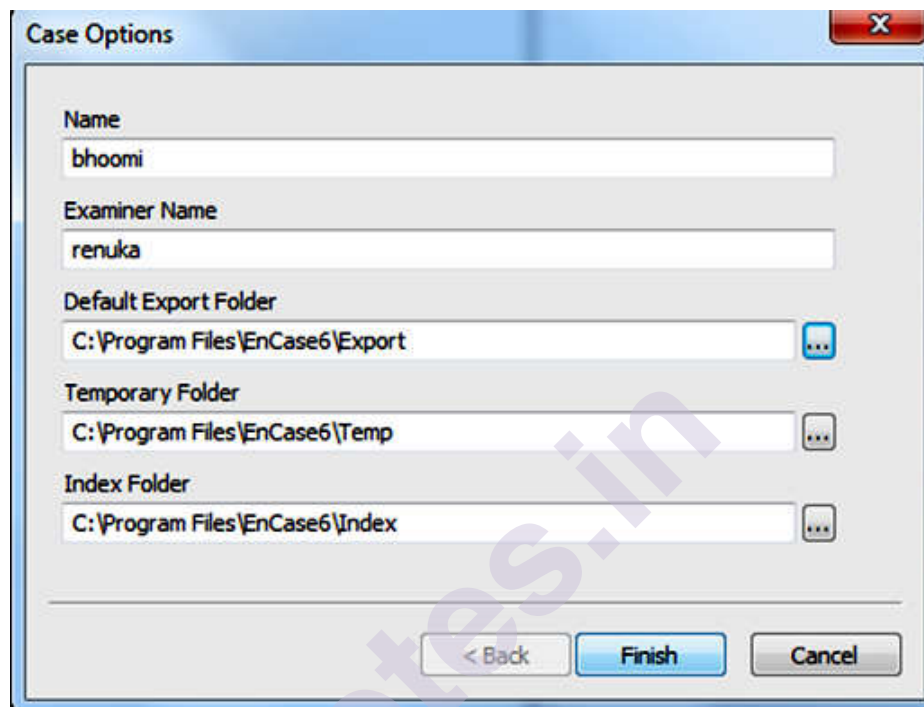
■ **Table Pane:** Table, Report, Gallery, Timeline, Disk, and Code tabs can be accessed from the Table pane which is the top-right pane in EnCase.

■ **View Pane:** Text, Hex, Picture, Report, Console, and Details tabs can be accessed from the View pane which is the bottom left pane in EnCase.

■ **Filter Pane:** EnScripts, Filters, Conditions, Queries, and Text Styles tabs can be accessed from the Filter pane which is the bottom right pane in EnCase.

Creating a New Case:

Click **File** then **New Case** and specify case name, examiner name, and folder locations to save the case under the designated folder -- not at the default location. Then click on the Finish button. Use the Save button frequently.

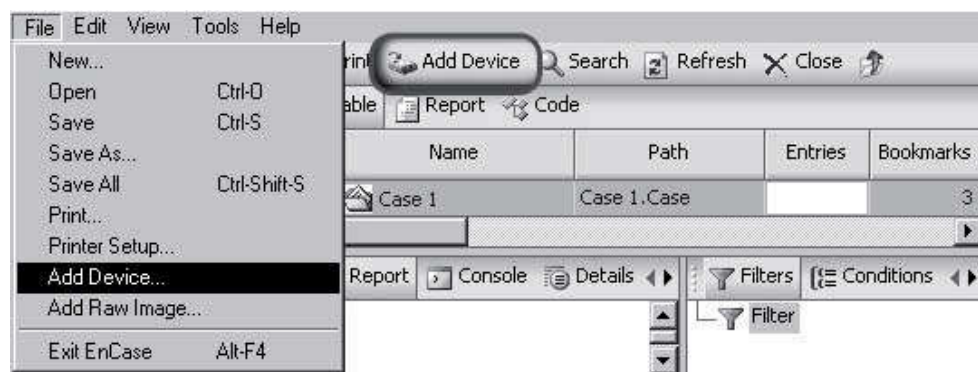


Adding Evidence Files

Evidence Files can be added to the case at any time via:

Add Device button on the button bar, or via selecting the **File** then **Add Device** option from the menu.

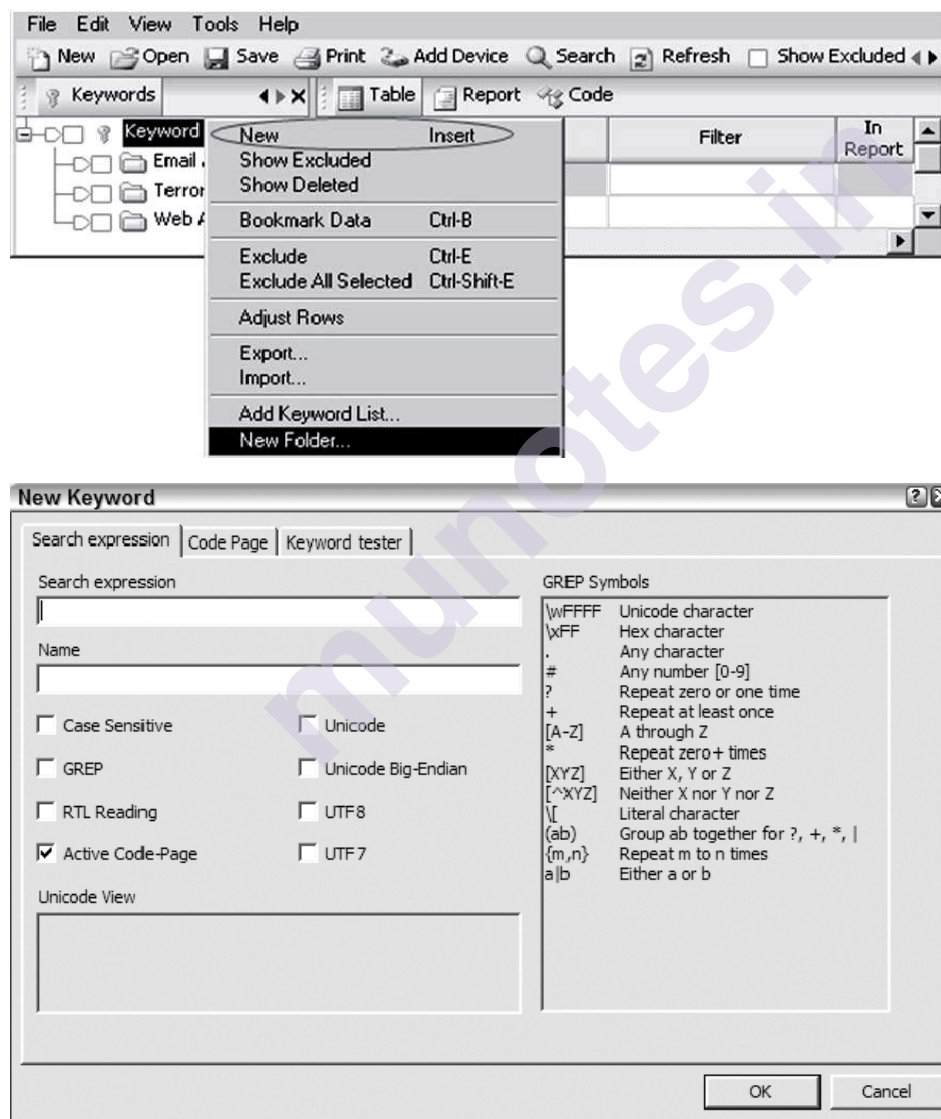
Navigate to the evidence folder and follow the rest of the dialog box prompts.



Keyword search:

Investigators can efficiently Search through suspected media by adding relevant keywords to determine if certain words, expressions, or strings exist in suspected media or not.

- Select **Keywords** from the **View** menu.
- Place a check in the box in front of Keywords, right-click Keywords and select **New Keyword**.
- Type the keyword you want to look for in the search expression box and select any other options that are relevant to the criteria of your search. Click on the **OK** button.

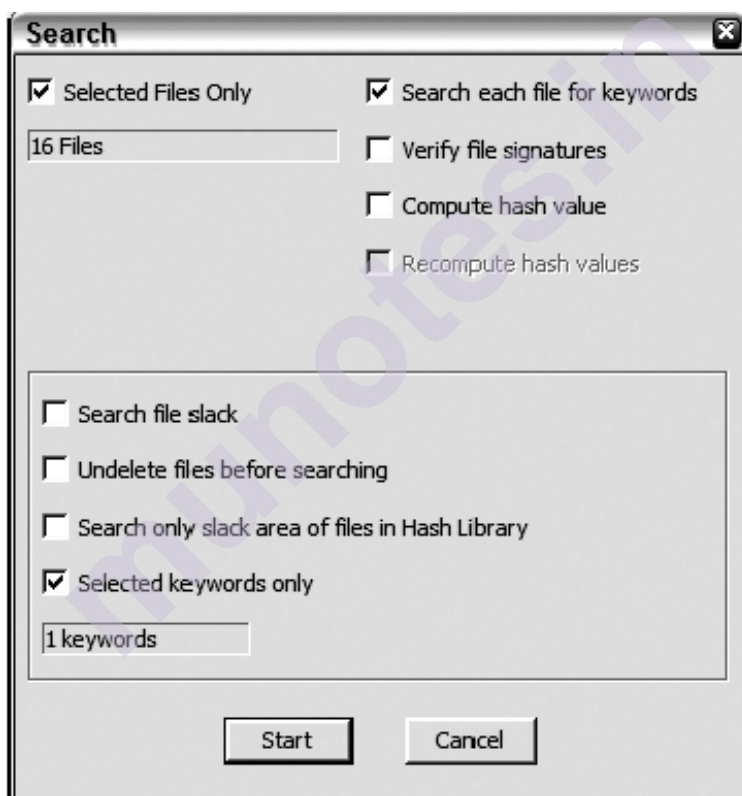


EnCase has the following searching options:

- Case sensitive: EnCase searches for keywords only in the exact case specified in the text box.

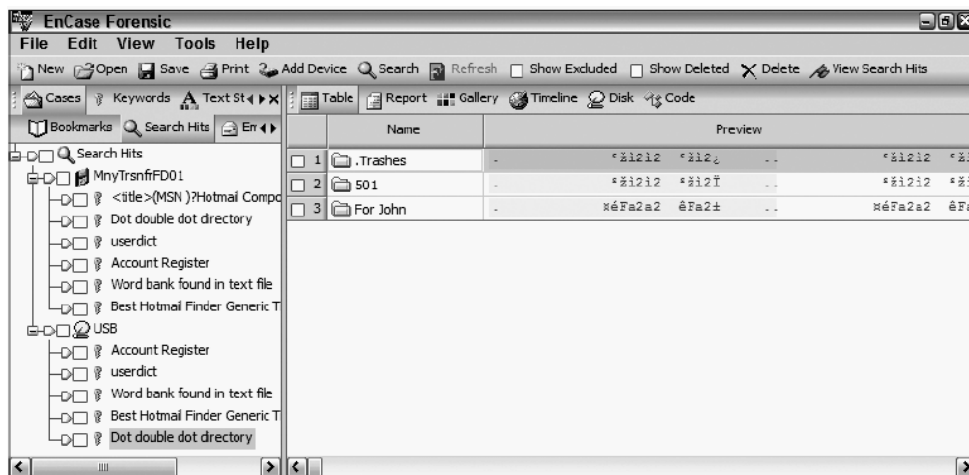
- GREP: Global Regular Expressions Post (GREP) search where the keyword is a regular expression.
- RTL reading: This is a keyword search in a right-to-left sequence for international language support.
- Active code page: This option allows an investigator to enter keywords in many different languages.
- Unicode: This enables investigators to search for keywords with international language characters.
- Big-endian Unicode: This enables investigators to search for keywords with international language characters.

To perform the search, Click on the **Search** button. Place check in front of **Search Each file for keywords** options and Click on the **Start** button.



Search hits are shown in group first by device and second by keywords.

Recovery of Deleted Files and Partitions, Using Access Data Ftk and Encase for Forensic Investigation



Bookmarks:

An investigator can highlight findings in a case by using Bookmark. Bookmark allows an investigator to include some extremely relevant items in the investigation report. Investigators can bookmark files, folders, or sections of files.

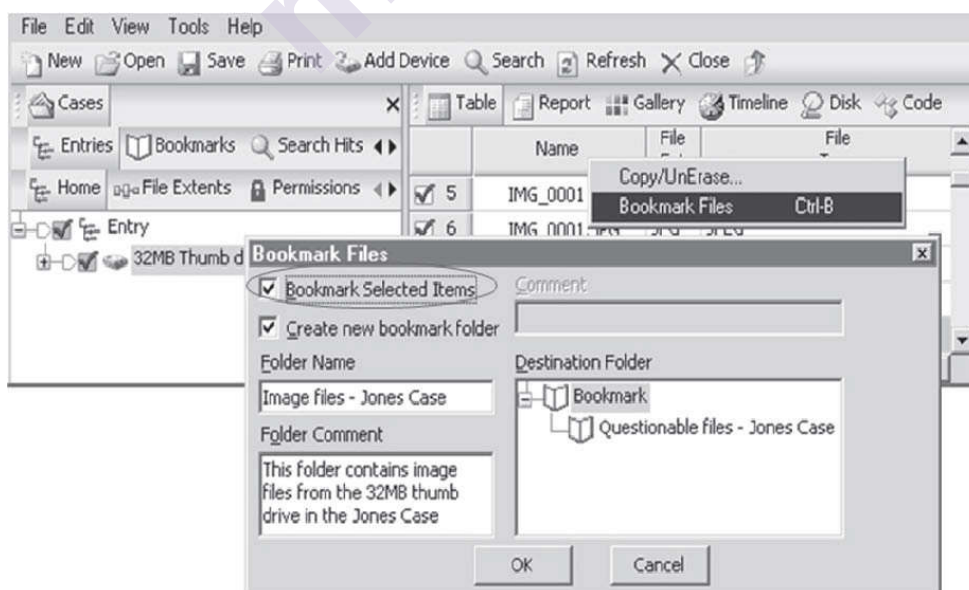
To view bookmark, click on **View** and then **Bookmark**,

Creating Bookmark folder

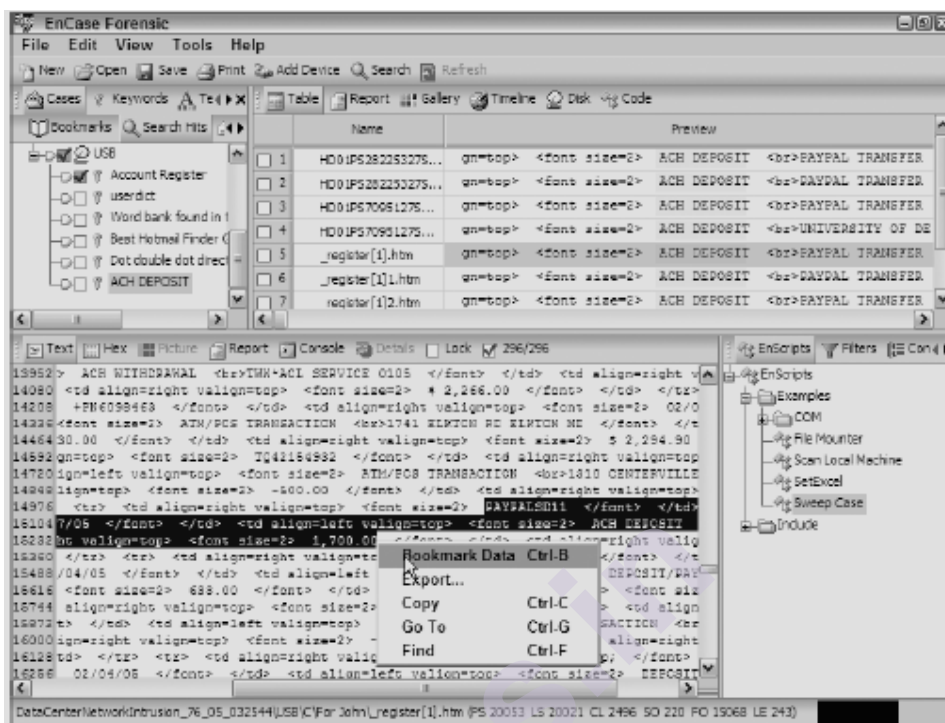
For creating a Bookmark folder, select **Create new bookmark folder** in the **Bookmark Files** window.

Adding a Bookmark to a case in EnCase

For adding a bookmark, right-click on any of the files and then select **Bookmark Files**.



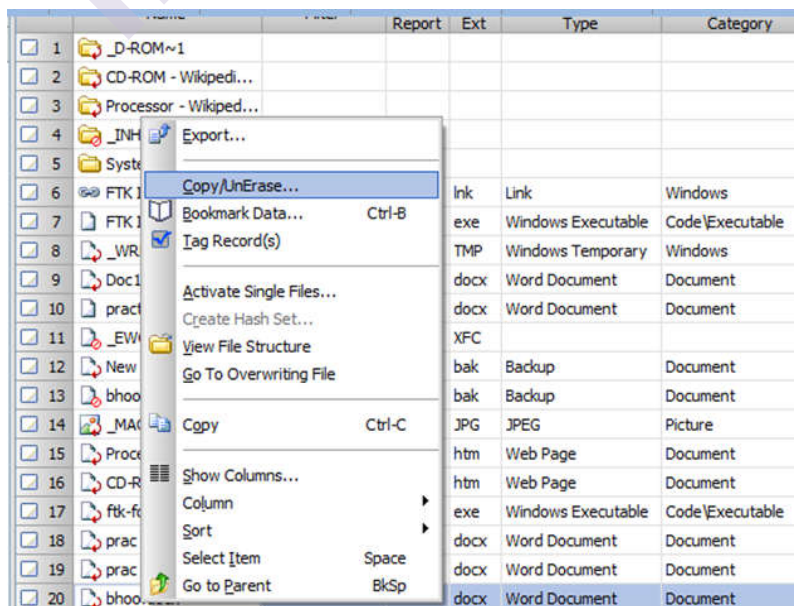
Right click on the Highlighted text area and then select the **Bookmark Data** for bookmarking the selected area.

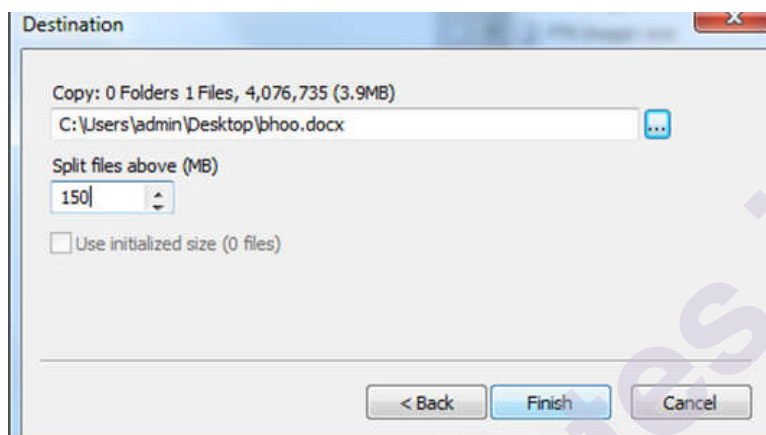
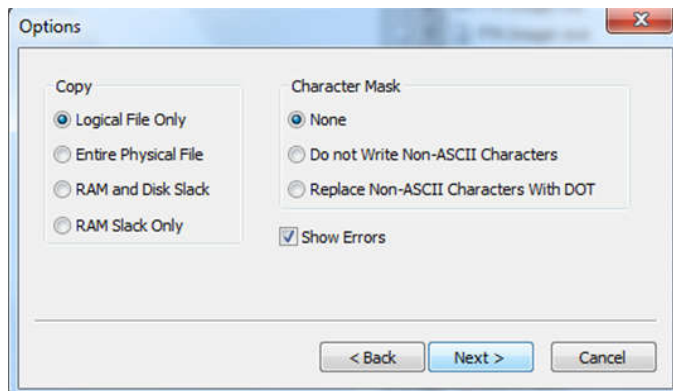


Recovering Deleted Folders and Files:

To recover files,

- Right-click on File,
- select **copy/Unerase**
- on option Screen, select the **Next** button
- Select **Destination Path**
- Select **Finish** button





To recover delete Folder:

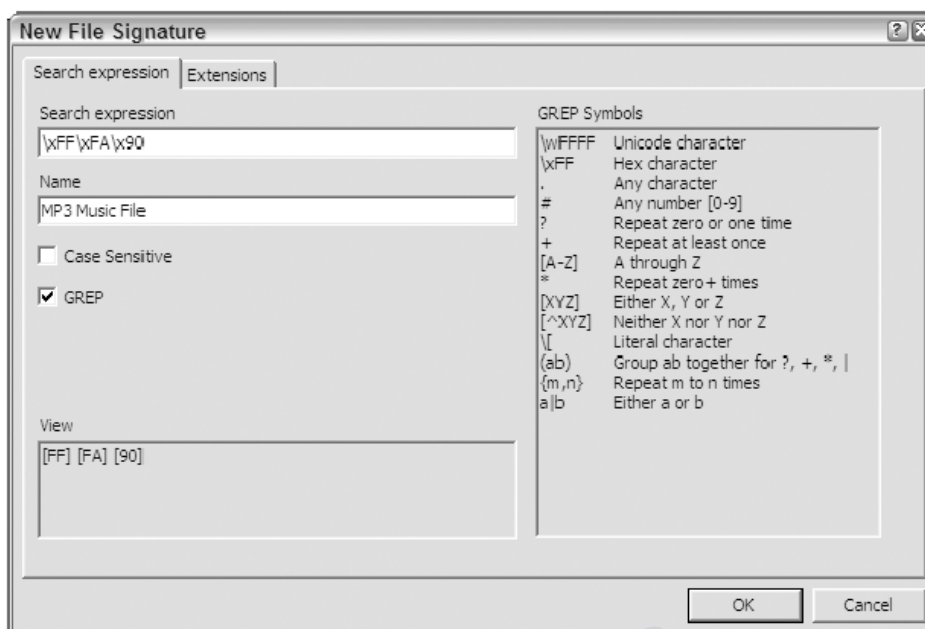
- Right-click on deleted Folder,
- select **copy/Unerase**
- on option Screen, select the **Next** button
- Select Destination Path and then click on the **Finish** button

Signature Analysis:

Executing signature analysis gives you an advantage in seeing all graphic files in Gallery view, regardless of what the current file extension is.

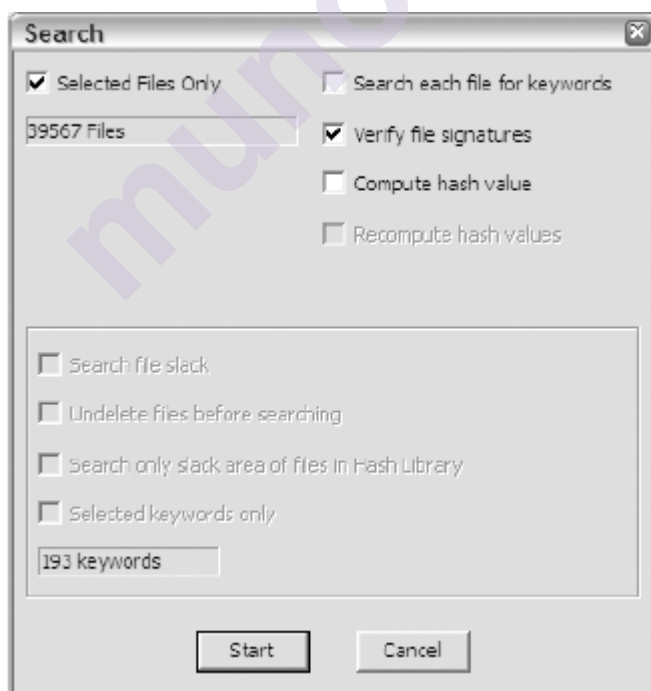
To create a new File Signature:

The new File Signature dialog box allows you to enter search expressions in the form of GREP, name of file signature, and the extension and click on the **OK** button. As shown in fig



Name: MPEG Movie File
 Search expression: \x00\x00\x01\xB3
 GREP: Yes
 Case Sensitive: No
 Extensions: mpg;mpeg;mps;mpv;mpa;mp2;13;m1s;m1v;m1a;m2s;m2v;m2a

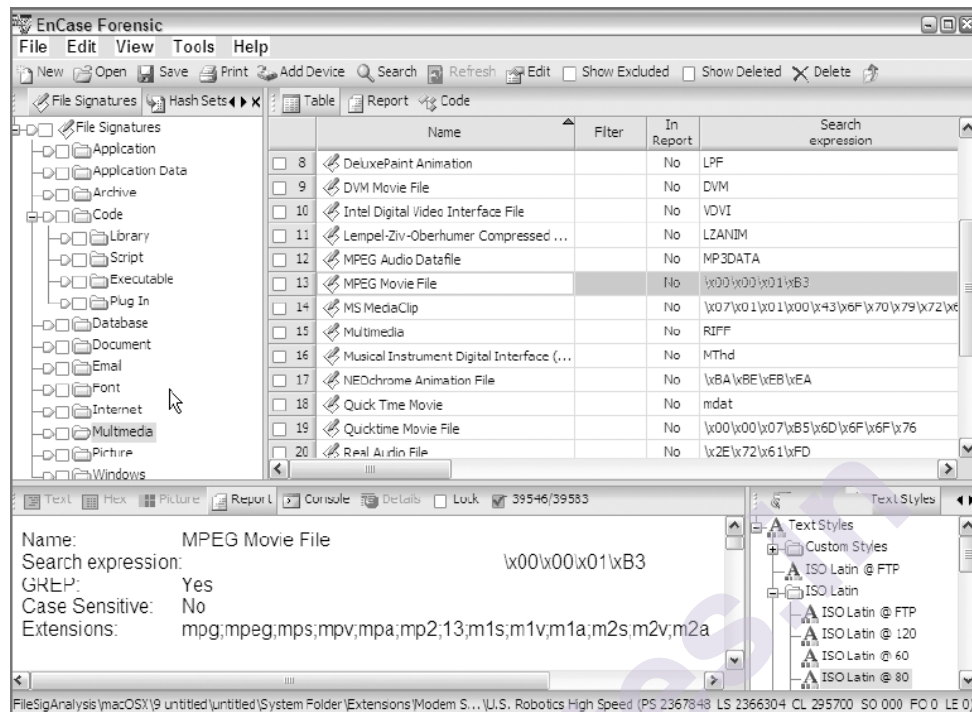
To perform file signature analysis Click on the **Search** button. Place check in front of **Verify file signatures**. Click on the **Start** button.



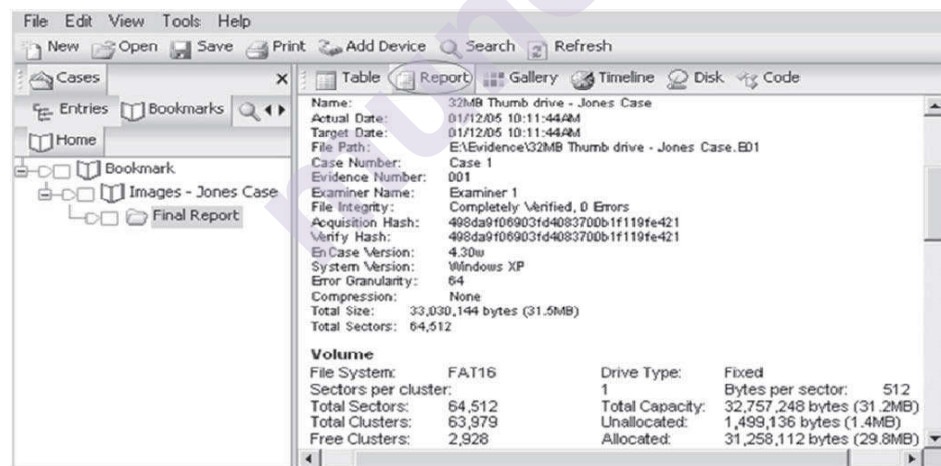
View File Signature Analysis Results

Click **View** menu, then **File Signatures**. Set green Home plate to show all items.

Recovery of Deleted Files and Partitions, Using Access Data Ftk and Encase for Forensic Investigation



To view disk geometry by highlighting the case and Clicking Report on the top menu.



Reporting:

Reporting is the final stage of Forensic analysis. Reports can be generated from bookmarks made in a case.

5.4 LET US SUM UP

This unit helps gain an understanding about recycle bin and partitions and the tools needed for recovery of deleted data and partition and also performing investigation using Access Data FTK and EnCase.

5.5 LIST OF REFERENCES

[1] The official CHFI Exam 312-49 Study Guide by Dave Kleiman, Syngress Publication, 2007.

5.6 BIBLIOGRAPHY

[1] EC-Council CHFIv10 Study Guide, EC-Council, 2018
[2] Forensic Toolkit User Guide, AccessData Corp.

5.7 UNIT END EXERCISES

1. _____ is a temporary storage place on windows desktop for deleted files where those deleted files are temporarily stored if they are not deleted permanently.
 - a. Temp Folder
 - b. Recycle Bin
 - c. Bin Box
 - d. My Documents
2. _____ are created by logically dividing Hard disk into volumes (Drive) and those volumes/drives are identified by letters like C or D or E etc.
 - a. Fragments
 - b. Partitions
 - c. Folders
 - d. Files
3. _____ is a commercial forensic imaging software package distributed by Access Data.
 - a. Autopsy
 - b. EnCase Imager
 - c. FTK Imager
 - d. Image MaSter Solo
4. Registry viewer, in-depth easy to read logging, standalone disk imager is the features of _____.
 - a. Autopsy
 - b. EnCase Imager
 - c. FTK Imager
 - d. Image MaSter Solo

5. An investigator can highlight findings in case by using _____.
a. Highlighter
b. Bookmark
c. keyword
d. Search
6. E01, E02 are the extension of forensic image files generated by _____ tool.
a. Autopsy
b. EnCase Imager
c. FTK Imager
d. Image MaSter Solo



munotes.in

FORENSIC ANALYSIS OF STEGANOGRAPHY AND IMAGE FILES, CRACKING APPLICATION PASSWORDS

Unit Structure

6.0 Objectives

6.1 Introduction

6.2 Forensic Analysis of Steganography and Image files

6.2.1 Steganography

6.2.2 Different types of Steganography

6.2.3 Tools for Steganography

6.2.4 Steganalysis

6.2.5 Tools for detecting Steganography

6.3 Cracking Application passwords

6.3.1 Password

6.3.2 Methods for cracking or attacking passwords

6.3.3 Password cracking tools

6.3.4 Recommendations for improving passwords

6.4 Let us Sum Up

6.5 List of References

6.6 Bibliography

6.7 Unit End Exercises

6.0 OBJECTIVES

After studying this unit, you will be able to know:

- What is Steganography
- Different types of Steganography
- Tools for the Steganography
- How to detect the Steganography

- What is the password and password cracker
- Various methods of cracking and attacking the passwords
- Various types of password cracking tools

6.1 INTRODUCTION

Investigator performs digital forensics by collecting and correlating and analyzing evidence to know the process and motive behind the crime and to identify criminals, but anti-forensic techniques such as data hiding, Steganography, cryptography and password protection are major concerns. Hence Computer forensic investigators should know those techniques, their functions.

6.2 FORENSIC ANALYSIS OF STEGANOGRAPHY AND IMAGE FILES

6.2.1 Steganography

The word Steganography is derived from the Greek name “steganos” which means meaning hidden or secret and “graphia” which means writing or drawing. So Steganography means hidden writing. It is the practice of concealing messages or files or images within another file/images or videos. Steganography is used for secure communication by hiding information in a file. It is also used for anti-forensic.

Steganography is different from cryptography but both are used for improving the security of protected data and prevent the detection of secure communication. Cryptography is about hiding the contents of a message in an unreadable format using algorithms like RSA, AES, DES, etc.

The main aim of Steganography is to prevent the detection of a secret message.

In Steganography, two types of files are used, one used to hide the text message or another file known as Carrier file and the other one which is inserted into the carrier file is known as a hidden file.

How Steganography works:

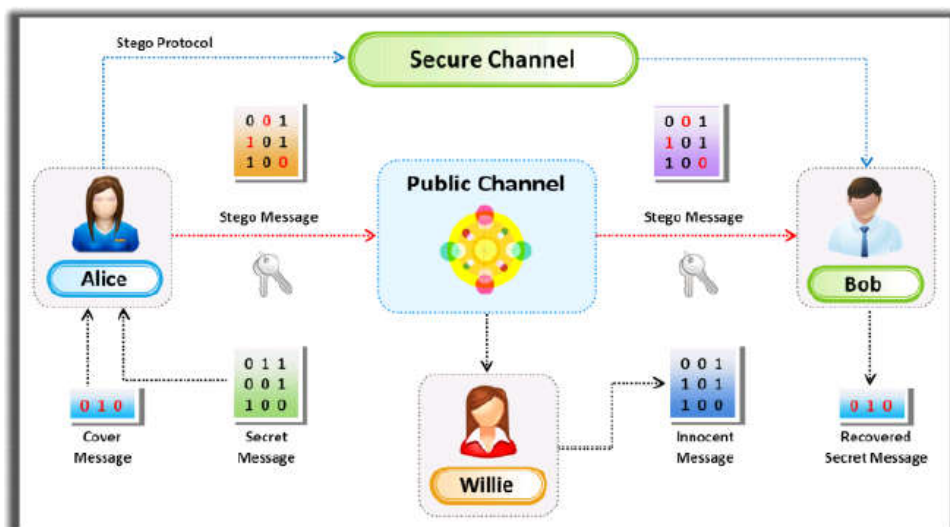


Fig. Steganography process

1. Alice embeds a secret message into the cover message (original Message) to generate a Stego message.
2. Stego message (message with a secret message) sent to Bob via a secured public channel.
3. Bob receives Stego message.
4. Bob decodes Stego message using a key to get a secret message.
5. Willie (Third person) thinks the message sent as a normal message.

6.2.2 Different type of Steganography:

Steganography can be applied to a variety of digital media such as image, audio, video, or text.

- **Image Steganography:**

The information is hidden in the image files of different formats such as .jpg, .png, and .bmp.

- **Video Steganography:**

It is a technique to hide files within carrying video files of different formats such as .avi, .mpg4, .wma, etc.

- **Audio Steganography :**

It is a technique to hide messages in a digital sound format using the following methods

- **Least Significant Bit(LSB) insertion:** Replacing least impact bit with a bit from the embedded message

- **Adding echo to the audio signal:** Adding a slight echo using two different delays to encode the 1s and 0s bits.
- **Differential phase variations:** By modified the Initial phase of the sound file with the secret message.
- **Spread spectrum scheme:** Hiding small or narrowband signal, the secret message, in large or wideband cover are used for audio Steganography.

- **Document Steganography:**

Document Steganography adds whitespaces and tabs at the end of lines.

- **Folder Steganography:**

In Folder Steganography, the user hides one or more files in the folders.

- **Whitespace Steganography:**

It is a technique to hide the messages in ASCII text by adding whitespace to the end of lines.

- **Web Steganography:**

It is a technique to hide web objects behind other objects and upload them on the server.

- **Spam/Email Steganography:**

It is a technique to hide embedded data in spam emails.

- **Hidden OS Steganography:**

It is a technique to hide one operating system within another.

- **C++ Source Code Steganography:**

It is a technique to hide a set of tools in the files.

6.2.3 Tools for Steganography:

A simple copy command available on windows and cat command on Linux OS will help to hide text files behind an image file

On Windows OS-

copy /b infile.jpg + hidetext.txt outfile.jpg

Users can open outfile.jpg using notepad to retrieve text data from the image file.

On Linux OS-

cat infile.jpg

hidetext.txt > outfile.jpg

There are significant amounts of both open source and commercial tools are available for creating Steganography Content

- **Snow:**

It is a type of whitespace Steganography tool which appends whitespace at the end of the line to hide information.

Command to hide the message “this is whitespace Steganography tool” inside the infile.txt

Command to extract information from outfile.txt

snow.exe -C outfile.txt

- **Steganos:**

A steganographic tool that hides files inside a bmp, wav, voc, or text file.

- **Gifshuffle :**

Steganographic tool for storing message inside all GIF files including with transparency and animation also by shuffling the color map.

It provides encryption and compression and works in message concealing and message extraction modes.

Command to hide the message “this is whitespace Steganography tool” inside the infile.txt

**gifshuffle -C -m “meet me at 10” -p “ hello world“ infile.gif
outfile.gif**

Command to extract information from outfile.gif

gifshuffle -C -p “ hello world“ outfile.gif

snow.exe -C outfile.txt

- **Outguess:**

A steganographic tool that allows you to insert hidden information into the redundant bits of data source: that is, jpeg or PNG image formats.

- **Stegomagic :**

A steganographic tool that hides any kind of file or message inside a text file, .wav file, or 256-bit color .bmp files but the size of hidden data can be approximately one-eighth of the size of the carrier file.

- **SilentEye :**

Open Source tool which hides messages into pictures or audios.

- **iSteg:**

Open Source tool which hides files inside a .jpeg pictures.

- **OpenStego:**

Open Source tool which hides data within images.

- **Open Puff:**

Free software from Microsoft for Steganography.

- **Steghide:**

A tool that hides messages in images and audio files.

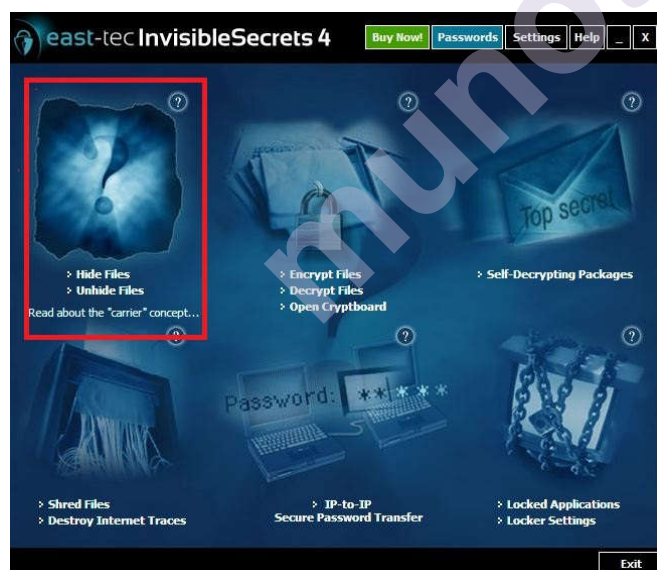
- **Invisible secret:**

A tool that hides the file within another file and later unhides that file.

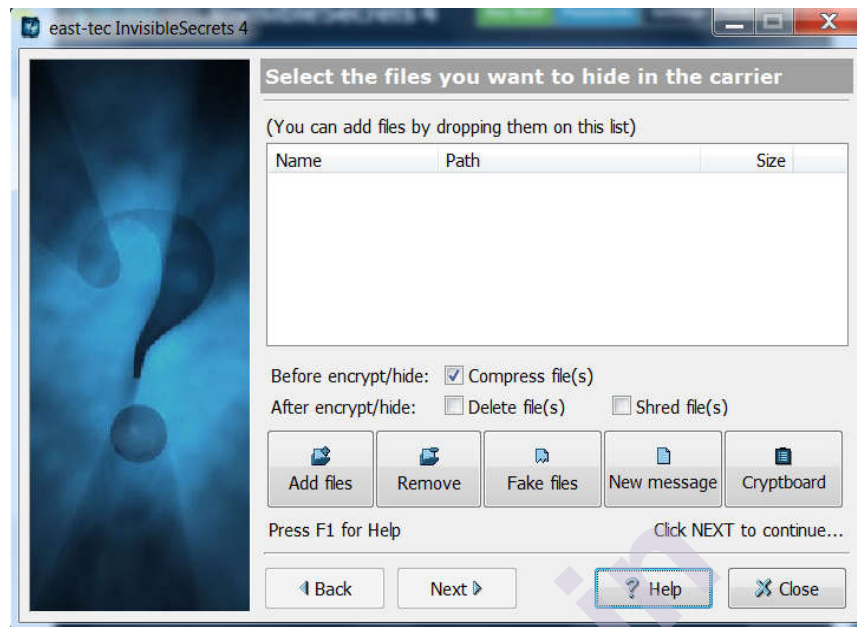
The invisible secret is software that is used to hide the file within another file and later unhide that file. Following are the step to hide the file using Invisible secret:

1. First Launch invisible secrets and Then select the option **Hide Files/UnHide files**

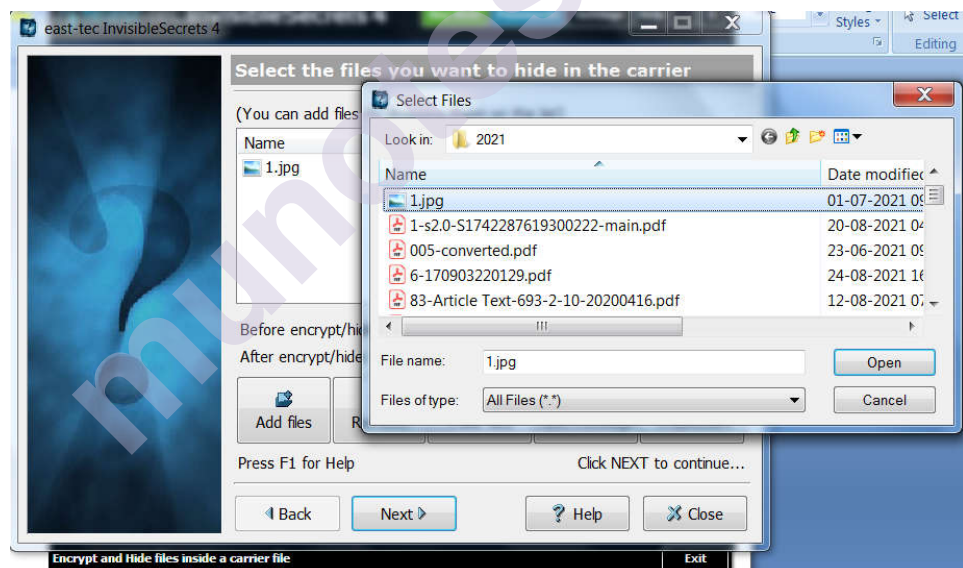
1.

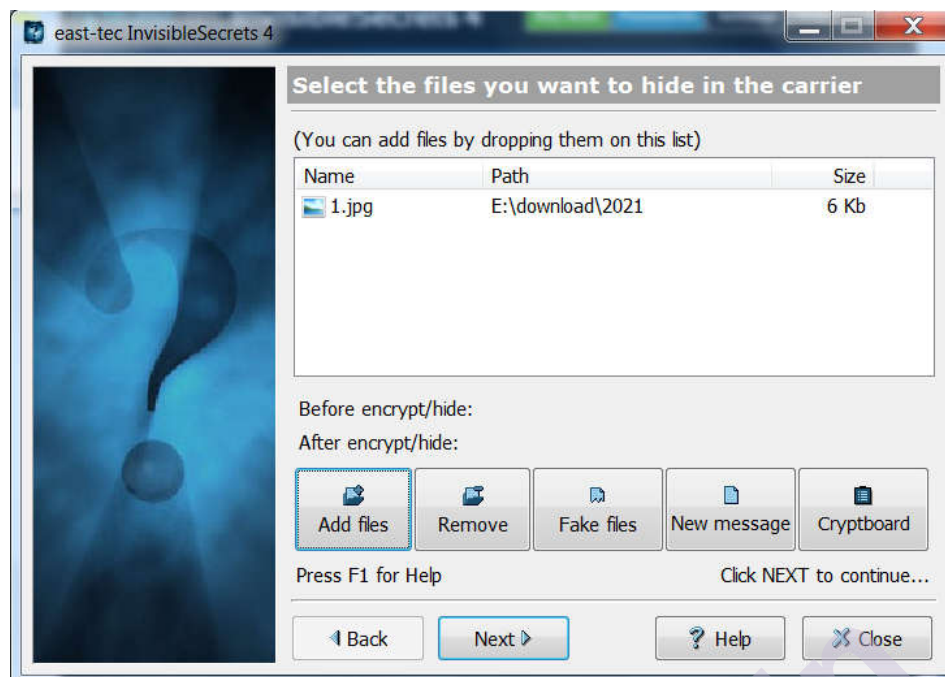


1. Click on the **Add file** button to select the file you want to hide in the carrier

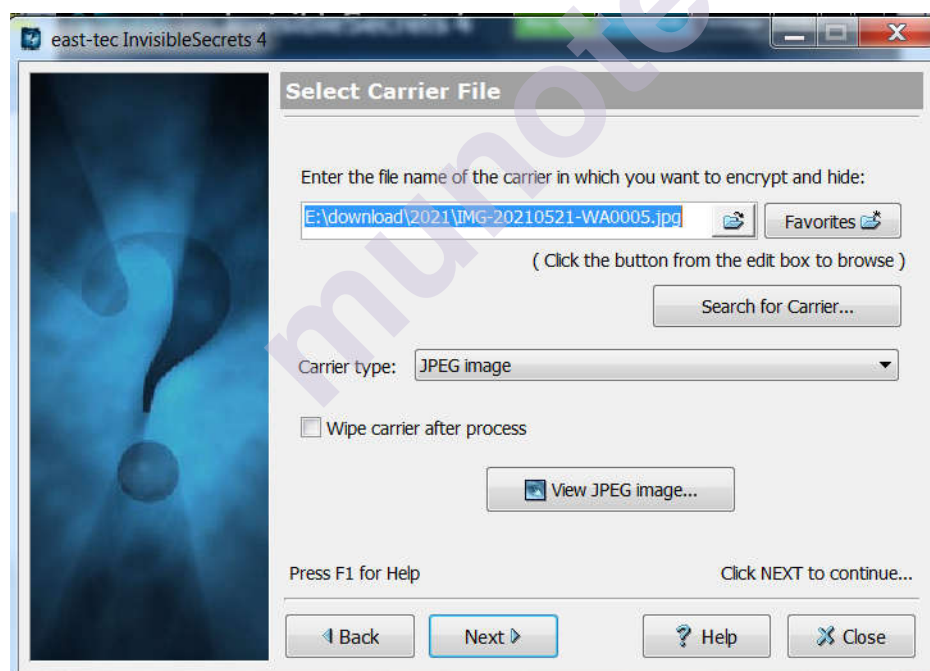


2. Select the file you want to hide

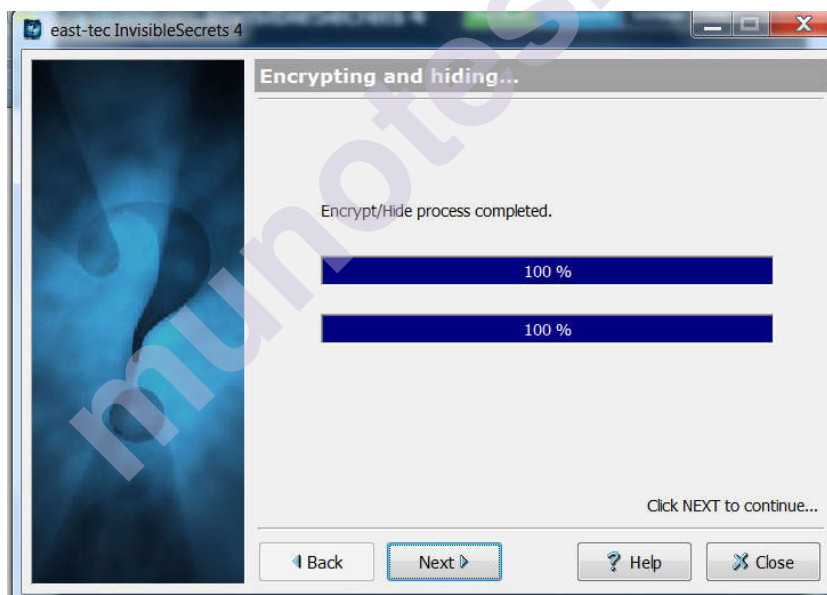
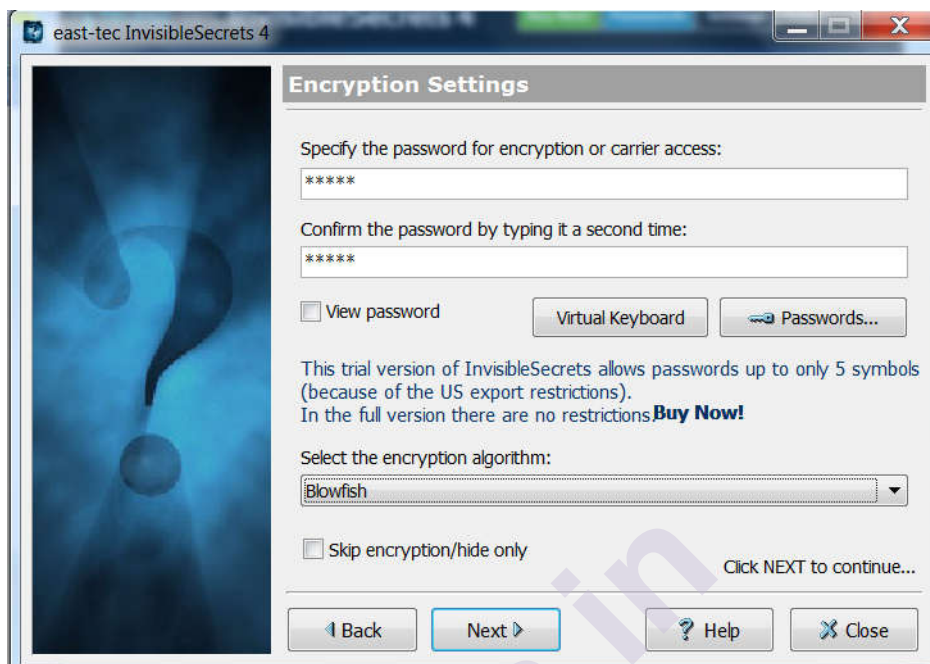




3. Click on the **Next** button and Select the Carrier file and the carrier type as jpeg image. Then Click on the **Next** button



4. Now specify the password for the Encryption and retype the password and click on the **Next** button



Finally you will get a Steganographic image.

6.2.4 Steganalysis

·**Steganalysis**: The process of discovering the existence of hidden information within the cover medium. It is a process of detection and distortion of messages. Steganalyst will try to detect hidden information in various digital mediums such as image, audio, video, etc.

Methods of detecting the Steganography:

- **Text/Document Steganography detection:**

Detection by looking for the text patterns or disturbance like unusual patterns used or appended extra spaces or invisible characters by using a simple word processor.

- **Image Steganography detection:**

Detecting Image Steganography by determining the changes in size, file format, last modification, last modification time stamp, and color palette of the image file.

- **Audio Steganography detection:**

The statistical method can be used for detecting audio Steganography as it involves the Least Significant Bit (LSB) modification and even the method of scanning for high or inaudible frequencies can be used for detection.

- **Video Steganography detection:**

A combination of Image and Audio Steganography detection methods can be used to detect Video Steganography. It mostly requires human involvement by observing Special codesign or gestures.

Types of Attack used by Steganalyst:

Steganography attack works based on what type of information is available with the attacker, Steganalysis is classified into six types: Stego-only, Known-Stego, Known-cover, Known-Message, Chosen-Message, and Chosen-Stego attack

- **Stego-only attack:**

In this attack, the attacker has only access to a stego-medium or stego object where Steganalyst will try every possible algorithm for recovering hidden messages.

- **Known-Stego attack:** In this attack along with access to Stego and the original object, Steganalyst knows the Steganographic algorithm. Steganalyst can extract hidden messages with this information.

- **Known-cover attack:**

In this attack attacker has access to the original and Stego object, Steganalyst can compare the original object and Stego object to detect changes for recovering hidden messages.

- **Known-Message attack:**

In this attack attacker has access to the message and Stego object, Steganalyst can detect techniques used to hide the message.

- **Chosen-Message attack:**

By using some Steganography tools and known messages, Steganalyst can find Steganographic algorithms used to hide information.

- **Chosen-Stegoattack :**

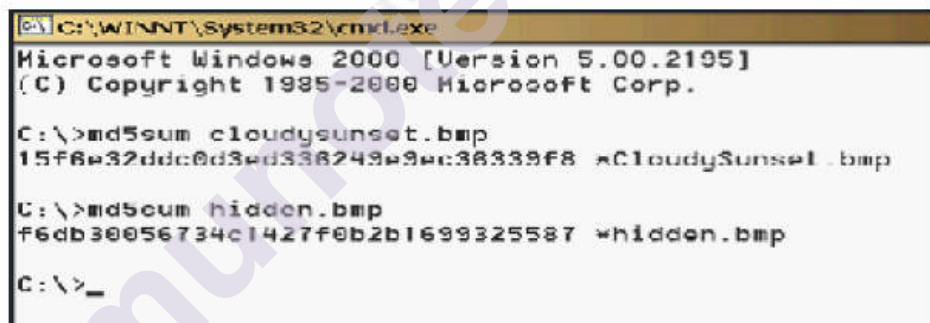
This attack takes place when along with access to Stego object, Steganalyst knows Steganographic algorithm used to hide information.

6.2.4 Tools for detecting Steganography

Various tools are available to detect Steganography which can be used by forensic investigators.

One of such methods is to detect Steganography by comparing the md5 hash values of two files. md5sum.exe program available on the internet to calculate the md5 hash value of any file.

As shown in Fig, md5 hash value of the original photo and same photo containing hidden information is calculated which gives different hash values.



```

C:\>md5sum cloudy sunset.bmp
15f6e32ddc0d3ed338249e9ec38339f8 *CloudySunset.bmp

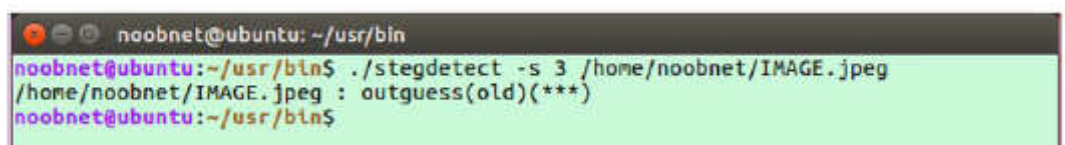
C:\>md5sum hidden.bmp
f6db30056734c1427f0b2b1699325587 *hidden.bmp

C:\>_
  
```

Stegdetect :

A Software to detect the Steganographic content of an image file. It can detect several different steganographic methods like jseg, JPHide, invisible secret, outguess, F5, appendX and Camouflage used to embed hidden information in JPEG images. It is available for Linux systems. Can be downloaded from https://centos.pkgs.org/7/forensics-x86_64/stegdetect-0.6-2.el7.x86_64.rpm.html

Stego file that we will identify is a jpeg image file.



```

noobnet@ubuntu: ~/usr/bin
noobnet@ubuntu:~/usr/bin$ ./stegdetect -s 3 /home/noobnet/IMAGE.jpeg
/home/noobnet/IMAGE.jpeg : outguess(old)(**)
noobnet@ubuntu:~/usr/bin$
  
```

Option `-s` will change the sensitivity of the detection algorithms.

`-t <tests>` sets the tests to run on the image):

`./stegdetect -t <tests>IMAGE.jpeg`

- Type `./stegdetect -t j IMAGE.jpeg` to check if the image has been embedded with jsteg.
- Type `./stegdetect -t o IMAGE.jpeg` to check if the image has been embedded with outguess.
- Type `./stegdetect -t p IMAGE.jpeg` to check if the image has been embedded with jphide.
- Type `./stegdetect -t i IMAGE.jpeg` to check if the image has been embedded with invisible secrets.
- Type `./stegdetect -t f IMAGE.jpeg` to check if the image has been embedded with F5.
- Type `./stegdetect -t a IMAGE.jpeg` to check if information has been added at the end of file.

```
noobnet@ubuntu: ~/usr/bin
noobnet@ubuntu:~/usr/bin$ ./stegdetect -t j /home/noobnet/IMAGE.jpeg
/home/noobnet/IMAGE.jpeg : negative
noobnet@ubuntu:~/usr/bin$ ./stegdetect -t o /home/noobnet/IMAGE.jpeg
/home/noobnet/IMAGE.jpeg : outguess(old)(**)
noobnet@ubuntu:~/usr/bin$ ./stegdetect -t p /home/noobnet/IMAGE.jpeg
/home/noobnet/IMAGE.jpeg : negative
noobnet@ubuntu:~/usr/bin$ ./stegdetect -t i /home/noobnet/IMAGE.jpeg
/home/noobnet/IMAGE.jpeg : negative
noobnet@ubuntu:~/usr/bin$ ./stegdetect -t f /home/noobnet/IMAGE.jpeg
/home/noobnet/IMAGE.jpeg : negative
noobnet@ubuntu:~/usr/bin$ ./stegdetect -t a /home/noobnet/IMAGE.jpeg
/home/noobnet/IMAGE.jpeg : negative
noobnet@ubuntu:~/usr/bin$
```

OutGuess is a Steganographic tool that allows you to insert hidden information into the unnecessary bits of data source: that is, jpeg or PNG image formats.

Other tools to detect Steganography:

- **XStegsecret:**

A java based multiplatform tool which detects hidden information from various digital medium sources. It is used to detect EOF, LSB, DCTs, etc.

- **StegSecret:**

Open Source Java-based multiplatform tool detects hidden information in different digital medium sources. It is used to detect EOF, LSB, DCTs, etc.

StegExpose:

- A command line based interface tool helps in detection of LSB Steganography on .bmp or .png files

- **ImgStegano:**

This tool helps in the detection of Steganography on .bmp or .png files, to detect image Steganography it uses an enhanced LSB technique.

- **StegSpyV2.1 :**

It's a Signature detection program that searches for Stego Signature and determines the program used to hide the messages, it identifies 13 different Steganography programs and also identifies the location of hidden messages.

6.3 CRACKING APPLICATION PASSWORDS

6.3.1 Password:

From the beginning of computer systems, some types of passwords are required for authentication purposes like to enter into the system, to change the BIOS setting, to login to computer systems or operating systems to perform the administrative task of operating systems, to protect the documents from unauthorized access, etc.

Passwords are in the form of a word, phrase, or string of characters. Password crackers are programs used to unauthorized access to applications or files which are password protected.

Devices can store or transmit passwords as clear text obfuscated or hashed Passwords.

Out which hashed password needs cracking and rest of the password type can assist in cracking.

- **Clear Text Passwords:**

Passwords stored in plaintext without any alteration.

E.g Windows registry stores automatic login password

(Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\WinLogon)

Cain and Ettercap used by the investigator to sniff the clear-text password.

- **Obfuscated Passwords:**

Passwords stored after one or more transformations.

The password becomes unreadable by applying an algorithm for reversible transformation, it returns a clear-text password after application of the reverse algorithm.

- **Hashed Passwords:** Hashed passwords are similar to Obfuscated Passwords but not reversible.

6.3.2 Methods for cracking or attacking passwords

Password crackers are the program to assist users to gain unauthorized access to an application; it is also used to retrieve lost or forgotten passwords of any application. Password crackers can use various methods to identify passwords.

Various methods for cracking or attacking passwords include:

- Password Guessing
- Dictionary search
- Brute Force method
- Syllabus attack
- Rule based attack
- Hybrid attack
- Rainbow attack

Password Guessing:

Attackers are successful because they can guess a person's password very easily. This can be the result of a blank password selected by the user or a simple password like "password" or "drowssap" selected by the user or a password selected based on their spouse, kids, relative, or personal information.

Dictionary Search:

In this method, password cracking tools are loaded with files having words from the dictionary. Cracking will be successful if the password matches one of the words from the dictionary.

Brute Force method:

It is a method of trying every possible combination of text/character and testing to see if it is correct or not. Password length increases, the amount of time also increases. Compare to the shorter the password takes less time, the longer password may take a decade;

Syllable attack:

If passwords do not contain a dictionary word then this method uses the technique by combining syllables from dictionary words use tokens later applying brute force attack.

Rule-based attack:

The attacker gets some information like organization password policy such as “Length of password should be less than eight characters”

and based on this information attackers customized their tools for password cracking

Hybrid attack:

It is used if the password is of type dictionary word combining with some characters. Cracking will be successful because most of the users select a password that is a dictionary word combining with some additional characters

Rainbow attack:

The attacker uses a rainbow algorithm to crack the password by calculating all possible hashes for characters and storing them in the table.

6.3.3 Password cracking tools:

- **Cain and Abel:**

Microsoft Windows-based password cracking tools use brute force, dictionary-based attacks methodologies, and other cryptanalysis tools. It works as a sniffer on the network to crack encrypted passwords.

- **OphCrack:**

Password cracking tools based on rainbow tables and available on Windows, Linux/Unix, and Mac OS X platforms.

- **LCP:**

Microsoft Windows-based password cracking tool and alternative to popular L0phtCrack tool and it uses brute force, hybrid, rainbow table, and dictionary-based attacks methodology.

- **John the Ripper:**

A free open-source password cracking tool to detect weak passwords and available on Windows, Linux/Unix, and Mac OS X platforms. The Pro version of the tool offers more features.

- **CMOSPwd:**

It is used to decrypt the BIOS setup password stored on CMOS which is used to access BIOS setup. It works with Acer/IBM BIOS, AMI BIOS, AMI WIN BIOS Award 4.5x, Compact old and new version, Toshiba, Zenith, Gateway solo, Phoenix, etc.

- **Smartkey Password Recovery Bundled Standard:**

A multifunction password recovery software that recovers the password from Microsoft Excel, Word, Access, PowerPoint, Outlook, ZIP/ WinZIP, RAR/ WinRAR, PDF, MSN, AOL, Google, Miranda, Opera, Firefox, IE Browser, etc.

- **Passware kit:**

This tool is a complete electronics evidence discovery solution that can recover passwords of 200+ different types of files. It also supports Distributed and Cloud computing password recovery.

Password cracking software based on cracking various application passwords include

- **Office password cracking software:**

Office password cracking software is used to recover passwords of any Microsoft office documents like Microsoft Word, Excel, Powerpoint, Access database, Outlook email account, OneNote Notebook, etc. It can also recover the password of read-only documents.

Office password recovery toolbox, Office password recovery Lastic, Stellar Phoenix Office Password Recovery, Online Password Recovery, Online password Genius, Smartkey office password Recovery, Advanced Office Password Recovery, Office Multi-document Password Cracker, Word Password Recovery Master, Accent Word Password Recovery, Smartkey PowerPoint Password Recovery, PDS Excel Password Recovery are the tools for cracking MS office files passwords.

- **PDF Password cracking software:**

Crack PDF, PDF Password Recovery, PDF Password Genius, Smartkey PDF password Recovery, Tenorshare PDF Password Recovery, Guaranteed PDF Decryptor, and Advanced PDF Password Recovery are tools that can crack the password of password-protected PDF files.

- **ZIP Password cracking software:**

Accent ZIP Password Recovery, ZIP password Genius, Smartkey ZIP password Recovery, KRyLack ZIP password Recovery, Stellar Phoenix ZIP password Recovery are tools that can crack the password of ZIP archives.

- **RAR password-Cracking Software :**

Accent RAR Password Recovery, cRARk 5.1, Smartkey RAR password Recovery, KRyLack RAR password Recovery are tools that can crack the password of RAR archives.

Some other popular tools for password cracking are Brutus, RainbowCrack, PWdump7, Fgdump, Wfuzz, KonBoot, Hashsuit, THC-Hydra, Offline NT Password, and Registry Editor, Password Unlocker Bundle, Proactive System Password Recovery, DaveGroh, Active@ Password Changer, etc.

6.3.4 Recommendations for improving password

There is some recommendation for improving passwords:

- Do not use dictionary words for selecting a password.
- Always select a difficult password, do not use a password that is based on a spouse, kids, relative, or personal information.
- Use multiple character sets while selecting passwords i.e. Combinations of alphabets, numbers, and special characters
- Change your passwords frequently once or thrice a month.
- Do not use the same password in more than one place, the password should be unique for each account.
- Use a longer password, it will take more time to crack the password if it is longer.

6.4 LET US SUM UP

This unit helps gain an understanding of Steganography and tools needed to detect Steganography and various password attacks and the tools for cracking application passwords.

6.5 LIST OF REFERENCES

[1] The official CHFI Exam 312-49 Study Guide by Dave Kleiman, Syngress Publication, 2007.

[2] Practical Cyber Forensics Niranjana Reddy Apress -- 2019

6.6 BIBLIOGRAPHY

[1] EC-Council CHFIv10 Study Guide, EC-Council, 2018

6.7 UNIT END EXERCISES

1. _____ is about hiding the contents of a message to an unreadable format using algorithms.
 - a. cryptography
 - b. password
 - c. Steganography
 - d. watermarking

2. _____ the practice of concealing messages or files or images within another file/images or videos.
 - a. cryptography
 - b. password
 - c. Steganography
 - d. watermarking
3. _____ Steganography adds whitespaces and tabs at the end of lines.
 - a. Image
 - b. Document
 - c. Video
 - d. Audio
4. In case of _____ password, Password stored after one or more transformations but not reversible.
 - a. default
 - b. Obfuscated
 - c. Hashed
 - d. Clear
5. _____ attack technique works by calculating all possible hashes for character and storing them in the table.
 - a. Brute Force
 - b. Rainbow
 - c. Rule based
 - d. Hybrid
6. _____ is a Windows based password cracking tools uses brute force and dictionary based attacks.
 - a. Passware Kit
 - b. ERD Commander
 - c. Cain and Abel
 - d. CMOSPwd



INVESTIGATING NETWORK TRAFFIC AND INVESTIGATING LOGS

Unit Structure

- 7.0 Objective
- 7.1 Introduction
- 7.2 Capturing logs and correlating to the events
- 7.3 Network Forensics – Investigating logs and Network traffic
 - 7.3.1 Overview of the OSI Model
 - 7.3.1.1 Layers of the OSI Model
 - 7.3.2 Network Addresses and NAT
 - 7.3.3 Network Information-Gathering Tools
 - 7.3.4 Intrusion Detection
 - 7.3.5 Snort
 - 7.3.6 Monitoring User Activity
 - 7.3.6.1 Tracking Authentication Failures
 - 7.3.6.2 Identifying Brute Force Attacks
 - 7.3.6.3 Tracking Security Policy Violations
- 7.4 Summery
- 7.5 References for further reading

7.0 OBJECTIVE

When working with these logs, there are a few things to keep in mind:

- In order to interact with the Security event log, Log Parser has to be able to distinguish between single and multiple events.
- It's critical to distinguish between benign events and true faults or warnings in order to have a complete picture of your system's state.
- It is vital to have a good understanding of the individual application you are dealing with while working with apps and the Application event logs.

7.1 INTRODUCTION

Networks are subjected to a never-ending barrage of attacks and vulnerabilities. External threats usually originate on the Internet and fall into one of three categories: denial of service (DoS), utilising the victim's

network as a launchpad to attack other networks, or threatening or altering information. Individuals with legitimate access or those who have exceeded their level of privilege can pose an internal threat. This necessitates a forensic expert's knowledge of how the network operates as well as how to obtain logged data.

Insider and outsider attack monitoring should be a proactive effort, yet many attacks are not noticed until after they have occurred. This will necessitate a review of log files. The attack can only be assessed and reconstructed by reviewing the audit and log data. Many forensic professionals don't make full use of log and audit data because they don't know how to get it or because reading through thousands upon thousands of log file entries takes a long time.

7.2 CAPTURING LOGS AND CORRELATING TO THE EVENTS

Capturing and analyzing the log files are necessary tasks for investigating the safety posture of the target network, as they contain information concerning all the system, device, and user activities that happened inside the network.

As a security admin, we should understand that almost each device on our network spits out some kind of log. and that we also understand that keeping track of these logs is a very important piece of the puzzle to knowing our security posture. However, we have to understand the purpose behind capturing logs before we are able to build a decent decision on what methodology we will use to capture the logs.

So what's the reason behind capturing logs? Do we have a tendency to mainly make an attempt to check what's happening with our network so as to identify potential security issues? If that's the case, then we want to analyze which technologies best do correlation and can facilitate seeing things on our network that we would have trouble seeing ourselves. These systems are generally complicated and require a lot of designing effort so as to produce sensible results. We'd like to possess intimate information about our network to understand avenues of attack and very important systems. Therefore, we are able to setup rules and alerts. They additionally need maintenance when changes are made to our network. However, if done right, these tools will provide you with a very good look at our network's security, and they can help you notice issues much faster than you might.

If alerting and intricate correlation aren't a concern, we could just want to capture the logs for forensic purposes and do some simple alerting. If that's the case, we'll need to look for technologies that prioritise disc space (high native capacity and expandability), log normalisation, and log protection (encryption and no repudiation).The reason for restricted log normalisation (or none if we can get away with it) and log protection is in case you have a security breach that could lead to a court lawsuit.To be accepted in court, we must be able to demonstrate that the logs are accurate and have not been tampered with.These boxes must also be able

to transport logs conveniently to storage while maintaining nonrepudiation. We require disc capacity since, if you are concentrating on forensics, you will most likely need to preserve logs for a long time.

Another reason people have these devices is to use them as an audit or compliance tool. Though I consider this to be the least relevant reason for installing log management, I am aware that if it will relieve me of the burden of an auditor, I will use it. Many manufacturers also include thorough audit and compliance information, which is a dream come true for auditors. If this is your requirement, make sure you concentrate on devices with strong reporting capabilities.

In terms of reporting, I've found that in my experience with these devices, a gadget is either very strong in one of the above attributes or very strong in reporting. Only a few people are good at both. However, I believe that manufacturers should place a strong emphasis on both. It doesn't matter if you have all the knowledge in the world if the user doesn't know how to access it. And the world's security administrators adore configurable dashboards that they can show their bosses (and the auditors I mentioned earlier) so that they receive fewer questions about what's going on in the network.

Most log management technologies will have all of the above features in some way, shape, or form, but their strength will vary. Determine what your company's log management focus needs to be when you're doing your risk analysis. For instance, if you are a large corporation with a complex network, you may need to find a good correlation engine. If you're a smaller company with high-value intellectual property, you might want to invest in a box with forensic capabilities to ensure that you can track down violations and recover your losses in court.

7.2 NETWORK FORENSICS – INVESTIGATING LOGS AND NETWORK TRAFFIC

7.3.1 Overview of the OSI Model

The Open Systems Interconnect (OSI) paradigm was created by the International Standards Organization in 1984. The concept is intended to offer order by defining a hierarchical structure in which each layer builds on the output of the previous layer. The model is still used as a guide to describe how a networking environment works today.

7.3.1.1 Layers of the OSI Model

The physical, data connection, network transport, session, presentation, and application layers are the seven layers of the OSI model. Let's look at each of these layers one by one. The physical layer, often known as Layer 1, is the first layer. Bit-level communication takes place at Layer 1. On the cable, the bits have no meaning, but the physical layer determines how long each bit lasts and how it is transferred and received. If no encryption is utilised, a large amount of sensitive information may be available at the physical layer from a forensics standpoint.

Layer 2 of the Data Link Layer is known as the data link layer. Before delivering data to the physical layer, the data link layer is in charge of preparing and arranging it. Data is organised into frames by the data link layer. A frame is a logical structure that can be used to store data. When a frame reaches the target device, the data link layer separates the data frame from the data packet and passes it up to the network layer. The logical link control layer (LLC) and the media access control layer (MAC) are two sublayers of the data link layer (MAC).

Layer 3 is the network layer, which is responsible for logical addressing and routing. The Internet Protocol (IP) lives at the network layer, and it makes every attempt to convey datagrams from their source to their destination. The Transport Layer-The transport layer, also known as Layer 4, maintains completeness by managing end-to-end error recovery and flow control. TCP, a connection-oriented protocol, is one of the transport-layer protocols. Handshaking, acknowledgments, error detection, and session deconstruction, as well as the connectionless User Datagram Protocol (UDP), offer trustworthy communication. Its key advantages are speed and reduced overhead.

The Session Layer (Layer 5) is the fifth layer in the stack. Its capabilities are used when starting, controlling, or terminating a TCP session. Here you'll find things like the TCP 3-way handshake and the TCP 4-way shutdown. Remote Procedure Call and Structured Query Language are examples of session-layer protocols.

The Presentation Layer-Layer 6 is in charge of converting data handed up from lower levels into a format that application layer programmes can understand. ASCII, EBCDIC, and ANSI are some of the most used forms.

The application layer, often known as Layer 7, is the seventh layer. This layer serves as the window for application services and is known as the top layer of the OSI model. Most users are familiar with the application layer, which houses e-mail programmes, FTP, Telnet, web browsers, office productivity suites, and a variety of other applications.

7.3.2 Network Addresses and NAT

The IP address scheme is used for logical addressing in TCP/IP networks. A physical address is a MAC address, whereas a logical address is an IP address. Dotted decimal notation is used to configure IP addresses. Four decimal integers separated by decimal points make up the IPv4 address format. To allow numbers to range from 0 to 255, each of these decimal values is one byte long.

- **Class A Networks.** Class A networks can have up to 16,777,214 client devices and an address range of 1 to 126 addresses.
- **Class B Networks.** Class B networks can accommodate up to 65,534 client devices and have an address range of 128 to 191.

- **Class C Networks.** Class C networks can support up to 245 devices and have an address range of 192 to 223.
- **Class D Networks.** These addresses range from 224 to 239 and are reserved for multicasting.
- **Class E Networks.** These addresses are only available for personal use. They have addresses ranging from 240 to 254 miles apart.

Network Address Translation (NAT) was created in response to the Internet's fast growth, and the number of available IP addresses is simply not enough for the growing number of residential and commercial networks. Internet Service Providers (ISPs) typically assign a single address to a single subscriber. Companies can purchase a large number of addresses, but they must pay for each one separately. Direct Internet access has its own set of risks. NAT is a secure and cost-effective option. A single device, such as a router, can operate as an intermediary between the Internet and the local network via NAT. This device, often known as a router, offers a pool of addresses that your local network can use.

7.3.3 Network Information-Gathering Tools

Network data collection tools are pieces of software that can be used to collect network data for forensic examination. These tools usually combine the features of a sniffer with an intrusion detection system. Sniffers are strong programmes that work by putting the network card in promiscuous mode on the host system. In promiscuous mode, a network device can receive any data it can see, not just packets addressed to it. Switches segment traffic and know which ports to send traffic to and which ports to stop it from. Although this feature provides much-needed efficiency improvements, it does create a barrier when sniffing all possible switched ports. Forensic analysis will usually require the switch to be configured to mirror a port. Some common network monitoring tools include:

- **NetWitness.** NetWitness is designed to analyze network traffic and monitor it.
- **Netresident Tool.** Captures, stores, analyses, and reconstructs network events such as e-mail messages, Web pages, downloaded files, and other sorts of network traffic.
- **Infinistream Security Forensics.** A commercial solution based on sniffer technology that provides high-end tracking of everything.
- **CA Network Forensics.** Allows the user to analyse and discover network traffic.

This tool collects raw network data and does forensic analysis to look for exploitation, internal data theft, and security breaches.

- **Wireshark.** An open source protocol analyzer that can capture traffic in real time.

- **Snort.** A well-known open source IDS that detects events using signatures. Sniffers work at the OSI model's data link layer. This means they are not bound by the same set of rules as apps and services higher up the stack. Sniffers can record everything that happens on the wire and review it later. They enable the user to examine all of the data included within the packet. Wireshark is a decent sniffer programme. It is not only free to use, but it also runs well on both Windows and Linux.

Next, we will discuss the second category of network information-gathering tools, intrusion detection.

7.3.4 Intrusion Detection

Intrusion detection systems (IDS) play a second crucial function in IT infrastructure security. Monitoring network traffic, detecting attempts to obtain unauthorised access to a system or resource, and notifying the proper personnel so that countermeasures can be taken are all part of intrusion detection. It's a powerful tool to be able to examine invasions and attacks. During a forensic investigation, four sorts of logs are of interest: authentication, application, operating system, and network—but the IDS will be most useful for network logs. There are plenty of good IDS systems on the market. Snort is an example of an IDS that has widespread acceptance in the industry.

7.3.5 Snort

Martin Roesch and Brian Caswell created Snort, a freeware intrusion detection system. It's a network-based intrusion detection system that can run on Linux or Windows. Although the primary software has a command line interface, there are GUIs available. Snort is a network sniffer that records activity that fits predetermined signatures. Internet Protocol, Transmission Control Protocol, User Datagram Protocol, and Internet Control Message Protocol are all examples of communication for which signatures can be created. A forensic analyst can only benefit from an intrusion detection system if the data is reviewed and evaluated.

Unfortunately, an IDS can occasionally generate large amounts of data that are difficult to process. We may use Microsoft Log Parser to capture snapshots of our IDS logs and show them in several easy-to-read reports to help us analyse the data.

We'll create an example IDS report utilising only Log Parser's capabilities. Snort Logs are being gathered.

We need a consistent technique for acquiring data before we can process the alert data. The Log Parser is a great tool for managing Snort logs since it allows you to query the file while Snort is still processing it. Many administrators set up scripts to cycle through the Snort logs on a regular basis, but this necessitates halting the service in order for the file to be released and moved by the script. We can utilise checkpoints in the Log Parser to read the most current data from the file.

Despite the fact that Snort offers a variety of output formats that Log Parser can use, I've found the CSV format to be the most versatile and consistent. Simply add the following line to the 0 snort.conf file to set Snort to use the CSV output format: To configure Snort to use the CSV output format, simply add the following line in the 0snort.conf file:

```
output alert_csv: alert.csv default
```

This tells Snort to produce an alert.csv CSV log file in the configured logsdirectory with the default output fields. The fields below are included by default in the CSV output processor:

- timestamp
- sig_generator
- sig_id
- sig_rev
- msg
- proto
- src
- srcport
- dst
- dstport
- ethsrc
- ethdst
- ethlen
- tcpflags
- tcpseq
- tcpack
- tcplen
- tcpwindow
- ttl
- tos
- id
- dgmlen
- iplen

- icmp type
- icmp code
- icmp id
- icmp seq

Snort CSV logs do not include a header row, so we need a separate file to name each column. To read CSV Snort alerts, you would use a command like this:

```
logparser.exe file:alert.sql -i:csv -headerRow:off -
```

```
iHeaderFile:AlertHeader.csv -iTsFormat:mm/dd/yy-hh:mm:ss
```

Note that we specify the CSV input format, but instead of using the header row, we specify a header file using the **iHeaderFile** option. We also specify the timestamp format so Log Parser can interpret that field as an actual time stamp rather than a string.

Building an Alerts Detail Report

In our IDS report we likely want to view summaries of the alert data such as:

- Most common source IP (Internet Protocol) addresses
- Most common target IP addresses

We can simply produce interactive HTML (Hypertext Markup Language) reports directly from Snort logs using Log Parser's multiplex functionality and template output format.

Alerts by IP Address

Each IP address in Figure 7.1 alerts report is a clickable hyperlink that takes you to a detail page with all of the alerts for that IP address. We utilised a two-pass technique to build a summary page (Figure 7.2) and detail page (Figure 7.3) using a process identical to that used for the alert messages. To create a fully interactive HTML IDS report, we repeated the technique for both source and destination IP addresses.

Alert: WEB-IIS %E-asp access
Created 2004-11-18 11:49:16

Back to alerts index

timestamp	proto	src	srcport	dst	dstport	ethsrc	ethdst	ethlen	tcpflags	tcpseq	tcpack	tcpplen	tcpwindow	ttl	tos	id
15:13:07	TCP	10.8.0.72	1913	3.179.100.233	80	0:90:4B:2F:36:F6	0:9:58:39:B7:F4	0x18B	***AP***	0x414ABAED	0x8B14AFD5	0x40B0	128	0	55238	1
15:18:13	TCP	10.8.0.72	1978	3.179.100.233	80	0:90:4B:2F:36:F6	0:9:58:39:B7:F4	0x1C6	***AP***	0x6E7D8A9A	0xF593EF97	0x40B0	128	0	57902	4
15:21:46	TCP	10.8.0.72	1997	3.179.100.233	80	0:90:4B:2F:36:F6	0:9:58:39:B7:F4	0x1DD	***AP***	0x9132E162	0xD0E0E18EA	0x40B0	128	0	61713	4
15:23:17	TCP	10.8.0.72	2034	3.179.100.233	80	0:90:4B:2F:36:F6	0:9:58:39:B7:F4	0x1E3	***AP***	0x1D11E86	0xE4F810B3	0x40B0	128	0	64931	4
15:23:43	TCP	10.8.0.72	2040	3.179.100.233	80	0:90:4B:2F:36:F6	0:9:58:39:B7:F4	0x1E4	***AP***	0x4FAE2058	0xD450269E	0x40B0	128	0	65161	4
15:23:46	TCP	10.8.0.72	2040	3.179.100.233	80	0:90:4B:2F:36:F6	0:9:58:39:B7:F4	0x1E4	***AP***	0x4FAE2058	0xD450269E	0x40B0	128	0	65170	4
15:25:10	TCP	10.8.0.72	2047	249.22.121.140	80	0:90:4B:2F:36:F6	0:9:58:39:B7:F4	0x2BE	***AP***	0xFDC4EA1E	0xA710F551	0x40B0	128	0	591	6
15:25:11	TCP	10.8.0.72	2048	249.22.121.140	80	0:90:4B:2F:36:F6	0:9:58:39:B7:F4	0x354	***AP***	0x904257A6	0x2B0514CA	0x40B0	128	0	642	6
15:25:12	TCP	10.8.0.72	2049	249.22.121.140	80	0:90:4B:2F:36:F6	0:9:58:39:B7:F4	0x352	***AP***	0xA145E873	0xDA018649	0x40B0	128	0	692	6
15:25:15	TCP	10.8.0.72	2047	249.22.121.140	80	0:90:4B:2F:36:F6	0:9:58:39:B7:F4	0x2FB	***AP***	0xFDC4ECAF6	0xA7111421	0x40B0	128	0	886	7
15:25:17	TCP	10.8.0.72	2047	249.22.121.140	80	0:90:4B:2F:36:F6	0:9:58:39:B7:F4	0x358	***AP***	0xFDC4EAF68	0xA71117C45	0x40B0	128	0	1017	8
15:25:18	TCP	10.8.0.72	2051	249.22.121.140	80	0:90:4B:2F:36:F6	0:9:58:39:B7:F4	0x358	***AP***	0xA1C0C0A3	0xC8F20FE8	0x40B0	128	0	1047	8
15:25:18	TCP	10.8.0.72	2052	249.22.121.140	80	0:90:4B:2F:36:F6	0:9:58:39:B7:F4	0x3F8	***AP***	0x82B86D66	0xD42E0688	0x40B0	128	0	1063	1
15:25:18	TCP	10.8.0.72	2053	249.22.121.140	80	0:90:4B:2F:36:F6	0:9:58:39:B7:F4	0x3F8	***AP***	0xB67A47C7	0x76C7ECC4	0x40B0	128	0	1068	1
15:25:18	TCP	10.8.0.72	2054	249.22.121.140	80	0:90:4B:2F:36:F6	0:9:58:39:B7:F4	0x3F8	***AP***	0x5C7E7E2A	0x7DE68E72	0x40B0	128	0	1082	1
15:25:19	TCP	10.8.0.72	2055	249.22.121.140	80	0:90:4B:2F:36:F6	0:9:58:39:B7:F4	0x3F8	***AP***	0x2D66108E	0x5C73DD08	0x40B0	128	0	1097	1
15:25:21	TCP	10.8.0.72	2056	249.22.121.140	80	0:90:4B:2F:36:F6	0:9:58:39:B7:F4	0x358	***AP***	0x67962C8C	0x6D2533EA	0x40B0	128	0	1174	1
15:25:21	TCP	10.8.0.72	2052	249.22.121.140	80	0:90:4B:2F:36:F6	0:9:58:39:B7:F4	0x3F8	***AP***	0x82B86D66	0xD42E0688	0x40B0	128	0	1188	1
15:25:21	TCP	10.8.0.72	2057	3.179.5.21	80	0:90:4B:2F:36:F6	0:9:58:39:B7:F4	0x2B4	***AP***	0xAF4CF59E	0xAAA72AB	0x40B0	128	0	1215	1
15:25:21	TCP	10.8.0.72	2058	249.22.121.140	80	0:90:4B:2F:36:F6	0:9:58:39:B7:F4	0x25A	***AP***	0x93B6B9A9	0x6F58CDCA	0x40B0	128	0	1220	1
15:25:22	TCP	10.8.0.72	2059	249.22.121.140	80	0:90:4B:2F:36:F6	0:9:58:39:B7:F4	0x259	***AP***	0xD6494891	0x5B9A84CF	0x40B0	128	0	1251	1
15:25:22	TCP	10.8.0.72	2060	249.22.121.140	80	0:90:4B:2F:36:F6	0:9:58:39:B7:F4	0x24D	***AP***	0xBC86F2FC	0xD3B123A6	0x40B0	128	0	1283	1
15:25:25	TCP	10.8.0.72	2060	249.22.121.140	80	0:90:4B:2F:36:F6	0:9:58:39:B7:F4	0x24D	***AP***	0xBC86F2FC	0xD3B123A6	0x40B0	128	0	1399	1
15:25:26	TCP	10.8.0.72	2061	3.179.5.21	80	0:90:4B:2F:36:F6	0:9:58:39:B7:F4	0x369	***AP***	0xE6640008	0x3C354142	0x40B0	128	0	1430	1

Figure 7.1 Detailed Alert Messages

Snort Alerts by Destination IP Address
Created 2004-11-18 12:19:29

Destination IP Address	Alerts
239.255.255.250	3330
249.22.121.140	828
63.241.72.111	378
209.239.57.147	288
69.20.62.196	216
192.168.70.201	216
60.154.80.250	198
3.179.100.233	180
164.82.201.36	180
192.168.70.17	162
209.73.83.85	72
209.239.57.99	72
66.135.208.226	54
192.168.70.49	54
192.168.10.252	54
10.37.16.51	36
209.20.231.199	36
3.179.5.21	36
209.43.17.114	36
192.168.70.238	36
69.20.118.37	36
66.135.208.101	18
66.135.192.88	18
66.135.202.140	18
63.215.198.192	18
33.113.198.252	18

Figure 7.2 Snort Alerts by Destination IP Address

Alerts for destination IP: 63.241.72.111
Created 2004-11-18 12:19:31

Back to destination IP index

timestamp	msg	proto	src	srcport	dstport	ethsrc	ethdst	ethlen	tcpflags	tcpseq	tcpack	tc
15:31:16	WEB-IIS %2E-asp access	TCP	10.8.0.72	2227	80	0:90:4B:2F:36:F6	0:9:5B:39:B7:F4	0x2B4	***Ap***	0xF7B180BE	0x5B8A3D96	
15:31:20	WEB-IIS %2E-asp access	TCP	10.8.0.72	2231	80	0:90:4B:2F:36:F6	0:9:5B:39:B7:F4	0x2B9	***Ap***	0xC4296033	0x7F659DA0	
15:33:34	WEB-IIS %2E-asp access	TCP	10.8.0.72	2354	80	0:90:4B:2F:36:F6	0:9:5B:39:B7:F4	0x2B4	***Ap***	0xD0706403	0xF971E60B	
15:33:35	WEB-IIS %2E-asp access	TCP	10.8.0.72	2358	80	0:90:4B:2F:36:F6	0:9:5B:39:B7:F4	0x2B9	***Ap***	0x38A6EF07	0x6680227	
15:34:43	WEB-IIS %2E-asp access	TCP	10.8.0.72	2437	80	0:90:4B:2F:36:F6	0:9:5B:39:B7:F4	0x2A4	***Ap***	0x9E488ECB	0x330305DE	
17:00:11	WEB-MISC weblogic/tomcat .jsp view source attempt	TCP	10.8.0.72	3898	80	0:90:4B:2F:36:F6	0:9:5B:39:B7:F4	0x28A	***Ap***	0xE5D77F	0xA5E4DA0B	
17:00:16	WEB-MISC weblogic/tomcat .jsp view source attempt	TCP	10.8.0.72	3901	80	0:90:4B:2F:36:F6	0:9:5B:39:B7:F4	0x309	***Ap***	0xA4E32019	0xC7127C3D	
17:00:30	WEB-MISC weblogic/tomcat .jsp view source attempt	TCP	10.8.0.72	3903	80	0:90:4B:2F:36:F6	0:9:5B:39:B7:F4	0x2EC	***Ap***	0xA163CE1	0x5461464F	
17:00:32	WEB-MISC weblogic/tomcat .jsp view source attempt	TCP	10.8.0.72	3904	80	0:90:4B:2F:36:F6	0:9:5B:39:B7:F4	0x39F	***Ap***	0x14210772	0x748F2DDF	
17:00:37	WEB-MISC weblogic/tomcat .jsp view source attempt	TCP	10.8.0.72	3909	80	0:90:4B:2F:36:F6	0:9:5B:39:B7:F4	0x353	***Ap***	0xED2D1358	0xAEBE9961	
17:00:37	WEB-MISC weblogic/tomcat .jsp view source attempt	TCP	10.8.0.72	3913	80	0:90:4B:2F:36:F6	0:9:5B:39:B7:F4	0x3C3	***Ap***	0x87E0DAD6	0x71E72A91	
17:01:00	WEB-MISC weblogic/tomcat .jsp view source attempt	TCP	10.8.0.72	3920	80	0:90:4B:2F:36:F6	0:9:5B:39:B7:F4	0x325	***Ap***	0xF56840CB	0xE2BC37	
17:01:01	WEB-MISC weblogic/tomcat .jsp view source attempt	TCP	10.8.0.72	3921	80	0:90:4B:2F:36:F6	0:9:5B:39:B7:F4	0x3EA	***Ap***	0x91FC7438	0x8166FF10	
17:01:30	WEB-MISC weblogic/tomcat .jsp view source attempt	TCP	10.8.0.72	3927	80	0:90:4B:2F:36:F6	0:9:5B:39:B7:F4	0x33D	***Ap***	0x507031F1	0xB197F470	
17:01:31	WEB-MISC weblogic/tomcat .jsp view source attempt	TCP	10.8.0.72	3928	80	0:90:4B:2F:36:F6	0:9:5B:39:B7:F4	0x40A	***Ap***	0xA919407F	0xC7807A43	
17:01:47	WEB-MISC weblogic/tomcat .jsp view source attempt	TCP	10.8.0.72	3931	80	0:90:4B:2F:36:F6	0:9:5B:39:B7:F4	0x359	***Ap***	0x5187349D	0xB8868268	
17:02:13	WEB-MISC weblogic/tomcat .jsp view source attempt	TCP	10.8.0.72	3934	80	0:90:4B:2F:36:F6	0:9:5B:39:B7:F4	0x386	***Ap***	0x30E0C5C7	0x557FF7F3	
17:02:13	WEB-MISC weblogic/tomcat .jsp view source attempt	TCP	10.8.0.72	3935	80	0:90:4B:2F:36:F6	0:9:5B:39:B7:F4	0x443	***Ap***	0xE6D3AE82	0x8A062746	
17:02:58	WEB-MISC weblogic/tomcat .jsp view source attempt	TCP	10.8.0.72	3936	80	0:90:4B:2F:36:F6	0:9:5B:39:B7:F4	0x358	***Ap***	0x1B6C48D	0xA061AC02	
17:03:03	WEB-MISC weblogic/tomcat .jsp view source attempt	TCP	10.8.0.72	3938	80	0:90:4B:2F:36:F6	0:9:5B:39:B7:F4	0x59A	***Ap***	0x664E63AA	0x3E1C122	
17:03:06	WEB-MISC weblogic/tomcat .jsp view source attempt	TCP	10.8.0.72	3938	80	0:90:4B:2F:36:F6	0:9:5B:39:B7:F4	0x59A	***Ap***	0x664E63AA	0x3E1C122	
15:31:16	WEB-IIS %2E-asp access	TCP	10.8.0.72	2227	80	0:90:4B:2F:36:F6	0:9:5B:39:B7:F4	0x2B4	***Ap***	0xF7B180BE	0x5B8A3D96	
15:31:20	WEB-IIS %2E-asp access	TCP	10.8.0.72	2231	80	0:90:4B:2F:36:F6	0:9:5B:39:B7:F4	0x2B9	***Ap***	0xC4296033	0x7F659DA0	
15:33:34	WEB-IIS %2E-asp access	TCP	10.8.0.72	2354	80	0:90:4B:2F:36:F6	0:9:5B:39:B7:F4	0x2B4	***Ap***	0xD0706403	0xF971E60B	
15:33:35	WEB-IIS %2E-asp access	TCP	10.8.0.72	2358	80	0:90:4B:2F:36:F6	0:9:5B:39:B7:F4	0x2B9	***Ap***	0x38A6EF07	0x6680227	

Figure 7.3 IP Address Details

At this point, you can run the entire report with these Log Parser commands:

```
logparser.exe file:Ch11Alerts-Index.sql -i:csv -
iHeaderFile:AlertHeader.csv -
```

```
iTsFormat:mm/dd/yy-hh:mm:ss -headerRow:off -o:tpl -tpl:Ch11Alerts-
Index.tpl
```

```
logparser.exe file:Ch11Alerts-DetailHeader.sql -i:csv -
```

```
iHeaderFile:AlertHeader.csv -iTsFormat:mm/dd/yy-hh:mm:ss -
headerRow:off -o:tpl
```

```
-tpl:Ch11Alerts-DetailHeader.tpl
```

```
logparser.exe file:Ch11Alerts-Detail.sql -i:csv -
iHeaderFile:AlertHeader.csv -
```

```
iTsFormat:mm/dd/yy-hh:mm:ss -headerRow:off -o:tpl -tpl:Ch11Alerts-
Detail.tpl -
```

```
fileMode:0
```

```
logparser.exe file:Ch11SrcIP-Index.sql -i:csv -
iHeaderFile:AlertHeader.csv -
```

```
iTsFormat:mm/dd/yy-hh:mm:ss -headerRow:off -o:tpl -tpl:Ch11SrcIP-
Index.tpl
```

```
logparser.exe file:Ch11SrcIP-DetailHeader.sql -i:csv -
```

```
iHeaderFile:AlertHeader.csv -iTsFormat:mm/dd/yy-hh:mm:ss -
headerRow:off -o:tpl
```



```
-tpl:Ch11SrcIP-DetailHeader.tpl
```

```
logparser.exe file:Ch11SrcIP-Detail.sql -i:csv -  
iHeaderFile:AlertHeader.csv -
```

```
iTsFormat:mm/dd/yy-hh:mm:ss -headerRow:off -o:tpl -tpl:Ch11SrcIP-  
Detail.tpl -
```

```
fileMode:0
```

```
logparser.exe file:Ch11DstIP-Index.sql -i:csv -  
iHeaderFile:AlertHeader.csv -
```

```
iTsFormat:mm/dd/yy-hh:mm:ss -headerRow:off -o:tpl -tpl:Ch11DstIP-  
Index.tpl
```

```
logparser.exe file:Ch11DstIP-DetailHeader.sql -i:csv -
```

```
iHeaderFile:AlertHeader.csv -iTsFormat:mm/dd/yy-hh:mm:ss -  
headerRow:off -o:tpl
```

```
-tpl:Ch11DstIP-DetailHeader.tpl
```

```
logparser.exe file:Ch11DstIP-Detail.sql -i:csv -  
iHeaderFile:AlertHeader.csv -
```

```
iTsFormat:mm/dd/yy-hh:mm:ss -headerRow:off -o:tpl -tpl:Ch11DstIP-  
Detail.tpl -
```

```
fileMode:0
```

We may wish to create a summary index page now that we have a thorough alert report. This page should provide access to detailed reports as well as graphs and data summaries to provide a rapid overview of the network.

```
---Ch11Summary-Index.sql---
```

```
SELECT TOP 10
```

```
sig_id,
```

```
msg,
```

```
Count(msg) as Alerts
```

```
INTO report\index.html
```

```
FROM alert.csv
```

```
GROUP BY msg, sig_id
```

```
ORDER BY Alerts DESC
```

```
---Ch11Summary-Index.sql---
```

The query for the pie graph is similar, but does not include the actual message, and this time processes all records:

```
---Ch11Summary-GraphTopAlerts.sql---
```

```
SELECT  
sig_id,  
Count(msg) as Alerts  
INTO report\AlertsTopAlerts.gif  
FROM alert.csv  
GROUP BY sig_id  
ORDER BY Alerts DESC
```

```
---Ch11Summary-GraphTopAlerts.sql---
```

Finally, there are three queries for the remaining graphs:

```
---Ch11Summary-GraphTopSrcIPs.sql---
```

```
SELECT  
src,  
Count(msg) as Alerts  
INTO report\AlertsTopSrcIPs.gif  
FROM alert.csv  
GROUP BY src  
ORDER BY Alerts DESC
```

```
---Ch11Summary-GraphTopSrcIPs.sql---
```

```
---Ch11Summary-GraphAlertsPerHour.sql---
```

```
SELECT  
Count(*) as Alerts  
USING QUANTIZE(timestamp,360) as Hour  
INTO report\AlertsByHour.gif  
FROM alert.csv  
GROUP BY Hour
```

```
---Ch11Summary-GraphAlertsPerHour.sql---
```

```
---Ch11Summary-GraphTopDstPorts.sql---
```

```
SELECT TOP 5
```

```
STRCAT(STRCAT(TO_STRING(dstport),' - '), proto) AS Destination,
```

```
Count(*) as Alerts
```

```
USING dst as DestinationPort
```

```
INTO report\AlertsTopDstPorts.gif
```

```
FROM alert.csv
```

```
GROUP BY Destination
```

```
ORDER BY Alerts DESC
```

```
---Ch11Summary-GraphTopDstPorts.sql---
```

Finally, we can generate the entire index page with these commands:

```
logparser.exe file:Ch11Summary-Index.sql -i:csv -
```

```
iHeaderFile:AlertHeader.csv -
```

```
iTsFormat:mm/dd/yy-hh:mm:ss -headerRow:off -o:tpl -
```

```
tpl:Ch11Summary-Index.tpl
```

```
logparser.exe file:Ch11Summary-GraphTopAlerts.sql -i:csv -
```

```
iHeaderFile:AlertHeader.csv -iTsFormat:mm/dd/yy-hh:mm:ss -
```

```
headerRow:off -
```

```
o:chart -chartType:Pie3D -groupSize:350x190 -values:OFF -chartTitle:""
```

```
-categories:OFF
```

```
logparser.exe file:Ch11Summary-GraphTopSrcIPs.sql -i:csv -
```

```
iHeaderFile:AlertHeader.csv -iTsFormat:mm/dd/yy-hh:mm:ss -
```

```
headerRow:off -
```

```
o:chart -chartType:Pie -groupSize:300x150 -values:OFF -chartTitle:"" -
```

```
categories:OFF
```

```
logparser.exe file:Ch11Summary-GraphAlertsPerHour.sql -i:csv -
```

```
iHeaderFile:AlertHeader.csv -iTsFormat:mm/dd/yy-hh:mm:ss -
```

```
headerRow:off -
```

```
o:chart -chartType:smoothline -groupSize:300x150 -values:OFF -
```

```
chartTitle:"" -categories:OFF
```

```
logparser.exe file:Ch11Summary-GraphTopDstPorts.sql -i:csv -  
iHeaderFile:AlertHeader.csv -iTFormat:mm/dd/yy-hh:mm:ss -  
headerRow:off -  
o:chart -chartType:BarStacked -groupSize:300x150 -values:OFF -  
chartTitle:""
```

The final result is a fully interactive IDS report using nothing more than Log Parser.

7.3.6 Monitoring User Activity

The forensic process necessitates the monitoring of user activities. Unusual user behaviour could be a symptom of a larger problem with the system, or it could be a genuine security risk. You can identify authentication issues and hacking activity by looking at the user activity reported in your system logs.

Identifying which activities are innocuous and which behaviour indicates trouble is an important part of detecting meaningful events in your system logs. If a user fails to authenticate once a week, for example, you may be very assured that the user merely mistyped his or her password and is not attempting to attack your system. Alternatively, if a user has two unsuccessful authentication attempts every hour for a long time, you should investigate more. Tools like Log Parser can help you spot occurrences that could signal a hacking attempt or even a user looking at something he or she shouldn't be looking at. You may also hunt out any security concerns at the file level by activating file access auditing and utilising Log Parser to analyse the data. With the enhanced capabilities of Microsoft's Log Parser software, manually digging through these same log files to search down this data is both onerous and wasteful.

7.3.6.1 Tracking Authentication Failures

It's always crucial to know how many unsuccessful authentication attempts have happened while performing regular security audits of your servers. This aids you in a variety of ways. To begin with, you can identify individual users who have lost their password and have not requested a new one. Second, and more crucially, by evaluating the results and noting an increase in failed logon attempts for a single user or numerous users, you may be able to discover probable hacking efforts against your server. Finally, you might be able to pinpoint system issues that are causing many users to fail to authenticate at the same time. These issues could be caused by a failure of an authentication server, network connectivity, or system utilisation.

Listing Failed Logons

Return to the Log Parser to discover how simply your event logs can be used to detail out failed logons over a given timeframe. The following command and query can be used to list all failed logons on a specific date:

```
logparser.exe file:Ch11ListingFailedLogons.sql -i:EVT -o:datagrid
```

```
--- Ch11ListingFailedLogons.sql ---
```

```
SELECT
```

```
timegenerated AS LogonTime,
```

```
extract_token(strings, 0, '|') AS UserName
```

```
FROM Security
```

```
WHERE EventID IN (529;
```

```
530;
```

```
531;
```

```
532;
```

```
533;
```

```
534;
```

```
535;
```

```
537;
```

```
539)
```

```
AND to_string(timegenerated,'yyyy-MM-dd HH:mm:ss') like '2004-09%'
```

```
--- Ch11ListingFailedLogons.sql ---
```

You may view how many authentication failures occurred on the date you specified, as well as which user IDs had difficulties, by performing this query.

We start by declaring that we want to get the timestamp for the event from the time generated field in this query. The query then becomes a little more difficult than usual. When an unsuccessful logon occurs, the event's UserID is always SYSTEM. We need to extract some data from the description or *strings* fields in order to determine the exact ID that the logon attempt was made with. To do so, we use the EXTRACT TOKEN function to tokenize the text and specify that we want the first or 0 token, which is the UserName.

We then specify that we want this data to be pulled from the current Security log. We utilise the WHERE clause to filter our data to a certain set of security events that signal logon failures. Table 7.1 gives a full account of each of these occurrences. We specify the date stamp we're seeking for in the WHERE clause in the same way that we did in the previous query. We also need to specify the input and output format, so we add this to the end of the command line using the syntax **-i:EVT -o:datagrid**.

Table 7.1 Failed Logon EventIDs

EventID	Description
529	The logon attempt was made with an unknown username or a knownusername with a bad password.
530	The user account tried to log on outside the allowed time.
531	A logon attempt was made by using a disabled account.
532	A logon attempt was made by using an expired account.
533	The user is not allowed to log on at this computer.
534	The user attempted to log on with a logon type that is not allowed, suchas network, interactive, batch, service, or remote interactive.
535	The password for the specified account has expired.
537	The logon attempt failed for other reasons.
539	The account was locked out at the time the logon attempt was made.

This event is logged when a user or computer attempts to authenticate with an account that has been previously locked out.

Identifying Single versus Multiple Failed Logons

When dealing with unsuccessful logons, it's occasionally useful to be able to rapidly determine how common logon failures are over time. We covered how to list failed logons in the previous section, but using this query requires manually determining how frequently a given user ID has problems.

Using a slightly different query, you can use Log Parser to automatically count the number of failed logons for each user. One example of how this can be done is using the command and query below:

```
logparser.exe file:Ch11SingleVsMltplFailedLogons.sql -i:EVT -o:datagrid
```

```
--- Ch11SingleVsMltplFailedLogons.sql ---
```

```
SELECT
```

```
extract_token(strings, 0, '|') AS UserName,
```

```
count(*) AS Number_of_Events
```

```
FROM Security
```

WHERE EventID IN

(529;

530;

531;

532;

533;

534;

535;

537;

539)

AND to_string(timegenerated,'yyyy-MM-dd HH:mm:ss') like '2004-09%'

GROUP BY UserName

HAVING Number_of_Events>2

--- Ch11SingleVsMltplFailedLogons.sql ---

We're doing a little more work up front with this query, but we're decreasing the manual effort required to find repeated login failures. We begin by using the EXTRACT TOKEN function to extract the real userid associated with the failed logon. The number of occurrences is then counted and the result is displayed as the Number of Events. We then select the Security event log as our data source and add a WHERE clause that specifies the events we want to monitor as well as the date range for which we want the data.

Finally, we add a HAVING statement and a GROUP BY statement to order our findings. We specify Number of Events>2 in the HAVING statement to limit the data to only show us data from events that occur numerous times.

7.3.6.2 Identifying Brute Force Attacks

The likelihood of a brute force attack on your system is a key worry when it comes to system security. The way in which an attack happens is the decisive factor in whether or not it is a brute force attack. When an attacker makes attempt after attempt to carry out a certain attack action, the entire event is classified as a brute force attack since the attacker is attempting to break into the system via brute force. The Log Parser can assist you in swiftly analysing your security event logs to see if one of these brute force attacks is taking place. You might be able to block a brute force attack before it succeeds if you create queries that watch for the behaviour of a brute force attack.

Identifying a Brute Force Authentication Attack

Investigating Network Traffic
and Investigating Logs

Someone attempting to guess the password for one of your users is an excellent example of a brute force attack. Let's imagine the attacker knows from past experience that you have a policy in place that disables an account if the same UserID makes three unsuccessful logon attempts within a one-hour span. Given this, the attacker will not risk locking out the account he or she is attempting to hack. However, the attacker will want to make the most of his or her limited time by launching as many attacks as possible in a given amount of time.

Using the same query outlined previously for discovering multiple unsuccessful logons is an easy approach to check for this type of activity. This query, with a little tweaking, can run an intelligent scan for brute force logon attempt behaviour. The original query is as follows:

```
logparser.exe file:Ch11SingleVsMltplFailedLogons.sql -i:EVT -o:datagrid
```

```
--- Ch11SingleVsMltplFailedLogons.sql ---
```

```
SELECT
```

```
extract_token(strings, 0, '|') AS UserName,
```

```
count(*) AS Number_of_Events
```

```
FROM Security
```

```
WHERE EventID IN (529;
```

```
530;
```

```
531;
```

```
532;
```

```
533;
```

```
534;
```

```
535;
```

```
537;
```

```
539)
```

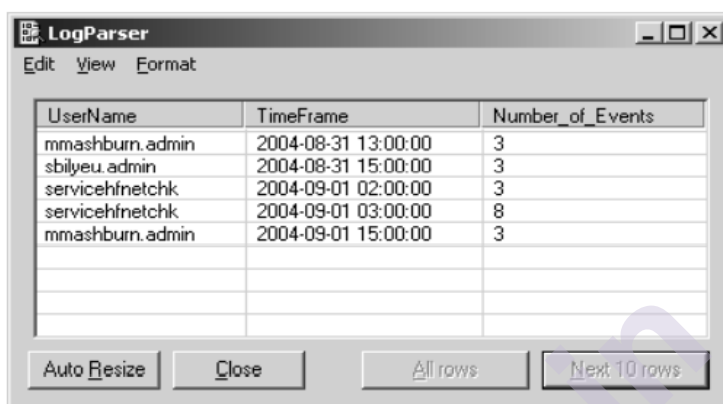
```
GROUP BY UserName,
```

```
Timeframe
```

```
HAVING Number_of_Events>2
```

```
--- Ch11BruteForceAttack.sql ---
```

The elimination of the date search and the inclusion of a TimeFrame value based on the quantized time—generated field were the only meaningful modifications to this query. When we perform this query, we'll get a datagrid with the number of failure occurrences for each username over the course of an hour. A brief glance at the results in Figure 7.4 reveals the accounts that may be under attack by brute force. When this type of behaviour is discovered, following up with the user to learn more about what is going on is a good idea.



The screenshot shows the LogParser application window with a menu bar (Edit, View, Format) and a table of results. The table has three columns: UserName, TimeFrame, and Number_of_Events. The data is as follows:

UserName	TimeFrame	Number_of_Events
mmashburn.admin	2004-08-31 13:00:00	3
sbilyeu.admin	2004-08-31 15:00:00	3
servicehfnetchk	2004-09-01 02:00:00	3
servicehfnetchk	2004-09-01 03:00:00	8
mmashburn.admin	2004-09-01 15:00:00	3

At the bottom of the window are four buttons: Auto Resize, Close, All rows, and Next 10 rows.

Figure 7.4 Brute Force Activity

7.3.6.3 Tracking Security Policy Violations

Most businesses have some sort of security policy in place to address issues such as account and password security, permissible system access, undesirable behaviour, and so on. These policies specify the particular rules that each user must follow when accessing information technology (IT) systems.

A Regular audit is a beneficial activity that admins often do to ensure that corporate security standards are followed. The Windows event logs contain some of the information needed for this type of audit. Tracking user logons for desktop systems is a fantastic example. You can identify whether or not users are violating a policy requiring them to log on to just one machine at a time by combining all of your event log data from many systems and sifting through it with Log Parser.

Determining Logon/Logoff Behavior

Determining if users frequently log off after their work day or leave their systems logged in is another example that does not involve log correlation. This activity is documented as a breach of some firms' corporate security policies. To get this information with Log Parser, we'll need to first figure out all of the logoff events, then see whether there's a logon event for the same day that doesn't have an accompanying logoff event for the same SID. The following command and query can help us determine this behavior:

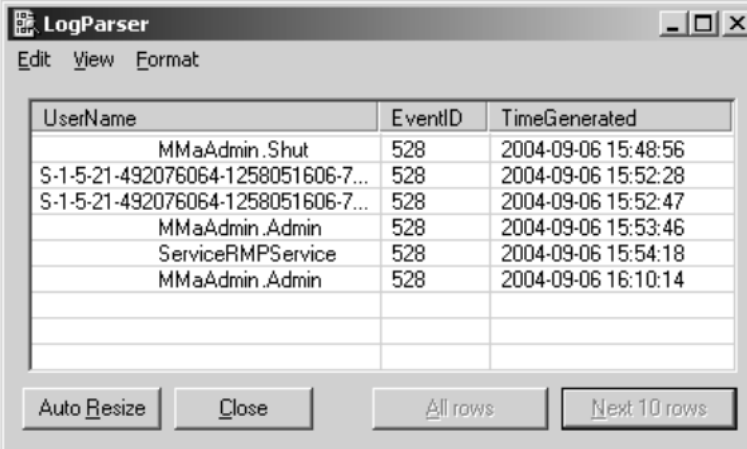
```
logparser.exe file:Ch11LogonLogoffBehavior.sql -i:EVT -o:datagrid
```

```
--- Ch11LogonLogoffBehavior.sql ---
```

```
SELECT
resolve_sid(sid) AS UserName,
eventid,
timegenerated
FROM Security
WHERE eventid='528'
AND to_date(timegenerated)='2004-09-06 00:00:00'
AND sid not in
(
SELECT DISTINCT
sid
FROM Security
WHERE eventid='538'
AND to_date(timegenerated)='2004-09-06 00:00:00'
)
--- Ch11LogonLogoffBehavior.sql ---
```

To retrieve the information we need in this query, we'll have to work backwards a little bit. We start by deciding whatever data we want to include in our report. We should collect the userID, the eventID we're dealing with, and the time the event occurred in this scenario. The security event log will then be used as our data source.

The more challenging element of this query is constructing the WHERE clause. The first two criteria are very straightforward; for a successful logon, the eventID must be 528, and the date for which we want information must be given. To limit our incoming data, we'll need to conduct a select within a select. We're looking for data in which the SID associated with the 528 event does not appear in a query of the 538 events on the same day. Figure 7.5 is an example of what you should expect.



UserName	EventID	TimeGenerated
MMaAdmin.Shut	528	2004-09-06 15:48:56
S-1-5-21-492076064-1258051606-7...	528	2004-09-06 15:52:28
S-1-5-21-492076064-1258051606-7...	528	2004-09-06 15:52:47
MMaAdmin.Admin	528	2004-09-06 15:53:46
ServiceRMPService	528	2004-09-06 15:54:18
MMaAdmin.Admin	528	2004-09-06 16:10:14

Figure 7.5 Logon Events with No Logoff Event

We can isolate those users who have signed on at some time during a specific day but have no associated logoff event for that day by running our query this way. Because it does not account for the possibility of numerous logon/logoff events for each user in a single day, it will not catch all users that log on without logging out. It can, however, help to reduce the number of such security policy infractions.

Auditing Successful and Unsuccessful File Access Attempts

The audit log for successful and unsuccessful file access attempts is another crucial metric to analyse when looking at overall system security. Individual files or directories can be audited at the file system level with NTFS (NT file system). This enables you, as an administrator, to assess whether or not critical data has been accessed or attempted to be accessed.

File access auditing is frequently deactivated because the audit logs create so much data that sorting through it and extracting events that are crucial to be aware of is nearly impossible. This is where Log Parser may assist you in your attempts to keep your systems secure.

Auditing Unsuccessful File Access Attempts

When NTFS object auditing is enabled, Windows adds events to the Security event log to show which objects are accessed. The object that was accessed, the person that accessed the object, and the date/time the object was accessed are all logged as part of this event entry. You may rapidly collect the events surrounding these object access attempts with Log Parser.

Obviously, the items that a user tries to access while they aren't supposed to are of greater importance to administrators. This usually results in an unsuccessful file access attempt with effective security implementation. You can rapidly discover these occurrences and export them for study by scanning through the security logs with Log Parser. The following command and query will find all of the failed file access events in your security log:

```
logparser.exe file:Ch11UnsuccessfulFileAccess.sql -i:EVT -o:datagrid
```

```
--- Ch11UnsuccessfulFileAccess.sql ---
```

```
SELECT
```

```
timegenerated AS EventTime,
```

```
extract_token(strings, 8, '|') AS UserName,
```

```
extract_token(strings, 2, '|') AS File
```

```
FROM Security
```

```
WHERE EventID = '560'
```

```
AND EventType = 'Failure Audit event'
```

```
AND extract_token(strings, 1, '|') like 'File'
```

```
--- Ch11UnsuccessfulFileAccess.sql ---
```

When this query executes, it searches the security log for events with the eventID 560 (Success Audit), but it narrows down the results to events with the type Failure Audit. It also checks the accompanying event description to make sure we're only looking at files and not directories. The Log Parser pulls the event time, the username connected with the event, and the filename from that subset. All of this information is then presented in a datagrid format. You can go one step further and have Log Parser export the data to an XML file or another format for evidence gathering purposes.

Auditing Successful File Access Attempts

Many administrators neglect to keep track of both successful and unsuccessful file access attempts. Although failures are the most significant events to watch for, it's equally vital not to overlook the auditing tools provided for successful file access attempts.

A scenario in which this can be used would be beneficial. Let's pretend you work as an administrator for a huge corporation with a legal department. The department is now putting together some information for a highly important case, which is being stored on the department's shared drive. During the course of events, word reaches the legal department that the opposing legal department has gotten a hold of the approach that your company's legal department was planning to utilise and is putting together a counterattack. Members of the legal department should have been the only ones with access to the files containing this information. They ask you to track down who has accessed those files.

You've already enabled successful file access auditing for the legal department's shared drive if you've planned ahead for this possibility. You may easily extract the information that the legal department requires and

send it to them fast using Log Parser. The following script demonstrates how to accomplish this:

```
logparser.exe file:Ch11SuccessfulFileAccess.sql -i:EVT -o:datagrid  
--- Ch11SuccessfulFileAccess.sql ---  
  
SELECT  
  
timegenerated AS EventTime,  
  
extract_token(strings, 8, '|') AS UserName,  
  
extract_token(strings, 2, '|') AS File  
  
FROM Security  
  
WHERE EventID = '560'  
  
AND EventType = 'Success Audit event'  
  
AND extract_token(strings, 1, '|') like 'File'  
  
--- Ch11SuccessfulFileAccess.sql ---
```

If you examine the code closely, you'll notice that it's nearly identical to the earlier script you saw for auditing failed file access attempts. The only actual distinction is the name of the event type. We're now looking for a "Success Audit event" instead of a "Failure Audit event." When you run this script, it will extract all of your security log's successful file access events. To reduce the quantity of data to go through, you may narrow the search to check for occurrences that occur with a specified directory path or filename.

7.4 SUMMERY

Security admins need to understand the purpose behind capturing and analyzing log files. If done right, these tools will provide you with a very good look at our network's security. They can help you notice issues much faster than you might if they're used correctly. The aim is to be able to see things that we would have trouble seeing ourselves. Many log management devices are designed to be used as an audit or compliance tool.

Many manufacturers include thorough audit and compliance information, which is a dream come true for auditors. Log management tools can also help you track down violations and recover your losses in court.

Many attacks go unnoticed until they've already happened. According to security expert John O'Hare, many forensic specialists don't make full use of log and audit data because they don't know how to access it or because scrolling through thousands of log file entries takes a long time.

7.5 REFERENCES FOR FURTHER READING

Investigating Network Traffic
and Investigating Logs

Chapter 9 - Investigating Network Traffic and Investigating Logs,
Editor(s): Dave Kleiman, Kevin Cardwell, Timothy Clinton, Michael
Cross, Michael Gregg, Jesse Var Salone, Craig Wright, The Official CHFI
Study Guide (Exam 312-49), Syngress, 2007, Pages 441-467, ISBN
9781597491976, <https://doi.org/10.1016/B978-159749197-6.50010-9>.



munotes.in

INVESTIGATING WIRELESS AND WEB ATTACKS

Unit Structure

8.0 Objective

8.1 Introduction

8.1.1 Basics of Wireless

8.1.2 Advantages of a Wireless Network

8.1.3 Disadvantages of a Wireless Network

8.1.4 Association of Wireless AP and a Device

8.1.5 MAC Filtering

8.1.6 Cloaking the SSID

8.2 Wireless Penetration Testing

8.2.1 Direct Connections to Wireless Access Point

8.2.2 Scanning for Wireless Access Points with Nmap

8.2.3 Scanning for Wireless Access Points with Nessus

8.2.4 Rogue Access Points

8.2.5 Information Gathering

8.2.6 Passive and Active Sniffing

8.2.7 Investigating Web Attacks

8.3 Summary

8.4 References for further reading

8.0 OBJECTIVE

When we are working in wireless network we must understand:

- The basics of wireless network and advantages and disadvantages of it.
- The security risk in wireless network.
- The examples of vulnerability and methods to protect your network.

Wireless devices are expanding the network perimeter beyond the boundaries of the office walls and into neighbouring buildings and public streets in many corporate networks across the country. Attackers are no longer required to break into an office or seek to circumvent strong firewall measures in order to get network access. They can now take advantage of a corporation that is unaware that its wireless infrastructure security is so weak that it can be hacked in under 15 minutes.

You've probably heard stories about hackers waiting in cars with a laptop and a powerful wireless antenna, looking for insecure wireless networks to break into. These hackers could be hunting for internal corporate intellectual property to sell to a competitor or data that could be used for extortion or blackmail. The more difficult you make it for the attacker, the more likely he will abandon your network in favour of one that is less secure.

Wireless attacks are taking place! Wireless networks have been compromised at BJ's Wholesale Club, Lowe's Companies Inc., DSW, Wake Forest University School of Medicine, and TJX. The true cost of these data breaches could be in the millions of dollars, but it's difficult to estimate because we have to factor in the money spent by the company to investigate the problem, compensate the victims, fix the vulnerabilities, and account for lost revenue due to low consumer confidence. An attacker may attempt to hack your wireless network regardless of how complex your architecture is.

It's no longer a question of "if," but "when" your wireless network will be attacked. Attempts to join your wireless network from the outside can range from basic automatic device pairings to targeted attacks. It can be difficult to tell whether someone is trying to break into your network or is just looking for a free Internet connection. Regardless of their motivation, you should make every attempt to keep your wireless network as safe as possible. You may reduce your risk by configuring strong encryption and following safe wireless best practices.

As the cost of deploying wireless networks continues to fall, an increasing number of businesses are considering doing so. Since 2006, London has witnessed a 160 percent increase in wireless access points, while New York has seen a 49 percent increase. However, data isn't required to see that wireless networks are becoming increasingly prevalent. When you open your wireless settings user interface, you should see three or four networks in the immediate vicinity. This number might be as high as 15 to 20 if you reside in the city. There are various benefits to deploying a wireless network. Workers may now connect to their company's network from everywhere in the building, from the cafeteria to the conference room, without having to reconfigure their laptops or plug them into a wall jack. This flexibility is advantageous to both the employee and the employer. Installing network wiring throughout the facility is often far more expensive than implementing a wireless solution. This chapter

covers the fundamentals of wireless networks as well as the tactics used by hackers to attack them. It's critical that you understand how hackers operate so that you can test your wireless networks for flaws. Because of their anonymity and the difficulties of tracing down attacks, hackers have an advantage when it comes to wireless attacks. Because once a hacker breaks in, they're on the internal network, bypassing many of the usual network security barriers. The attack surface is enormous and the results are enticing.

8.1.1 Basics of Wireless

A wireless access point connects a typical wired network to wireless clients by transmitting network data through the air. Between the wired network and wireless clients, the wireless access point serves as a relay. Many businesses have multiple wireless access points that may hand off the wireless signal to keep clients connected. These access points range in price from under a hundred dollars for home or home office devices to thousands of dollars for enterprise access points with advanced security features and specialist configuration and management.

Wireless access points merely offer a conduit for data to move from the wired network to the client. Client network infrastructure services must still be provided. While most access points now have these functions built in, you may still use your traditional servers to deliver services like DHCP and routing. There are several types of wireless networks, the most prevalent of which is 802.11 b/g. The 802.11b wireless standard was the first to be designed for commercial usage. It transmits data at a rate of 11 megabits per second and runs at 2.4GHz (Mbps). 802.11g was a welcome enhancement for users who wanted greater throughput from their wireless infrastructure, increasing data transfer to 54 Mbps. Although interference concerns were common in the 2.4GHz band, backwards compatibility and early acceptance helped this combination become the industry standard for wireless devices.

802.11a, which works on the 5GHz frequency, was released for companies who needed less interference or couldn't embrace the 2.4GHz band as an acceptable solution. While maintaining the 54-Mbps transfer rate, 802.11a improved wireless stability by minimising failed connections. The cost of upgrading both the wireless access points and the client's wireless cards to devices that support this standard is the biggest disadvantage. Wireless devices can also connect two distant places by using line-of-sight antennas to convey data from one point to another when a cable would be impossible to establish. Instead of paying the recurring expense of a typical T1 line, a company with a second building less than a mile from the main facility may choose to implement a line-of-sight wireless solution for Internet connectivity.

To connect wirelessly to a LAN, a client must have a wireless network card that is compliant with the destination network's wireless standard. Wireless networks are becoming a commonplace in most household and corporate networks, with the majority of laptops now containing built-in

network devices. While wireless LANs have typically been used for mobile devices, several businesses are now installing wireless cards on their desktop computers due to the ease and cost-effectiveness of extending the network.

Even with all of the advances in recent years, creating a wireless network on your LAN should not be undertaken without careful consideration. Before incorporating wireless connectivity into your network, you should be aware of the primary benefits and drawbacks of doing so.

8.1.2 Advantages of a Wireless Network

Wireless networks offer users the following advantages:

- **Ease of accessing the network:** Employees are no longer restricted to regions where they can connect to the network via a wall jack. The ability to connect your laptop to the network from any location in the building gives you additional flexibility.
- **Reduce cost of running cable:** When compared to the cost of purchasing and installing a wireless device and cards, the labour cost of wiring an office or office building might be fairly significant. With the availability of wireless cards for desktop PCs, a workplace may be network ready in minutes.
- **Productivity :** Employees can now bring their laptops to meetings or any other location where they are needed to work and continue to do so.

8.1.3 Disadvantages of a Wireless Network

Wireless networks also have some disadvantages as well:

- **Security:** Wireless's biggest problem is its lack of security. Any wireless network can be readily attacked if adequate planning and configuration are not taken into account.
- **Complexity and reliability:** While adding wireless access points improves the wired network's accessibility, it also increases the network's complexity. Wireless devices have an impact on the network. Therefore, system administrators must be aware of this and address issues like weak signals and failed wireless connections.
- **Network performance :** While a wireless connection's claimed speed is 54 Mbps, the real data throughput is frequently substantially lower, especially when multiple PCs are utilising the same wireless connection. A wired network connection will nearly always perform better than a wireless connection.

8.1.4 Association of Wireless AP and a Device

The client must be associated with the access point in order to send and receive data over a wireless connection. This connection establishes a link between the two devices, allowing the client to obtain an IP address and communicate across the network. The affiliation procedure can be

hampered by signal strength and security settings. Microsoft provides the Windows Wireless Zero Configuration (WZC) programme for the Windows XP and Windows Server operating systems to aid users in connecting to wireless networks.

While it simplifies the registration process, it also raises several security risks that you should be aware of. WZC will query for networks that are already connected if a preferred network is not available. Anyone with a wireless analyser may see this data, which can be exploited to create bogus access points to entice clients to connect. WZC will also try to connect to the strongest wireless network available. Knowing this, an attacker can employ high-power antennas to build phoney wireless networks, causing machines to connect to their access point rather than the authentic one. It is advised that you utilise the wireless administration tool provided by the manufacturer whenever possible. If you're using a wireless card from Linksys, Dell, or Netgear, you've probably installed management software from the manufacturer to regulate the wireless device's association.

This software is often more secure because it was created by the manufacturer to interact with the associated hardware. Selecting the wireless network to which you want to connect is a requirement of any wireless management applications. The Service Set Identifier will be chosen (SSID). The SSID is the wireless network's public name. If security is enabled on the network, you will be asked to enter a password or encryption key. You will not be permitted access to the network if you do not know the key. Your computer will try to join the network if it is open or if you enter the relevant security key. Controlling Access To make the wireless network as secure as possible, security controls can be put in place to limit an attacker's ability to get access. These access controls can be used separately or in combination to increase security. Depending on the sort of wireless access point you're configuring, you'll have different access controls. Encryption and Media Access Control (MAC) filtering can be configured on most access points.

Encryption Wireless data is being transmitted in the air, and it is vulnerable to non-authorized individuals capturing and reading it. Wireless networks adopted encryption as a network standard to prevent data from being delivered over the air in clear text. Unfortunately, early solutions to wireless encryption were quickly cracked. Encryption is growing increasingly complicated and difficult to penetrate as wireless networking advances. As an alternative to preshared keys, new technology is being adopted, such as certificate-based encryption.

The 802.11 protocol specifies WEP Wired Equivalent Privacy (WEP) as an optional security feature for providing authentication and confidentiality on a wireless access point. It was one of the first means of securely transmitting data across a wireless network. When the IEEE committee accepted WEP as a technique, it also stated that WEP should not be regarded as acceptable security and that it should not be utilised without a key management authentication process. WEP uses a symmetric

key to authenticate wireless devices and encrypt data transactions to ensure data integrity. In order for authentication to take place, each wireless access point and client must share the same key. After WEP is enabled, a challenge and response authentication process is initiated. Data is encrypted before it is sent from the machine, and it is decrypted at the access point by WEP. Its security mechanisms were shown to be significantly weak, and it was replaced as the preferred wireless encryption method in 2003. It employs the RC4 stream cypher (Rivest Cipher). Because both the access point and the wireless device use the same key, its authentication mechanism is essentially Shared Key Authentication. WEP keys are always 40 or 104 bits long. The fact that the Initialization Vector (IV) is 24 bits results in the stated 64-bit and 128-bit encryption. With WEP's encryption mechanism, an attacker with enough IVs can crack the key and acquire complete network access. WEP networks have been broken into very quickly in research. The Federal Bureau of Investigation demonstrated how to breach WEP in three minutes at an information security conference.

Overall, the use of WEP can give a misleading feeling of security to the average user. An attacker can swiftly get complete access to the network in the worst-case scenario, hence this should not be utilised to secure a sensitive network. WEP is no longer regarded as a secure technique for securing wireless access points in today's access points. WPA WPA resolves the issue of weak WEP headers, or IVs, as previously described, and provides a method of ensuring the integrity of messages that pass the integrity check by utilising TKIP (Temporal Key Integrity Protocol) to improve data encryption. WPA-PSK is a special mode of WPA that provides the same strong encryption security as WPA but without the need for a corporate authentication server. WPA-PSK is extra-strong encryption in which encryption keys are automatically changed (called rekeying) and authenticated between devices after a set length of time or a set number of packets are transferred. The rekey interval is what it's called. For two reasons, WPA-PSK is considerably superior to WEP and provides improved protection for home/SOHO users. The encryption key is generated using a rigorous technique, and the rekeying (or key shifting) is completed rapidly.

Because WPA employs a per-session encryption key, it outperforms WEP. When a station associates, a new encryption key is created based on randomization and the wireless access point's MAC addresses.

Unfortunately, the simplest method of using WPA makes it easier to breach than WEP. When WPA does not use 802.1X authentication, a simpler technique called Pre-Shared Key (PSK) is used instead. A pre-shared key is a password that must be entered by all clients in order to gain access to the access point. WPA with the PSK pre-shared key is supported by the majority of consumer routers. If you use a short-character password with WPA-PSK, or nearly any password, you are vulnerable to an offline dictionary attack, in which an attacker captures a few packets when a valid station joins the wireless network, and then uses those packets to recover the PSK used. An assailant can obtain all he requires in

order to estimate the PSK and flee without being noticed. Because the attacker only needs to be near the WLAN for a few seconds and the LAN does not need to be highly busy, this might happen. Although password cracking techniques improve all the time, this assault is dependent on the password chosen. The WPA has been defeated. WPA has a mechanism built into most wireless access points that turns an 8-to 63-character string you type into a 64-digit or 128-digit key (as used with WEP). Most wireless access points, however, will not be able to use the entire 64-bit key in pass mode.

The underlying issue is that a pass is easy to guess. An eight-to ten-character pass has less than the 40 bits of security offered by the most basic form of WEP, according to the IEEE group that created 802.11i, and a pass of less than 20 characters is unlikely to stop attacks. Wireless cracking tools that are expressly designed to recover the PSK from a WPA-protected network (like Kismet) are readily available to download, just like WEP cracking tools. WPA plus 802.1X authentication (also known as WPA-Enterprise) creates a significantly more secure network. While deriving a secure, per-session encryption key that is not vulnerable to any casual attack, 802.1X provides robust positive authentication for both the station and the WLAN infrastructure. As previously stated, this is often used with a RADIUS server for authentication. 802.1X authentication, paired with WPA's increased encryption, is the finest wireless security solution with the most access points. Rather than pointing out all of the weaknesses in sending data via unlicensed radio frequencies, WPA, which is included with most modern consumer routers, is a good approach to keep your Internet browsing and home network as secure as possible. When you add VPN connections and MAC filtering, you have the same level of security as a house alarm system. It discourages people who do not have a strong desire to gain access.

8.1.5 MAC Filtering

Network devices, with a few exceptions, have a burned-in MAC address that is physically unique. This serves as a unique identifier for that particular piece of equipment. It is pre-assigned by the manufacturer to the devices and is, in principle, absolutely unique. The MAC address is usually 48 bits long. For writing MAC addresses, a standard format exists, which consists of three groups of four hexadecimal digits separated by dots. For example, 00-07-E9-E3-84-F9 is written using six sets of two hexadecimal digits separated by colons or hyphens. Because each MAC address is unique, it can be used to restrict access to a network.

The steps to do so will vary by access point, but will always involve the following:

- Finding the MAC address of the devices that will be allowed to connect to the network (this can be done by looking at the device itself, or by using the `ipconfig/all` command in the Windows command terminal, or `ifconfig` in the Linux and OSX command consoles).

- In the setup for the access point, enter the MAC address (this will vary by device).

In principle, once the MAC addresses have been entered into the access point, those are the only devices that will be allowed to connect to the network. In practice, a number of complications can arise, including the fact that any time a new system is used in combination with the access point (for example, a visiting client who has to connect to the network), the access point's MAC address must be input manually. This may divert the network administrator's attention away from other network management chores. Information for devices that are no longer in use must be removed on a regular basis by the administrator. Spoofing of MAC addresses is another issue that exists. While the address is usually encoded on the network equipment's physical medium, software can be used to give a device access point a different MAC address than it actually has. While this has genuine and important uses, such as privacy and interoperability, it can also be modified to gain unauthorised access to a system. Because of this significant security flaw, MAC address filtering should not be used in isolation, but rather as part of a larger security policy that includes encryption and other authentication mechanisms.

8.1.6 Cloaking the SSID

The SSID is the name of the wireless network or access point that the user sees. There are only two ways for a client to learn their SSID: the access point can actively tell them, or you can passively put it in the client's settings. When the SSID is broadcast over the radio frequency, it is known as Open Network mode. When the SSID is not broadcast over the radio frequency, it is known as the Closed Network mode. A beacon is an automatic transmission of the SSID that occurs every 100 milliseconds and contains synchronisation information like channel, speeds, timestamps, encryption status, and other information. The SSID is not broadcast to the user or administrator programmes in Closed Network mode. As a result, the client must probe the access point, and if the SSID matches, the client will synchronise and begin the authentication process. An open system or shared key authentication can be used for authentication. No credentials are required for an open system. In wireless networks, the SSID is used to identify the wireless access point and its associated network. It is connected to all packets sent over the wireless connection and can be up to 32 alphanumeric characters long. Because many access points in the same area might broadcast the same SSID, its utility as a security or authentication technique is limited. However, in order to reduce network visibility, the SSID can be modified and cloaked (that is, it is not set to be broadcast by the AP). Most APs broadcast their SSID to the nearby region by default. Every 0.1 seconds, this beacon mechanism is used. Most APs come with a default SSID that is well recognised and may be found on a variety of websites. Using a default SSID may attract malevolent users who think that the AP's other settings are also set to default (such as the administrative password). Changing the SSID may cause some potential attackers to choose a wireless network with default settings, which is risky. Changing the SSID is a relatively

straightforward task for a nontechnical user, and it is a step toward protecting the AP, albeit a tiny one. It's worth noting that turning off the SSID broadcast doesn't totally hide the AP. It simply reduces its visibility.

8.2 WIRELESS PENETRATION TESTING

Many managers and system administrators are uninterested in learning about the hacking techniques used by hackers to attack wireless networks. The usage of hacker tools and tactics is generally connected with a bad reputation. They frequently regard the deployment of these tools as a validation of hacker techniques and strategies. This mindset may result in an insecure wireless network that has not been thoroughly evaluated to determine its capabilities to prevent a successful attack. Penetration testing is critical for determining the security of your wireless infrastructure. One can better assess vulnerabilities, overcome weaknesses, and strengthen defences by learning, understanding, and adopting the same attack methods as the intruder. It's critical to obtain as much information about the network as possible during a wireless penetration test. Because most vulnerable networks are identified during war driving (the process of scanning for them), the assault could be aimed at a wireless weakness rather than a specific corporate network. When doing a penetration test, you should consider both an internal and external attacker. You can leverage information you already know about the network, such as encryption keys, network design, and signal ranges, with the internal method. This type of test verifies the network's security from the perspective of internal personnel. External testing is carried out without the use of any network infrastructure knowledge. The tester replicates a genuine attack by using tools that an intruder might employ. This test should be carried out by a qualified security professional to guarantee that these tools do not have a detrimental influence on network and server systems.

The most important thing to remember during a wireless penetration test is that your goal is to evaluate the wireless network's security. It's a good idea to get management's agreement in writing about the tests that will be performed and the potential network impact. This way, no party will be surprised.

- Nothing you do should ever jeopardise or affect a neighbouring wireless network.
- Without permission, you should not attempt any form of Denial-of-Service attack on the network.
- You'll be trying to break into various parts of the network. Make sure that the results of the scan and penetration test are kept private and securely stored.
- All discoveries should be reported to management, along with full explanations and security suggestions.

A search warrant may be required before you can investigate a gadget that belongs to someone else. You should double-check that the search warrant includes the authority to examine computer equipment, such as wireless access points, on-site. Perform no forensic investigation on equipment that you haven't been given permission to examine.

8.2.1 Direct Connections to Wireless Access Point

Users who are adamant about connecting to an illegal access point should keep a watch out for security professionals conducting wireless audits and unplug the access point until the scan is finished. Physical wireless scans demand a lot of effort, so they aren't done as frequently as they should be. There are numerous advantages to detecting wireless access points from your wired network. You may create automatic scripts that continuously search your network, saving you time and money. You can scan areas of your network that aren't easily accessible for wireless scanning with tools like Network Mapper (Nmap). You must be connected to the internal network and have the ability to connect to all of the subnets you want to scan in order to run wired network scans for access points.

8.2.2 Scanning for Wireless Access Points with Nmap

The Network Mapper (Nmap), a Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) Internet Protocol (IP) scanner, is one of the more common tools for performing network scans. Nmap supports a variety of scanning techniques, the most essential of which is "stealth" scanning. The intruder's ability to "fly under the radar" of the target system's administrator is critical to the intruder's success, and stealth scanning has the advantage of passing unmolested and mostly unnoticed via most firewall and network monitoring systems. We may use these scans to see what ports on our network equipment are open, as well as discover unwanted wireless access points. Nmap is used to determine the target system's operating system. Be aware that OS fingerprinting scans are easily observable and will be flagged by intrusion detection systems right away (IDSes). Nmap is a network exploration and security auditing tool that is available for free. It was created to quickly scan large networks, but it also works well with single hosts. Nmap analyses raw IP packets in unique ways to figure out what hosts are on the network, what services they offer (application name and version), what operating systems (and OS versions) they're running, what kind of packet filters/firewalls they're using, and thousands of other details. Nmap is available in both console and graphical versions, and it runs on most sorts of PCs. Nmap is a free and open-source application. By scanning from the wired side of the network, we will use the text description, vendor name, operating system, and device type provided by Nmap during OS fingerprinting to detect wireless access points (WAPs). Nmap fingerprinting is a powerful tool for identifying WAP devices.

To determine if an access point was connected to the network, we can run a scan of a local class c subnet using the following command:

```
nmap -A -T4 192.168.0.1/24
```

This command does a few things.

The `-A` tells Nmap to enable operating system and version detection.

The `-T4` sets the timing template to 4, which speeds up the scan by setting the timeout value to 500 milliseconds.

When scanning huge subnets, this can be quite valuable for ensuring quick results. Device type: WAP is what we're looking for in the Nmap output. This is our confirmation that we have scanned a network wireless access point.

8.2.3 Scanning for Wireless Access Points with Nessus

Nessus is a powerful and up-to-date open source scanner that looks for security issues on a network. Nessus is very fast and dependable, with a modular architecture that allows you to tailor it to your exact needs. Scans can be tailored to seek only the vulnerabilities that matter to you. Each security test is written as a plug-in for a third-party application. This allows you to rapidly add your own tests without having to read the code of the Nessus engine. The Nessus scanner is made up of two parts: a server that performs security checks and a client that serves as the user interface. You can run the server and the client on different systems. Additionally, several clients are available: one for X11, one for Win32, and one written in Java.

Using a number of strategies, the Nessus plugin # 11026 was created to identify the presence of wireless access points on the network. It uses the TCP/IP Nmap fingerprint to scan the device, examine the HTTP management interface, and verify the presence of the FTP banner and SNMP information. If one of these procedures concludes that the device is a wireless access point, the scan continues to the next device, identifying it as a WAP.

To scan using the #11026 plug-in for Nessus, complete the following steps:

- To make sure the plug-ins are up to current, run `nessus-update-plugins`.
- Start a fresh scan and make sure the Access Point Detection plug-in is selected on the Plugins tab of the client's General plug-in section.
- Ensure that the Enable Dependencies box is checked.
- Because the plug-in requires the system information type via SNMP and HTTP Server-type dependencies to be able to scan, the At Runtime option is checked.

8.2.4 Rogue Access Points

You might want to consider investing in a wireless IDS/IPS solution for enterprise-class access point detection. A wireless IDS/IPS is a network intrusion detection and prevention system that monitors the network 24 hours a day, 7 days a week and can dynamically respond to wireless threats. A wireless IDS/IPS can also terminate rogue devices by utilising air or port suppression on the switch, do forensic analysis of packets sent and received, and monitor the device's location by triangulating the signal between numerous sensors. Because users may plug in a wireless access point with no configuration and extend the network wirelessly, rogue access points are becoming a rising danger to network managers. This results in a lack of control over where data is delivered and, more importantly, who is listening. Connect to a Wireless Access Point (WAP). In this section, we'll look at the methods hackers use to break into wireless access points. A hacker will want to learn as much as possible about the target network before launching an attack, and will use a variety of wireless tools to do so. Once the hacker is satisfied with the information acquired, injection techniques can be used to force information through the wireless network, which can be used to crack encryption algorithms. Once the data has been obtained, the encryption key will be acquired, and the hacker will be able to login to the internal network via the wireless access point. These attacks were carried out with tools that were widely available on the Internet and included in live security releases. Many of the Aircrack-ng programmes (www.aircrack-ng.org) will be used, as well as Kismet (www.kismetwireless.net), a popular wireless analyzer. While you may be able to find tools for other operating systems, most are written for Linux, so some knowledge of Unix commands will be helpful.

8.2.5 Information Gathering

When attempting to acquire unauthorised access to a wireless network, a hacker will first do reconnaissance to learn more about the tools that will be required next. This stage identifies rogue wireless access points, ad hoc wireless networks, and open or badly configured access points that could be used to obtain access. Because all of this information will be used to acquire vital connection data, hackers will want to get as much information about the wireless access points as they do about the connected clients.

Kismet

It's time to check if our network is up and running. To do so, we'll use Kismet as a starting point. Kismet is a layer 2 wireless packet analyzer that works with raw monitoring mode wireless devices. By intercepting wireless packets and recovering information such as whether they have security enabled or allow SSID masking, Kismet can swiftly detect wireless networks. Kismet can also determine a network's channels as well as its SSID.

This phase will imitate what an attacker would look for while scanning for weak points in a network. When you first open Kismet, you'll see that wireless networks appear on the screen.

Kismet organises the network listings by auto-fit by default, which can make them difficult to read if there are a lot of them. The first step is to sort the access points by SSID by pressing "s" to bring up the sort menu, then pressing "s" again to sort by SSID. This view groups networks into categories such as Probe Networks and Ad-hoc Networks, in addition to sorting them by SSID. This is crucial to understand as we continue to gather data on our target wireless network.

Highlight a cluster and press the Spacebar to enlarge or collapse it.

Let's look at the different columns now that we have our Network List screen sorted by SSID.

- Name: SSID of network
- T: Type of network (A = Access Point, H = Ad-Hoc, P = Probe request, A = wirelessclient searching for a network, D = Data network, T = Turbocell network, and G = Group of wireless networks)
- W: Identifies if network is secured (Y = Yes, N = No)
- Ch: Channel number of network
- Packts: Number of packets captured
- Flags: Method in which IP was gathered
- IP Range: IP of the network

The Kismet colors make identifying networks easier. The following are the possible color combinations:

- Yellow: Unencrypted network
- Red: Network is using factory defaults
- Green: Secured Network
- Blue: Hidden networks that are cloaking the SSID

The network channel and whether or not the network is encrypted are two pieces of information we'll get from Kismet in the next stage. It'll also be useful to keep track of whether Kismet was able to identify an IP range or whether the network was Red or Yellow. Both suggest that security is inadequately designed and that the network is vulnerable.

Aircrack-ng

Aircrack-ng (www.aircrack-ng.org) is a suite of tools for auditing wireless networks. We will be using the *airodump-ng*, *aireplay-ng*, *aircrack-ng*, and *airdecap-ng* tools from the Aircrack-ng suite.

- *Airodump-ng* captures raw 802.11 packets to be used with *aircrack-ng*. *Airodump-ng* is also capable of logging the coordinates of access points.

- *Aireplay-ng* is primarily used to inject frames into wireless traffic, which will later be used by *aircrack-ng* to crack WEP and WPA-PSK keys. *Aireplay-ng* supports deauthentications, fake authentications, interactive packet replay and ARP request (re)injections.

- *Aircrack-ng* can recover keys once enough data packets have been captured.

Optimizations to the standard attack algorithms make wireless encryption cracking with Aircrack-ng much faster compared to other WEP cracking tools.

- *Airdecap-ng* is used to decrypt encrypted capture files. It can also be used to strip wireless headers from capture files.

Our first command will begin sniffing the wireless packets using the *Airodump-ng* utility. The packets will be captured and written to a file that will later be used to crack the encryption key. From a command prompt, run the following command:

```
airodump-ng -w output -c 6 ath1
```

This command runs the *Airodump-ng* command and sets the capture file to output using the `-w` switch. Since we know from our Kismet scan the wireless network of interest is on channel 6, we use the `-c` switch to ensure that *airodump-ng* stays on that channel and captures as much data as possible. Finally, we tell the command to use the interface `ath0`. The interface may vary, depending on the wireless card you are using.

You should now see the *Airodump-ng* screen. The screen is broken into two sections: the top section shows the wireless access points; the bottom section shows the wireless clients.

Now that we have *Airodump-ng* running, we will look for associated wireless clients. We will need to document the BSSID and Station address to perform packet injection.

Injection

Wireless packet injection allows a hacker to change packets in the air, forcing wireless devices to generate traffic that can be intercepted and exploited to crack the encryption key. If the network has a lot of traffic, the hacker won't need to inject anything to compel traffic to be generated. If the hacker is impatient, however, deauthenticating an already authenticated client is a quick way to create traffic. This deauthentication compels the client to reauthenticate, resulting in the handshaking packets used by the hacker during the cracking step.

We'll utilise the *aireplay-ng* software to do packet injection as part of our penetration test. This tool can carry out a variety of attacks. Fake

authentication, ARP packet replay, and deauthentication will all be put to the test.

First, we will associate the attacking machine with the target network. This will be done using the fake authentication method. To perform fake authentication, we will run the following command.

```
aireplay-ng -1 0 -e TestNet -a 00:0F:B5:29:8C:32 -h 06:18:4D:95:32:61 ath1
```

This command runs the *aireplay-ng* command and sets the attacktype to -1, which is fake authentication. The 0 sets the reassociation timing to 0 seconds. To set the wireless network name, the -e switch is followed by the SSID of the wireless network. Then, the -a switch is followed by the MAC address of the access point and the -h switch is followed by the MAC address of the network card used for the injection. We complete the command by adding the wireless interface name. If the command is successful, you should receive the following response:

- Sending Authentication Request
- Authentication successful
- Sending Association Request
- Association successful

The target access point is now paired with your wireless network card. Setting up ARP request packet replay is the next step. This is the most efficient method for generating the necessary traffic to crack the encryption key. The access point responds with new IVs while the attack retransmits the same ARP packet. These packets are crucial in figuring out the encryption key.

We will now set up the ARP request replay using the *aireplay-ng* command. To perform this attack, we open up a new command window and run:

```
aireplay-ng -3 -b 00:0F:B5:29:8C:32 -h 00:13:CE:86:08:A6 ath1
```

The *aireplay-ng* command is executed with the -3 attack type, standard ARP request replay. The MAC address of the access point is followed by the -b switch, and the MAC address of the associated client is followed by the -h switch. When we issue the deauthentication command, the ARP request replay will begin flooding the access point with retransmitted ARP packets and creating the IV packets that are required.

To generate the deauthenticate attack, we will again use *aireplay-ng*. Once this process is initiated, we should see a substantial rise in traffic on our airodump-ng screen. To run the deauthenticate command, we open up a new command window and run:

```
aireplay-ng -0 5 -a 00:0F:B5:29:8C:32 -c 00:13:CE:86:08:A6 ath1
```

This command runs the *aireplay-ng* command using the -0 attack which means deauthentication. The next number sets the number of deauthentication packets to 5, setting this number to 0 sends continuous deauthentication packets. The -a switch is followed by the MAC address of the access point and the -c switch is followed by the MAC address of the client you are trying to disassociate. The final option is the wireless interface name.

Now that all of the injection commands have been completed, you can move on to the next step. The data column for the wireless network you're testing should gradually increase. The ARP request replay should also read and retransmit ARP packets to the access point. With 300,000 IVs, 40-bit WEP can be cracked, but 128-bit WEP may require 1.5 million IVs. Once you've recorded enough packets, you can check to determine if the wireless encryption key is vulnerable to cracking. Cracking We can now test our encryption key to see if it is subject to cracking now that we have a capture file containing the relevant data. Aircrack-ng employs a variety of statistical approaches, including brute forcing the key, to crack WEP keys. Only a dictionary attack is possible due to the intricacy of WPA/WPA2 preshared keys.

In a new command window, we will use the *aircrack-ng* command to attempt to crack the wireless encryption key. For a typical WEP attempt, we would use the following command.

```
aircrack-ng -m 00:11:22:33:44:55 -n 64 output.cap
```

This command executes aircrack-ng with the -m option and the MAC address of the access point we're attempting to crack. This option is optional, but it aids in concentrating the attack on our target access point. The -n switch determines the key's length. If you're not sure what length to use, consider 64 or 128. Finally, we'll offer the capture file, which contains the data gathered by airodump-ng. If the command is successful, the target network's encryption key will be displayed.

8.2.6 Passive and Active Sniffing

You will be able to associate your computer with the target network once you have found the target network's encryption key. Your network has been compromised, and now is a good opportunity to reassess the security restrictions on your wireless network. It's likely that hackers have already done what you've done and are attempting to steal data from your company's network. When most administrators believe their network has been compromised, the first thing they do is check the logs to determine if anyone who isn't authorised has connected to the network. While this is a decent starting step in determining whether you are actively connected, keep in mind that wireless data is sent in the air, and an attacker with the encryption key can sniff the network traffic and passively decrypt it. This implies they'll never be able to connect to the internet! Let's look at the capture file you saved with airodump-ng to use with aircrack-ng to show this. This file was created with the intention of being used with aircrack-ng to decrypt the encryption key. Now that we know the key, we can use

the *airdecap-ng* software to remove the wireless headers and decrypt any encrypted packets, leaving us with a capture file that any packet analyzer, such as Wireshark, can read data from the target network in plain text.

To run the *airdecap-ng* command, we will open up a new command window and run:

```
airdecap-ng -e TestNet -w 145AA34FA1 output.cap
```

This command runs the *airdecap-ng* command and supplies the following options. The *-e* switch is followed by the ESSID of the target network. The *-w* switch is followed by the hexadecimal WEP key. Then the capture file is provided. This will decrypt the capture file and save it to a file name *output-dec.cap*. If the command is successful, you should see a similar result:

Total number of packets read 1658828

Total number of WEP data packets 255816

Total number of WPA data packets 0

Number of plaintext data packets 30

Number of decrypted WEP packets 255816

Number of decrypted WPA packets 0

You can now read the contents of decrypted captured files and network traffic. Because the attacker does not need to connect to the network to get network data after the encryption key is known, this is a passive technique of data capture. If the system administrator fails to recognise and respond to the initial packet injection attack on the access point, the attacker will be able to sniff data unnoticed until the key is changed.

If an attacker isn't concerned about being identified on the network, they can connect and try to sniff data directly from the wireless connection. Despite the fact that this technique makes a direct connection with the target network and can be logged by the access point, it will be difficult to detect unless there is a wireless IDS/IPS in place or constant scanning to find unwanted MAC addresses on the network. The hacker's ability to deploy more complicated tools on the internal network to obtain further information is one of the many threats linked with active scanning. Instead of being limited to reading only wirelessly transmitted data, tools like Ettercap allow you to sniff wired network traffic from a wireless connection if the computers are on the same subnet. Logging The majority of wireless access points can log traffic and connections. Before an incident occurs, it's critical to think about logging requirements. The ability to go back in time to a precise point in time when an event is thought to have occurred allows the investigator to study and decide whether a wireless attack on the network occurred. Most access points' logging does not provide the granularity required for successful logging. Using wireless sensors, wireless IDS/IPS systems can be set up to detect

and log any suspicious wireless activities. These sensors detect and log faulty wireless packets for subsequent forensic investigation.

Due to the nature of the technology, investigating wireless assaults is tough. This is precisely why attackers use this method of gaining access to business networks. The best option is to set up your wireless network securely to prevent hackers from quickly gaining access. If a wireless incident occurs, an investigator can use the same tools that the attacker used to figure out how the attack was carried out and how much data was potentially exposed. Examining event logs on servers and network devices on a regular basis is always an excellent way to spot attacks early and respond correctly.

8.2.7 Investigating Web Attacks

Web attacks are a broad and diverse issue that encompasses a wide range of attack types and attack channels. Web assaults are often divided into two categories: attacks on the Web infrastructure and attacks on the Web application. Although there may appear to be a small distinction between the two, infrastructure deals with assaults on the Web server operating system and server software (such as directly attacking Apache or the Microsoft IIS server). Server and operating system configuration flaws, buffer overflows, command injection, and protocol-based assaults are all examples of infrastructure attacks. Attacks against Web applications are typically not related to infrastructure, but rather to the site's application code. There's a lot to say about Web application assaults; in fact, Web application security has grown into its own specialist sector within information security.

Types of Web Attacks

As previously stated, there are numerous sorts of Web attacks, each of which might easily fill its own book. In fact, there are countless books that go into great detail about web attacks. At the application level (attacks like cross-site scripting (XSS), cross-site request forgery (CSRF), parameter tampering, and cookie poisoning) and at the infrastructure level (attacks like code/command injection, buffer overflows, and protocol-based attacks), we'll look at a few common Web attacks.

Cross-Site Scripting

To completely comprehend cross-site scripting (XSS) attacks, it's important to realise that attackers employ a number of different theories and ways of getting their code into your browser. From the most basic to the most complicated, this section breaks out the various forms of XSS attacks and related code injection vectors. Injecting a script into a search field is a legitimate attack vector, but what if the value is filtered? Is there a way to get around the filter? The truth is that XSS is a vast field that continues to surprise the world with new and unique methods of exploitation and injection. There are, however, basic underpinnings that Web developers, security researchers, and IT workers responsible for maintaining the infrastructure together must completely comprehend.

XSS is a type of attack that induces a website to display malicious code, which then runs in the user's browser. Consider that XSS attack code, which is usually (but not always) written in HTML/JavaScript (a.k.a. JavaScript dangerous software [malware]), does not run on the server. The server only serves as a host for the assault, which takes place entirely within the Web browser. The trusted Web site is just used as a conduit by the hacker to carry out the assault. The user, not the server, is the intended victim. Once an attacker has a thread of control in a user's Web browser, he can perform a variety of criminal behaviours, such as account hijacking, keystroke recording, intranet hacking, history stealing, and so on, as explained throughout this book.

For a Web browser to become infected it must visit a Web page containing JavaScript malware. JavaScript malware could become resident on a Web page in many ways:

- The Web site owner may have purposefully uploaded the offending code.
- The Web page may have been defaced using a vulnerability from the network or

operating system layers with JavaScript malware as part of the payload.

- A permanent XSS vulnerability could have been exploited, where JavaScript malware

was injected into a public area of a Web site.

- A victim could have clicked on a specially crafted nonpersistent or Document

XSS connection based on the Object Model (DOM). Persistent, nonpersistent, and DOM-based XSS attacks are the three most common varieties. We'll take a look at each one separately. Persistent (or HTML Injection) XSS attacks are especially common on community content-driven Web sites or Web mail systems, because they don't require specially crafted links to work. A hacker simply places an XSS attack code in a section of a website that other users are likely to visit. Blog comments, user reviews, message board posts, chat rooms, HTML e-mail, wikis, and a variety of other places could be used. Execution is automatic once a person accesses the infected Web page. Because the user has no way of protecting himself, persistent XSS is far more harmful than nonpersistent or DOM-based XSS. Once a hacker has his exploit code in place, he will publicise the URL of the infected Web page in the hopes of catching unsuspecting people. Even users who are aware of nonpersistent XSS URLs are vulnerable. When most people hear the term "XSS," they instantly think of nonpersistent XSS. Consider a hacker attempting to XSS a user on the prominent e-commerce site <http://victim/>. The hacker must first locate an XSS vulnerability on <http://victim/> before creating a

specially constructed URL. To do so, the hacker goes through the website looking for any functionality that allows client-supplied data to be transferred to the Web server and then echoed back to the screen. A search box is one of the most common vectors for this.

DOM-based XSS is a special type of XSS that works similarly to nonpersistent XSS but doesn't require the JavaScript malware payload to be sent or echoed by the Web site in order to infect a user. The World Wide Web Consortium (W3C) defines the object model for expressing XML and HTML structures in the DOM specification. There are essentially two sorts of parsers in the XML world: DOM and SAX. SAX is a parsing system that is substantially faster and uses less memory, but it is also difficult to use because it is difficult to return to the document nodes (i.e., the parsing mechanism is one-way). DOM-based XSS is a special type of XSS that works similarly to nonpersistent XSS but doesn't require the JavaScript malware payload to be sent or echoed by the Web site in order to infect a user. The World Wide Web Consortium (W3C) defines the object model for expressing XML and HTML structures in the DOM specification. There are essentially two sorts of parsers in the XML world: DOM and SAX. SAX is a parsing system that is substantially faster and uses less memory, but it is also difficult to use because it is difficult to return to the document nodes (i.e., the parsing mechanism is one-way). The exploitation of a client-side input validation flaw, rather than a server-side vulnerability, is known as DOM-based XSS. In other words, DOM-based XSS is caused by an erroneous processing of user-supplied data in the client-side JavaScript, rather than a vulnerability in the server-side script. DOM-based XSS, like other types of XSS vulnerabilities, can be leveraged to steal sensitive information or hijack a user's account. It's important to note, however, that this vulnerability is purely due to JavaScript and the unsafe usage of dynamically derived data from the DOM structure.

Here is a simple example of a DOM-based XSS provided by Amit Klein in his paper

“DOM-Based Cross-Site Scripting or XSS of the Third Kind”:

```
<HTML>
<TITLE>Welcome!</TITLE>
Hi
<SCRIPT>
var pos=document.URL.indexOf("name=")+5;
document.write(document.URL.substring(pos,document.URL.length));
</SCRIPT>
<BR>
Welcome to our system
...
</HTML>
```


If we look at the code above, we can see that the developer failed to sanitise the value of the "name" get argument, which is then written into the page as soon as it is retrieved. In the next part, we'll look at a few additional DOM-based XSS instances based on a hypothetical application that we constructed to demonstrate that XSS is omnipresent.

Investigating XSS

When researching XSS assaults, the Web server logs will be one source of information. Look at the server's standard traffic logging and referrer information to discover where the incoming page request is coming from. Although it is quite simple to spoof referrer information, many attackers take the risk that you will not notice the referrer information before they travel to the XSS site. Any pages that require login or authentication are of particular importance.

When analysing an active XSS attack, a Web proxy such as Paros Proxy (www.parosproxy.org) can be used to examine Web server transactions in real time and see any communications with outside servers. You can also look at the source code of any HTML-formatted e-mail messages to see if there are any embedded scripts or links in the URL of the victim site. Although traffic capture visualisation tools can provide insight into XSS assaults, average traffic loads make this form of investigation expensive and time-consuming.

Cross-Site Request Forgery

Cross-site request forgery (CSRF) or Sea Surf attacks are relatively recent in comparison to XSS attacks. As the name suggests, this is a variation on XSS-style attacks, but this time the victim is the one who initiates the exploit rather than the attacker. The CSRF attack is based on the assumption that a site has a specified level of trust with a user. This trust could take the form of a session variable, cookie, or other token that stays on the victim's system for longer than necessary. When this attack first appeared, it was presumed that the attacker had inside information about the victim's use of these vulnerable sites, and that this was how the assault was launched. We've since discovered that, similar to testing for cookies, it's possible to interrogate for tokens and then launch an attack if the token is detected.

There are many ways to initiate a CSRF attack. One classic method uses the image tag to post a request containing the attacker's code. This is the one we will look at in depth.

Anatomy of a CSRF Attack

In this example, we will make the following assumptions:

- The attacker wants to reduce the number of users of a competing Web site.
- The attacker has realized that the page for removing yourself from the site is vulnerable.

- The attacker has a page on his site that looks for the token and generates the attack.

The session left a valid access token on the victim's machine when the victim last visited the target Web site, www.worldofwidgets.org. After that, the victim goes to the attacker's website. The attacker's main page checked for the token before launching the attack. The member's e-mail address and a section that requires an uppercase YES to be input as verification that the member wants to be removed are both on the page for removing the member from the worldofwidgets site. The key parts of this form are shown here:

```
<FORM Action="Account_Close.asp" method="POST">
```

```
E-Mail Address: <INPUT type="TEXT" Name="emailAddr"><br>
```

```
Confirm Account Close (YES): <INPUT type="TEXT"
Name="confirm"><br>
```

```
<INPUT type="SUBMIT" value="Close Account"><p>
```

```
</FORM>
```

The attacker can easily integrate the attack into an image request on one of his website's pages once he has this information. A common way is to utilise the get image HTML tag and append the victim's information. Because the request comes from the victim's machine, the token is used to validate the victim's identity and authorise the removal.

```
<IMG SRC="http://widgetworld.org/remove_member.asp?email=FredS@
bignet.com&confirm=YES">
```

This tag sends the e-mail address of the victim, in this case FredS@bignet.com, and the confirmation field YES to the remove_member.asp page instead of fetching an image, which is what IMG SRC is supposed to be used for. In this example, the victim may see an acknowledgment screen that would confuse him. If the worldofwidgets site designer uses security best practices, the victim would receive an e-mail letting him know this happened.

Pen-Testing CSRF Fields

The token is the most important part of any CSRF vulnerability test. It is vital to guarantee that tokens expire or become invalid when they are no longer required if a site employs cookies or session variables. In the case of cookies, depending on the type of site usage you foresee, it may be prudent to set the expiration to a reasonable time. Setting the expiration 10 minutes in the future may be a sensible choice if your logs show that the average duration a user spends on the site is 10 minutes. This will prevent numerous CSRF attempts.

When the site is utilised differently or the average user time is too varied, storing session variables that are no longer valid in a log may be the solution. It would also work to have a routine set a session variable to be invalid after a logout or a period of inactivity. Adding a code at the top of every page to test the session variable and requiring a login if the variable is no longer valid would alert the victim to the CSRF attack. If the token is configured to expire in 10 minutes, you should visit the site and wait several minutes after the timeout has passed before attempting to access an internal page that you should not have access to. You can tell if a page hasn't been hardened against the CSRF attack if it loads or grants you access when it shouldn't.

Code Injection Attacks

A Code injection attack is possible whenever a scripting or programming language is utilised on a Web page, and all an attacker needs is an opening. The opening is usually in the form of an incorrectly validated input field. A code injection attack's "code" doesn't have to be on the Web page, though. It can be found in the backend as part of a database query or as part of a CGI for the Web site. Between the Internet and the data, any part of the server that employs Java, JavaScript, C, Perl, Visual Basic, SQL, or any other code is vulnerable. SQL injection attacks are now popular and well reported in the media, therefore they may be the most well-known sort of code injection attack at the time of writing. Every day, however, there are various assaults on Cold Fusion, Active Server, Java, Perl, and Awk-based code. A large part of the problem is programmers who don't examine every single input that a user may possibly enter. Most of these attacks can be blocked if a programmer creates a list of all permissible inputs and then builds input validation methods that only accept good inputs and reject bad inputs.

Investigating Code Injection Attacks

The Web server logs rarely include evidence of a code injection attack. You'll probably observe the different attempts to get the attack right if the Web designer writes failed input information to a log file. You may have to rely on network traffic sniffer records if there are no logs of erroneous attempts to fill out a form or other inputs. Using an open-source tool like Wireshark to capture server traffic and then scanning for either all requests travelling to the input page or field names on the page may give you a good accounting of the malicious traffic and the sender's IP address. To catch one of the attempts, you may need to gather some fairly huge files. You can significantly minimise the capture file size by setting the capture filter on the sniffer of your choice to only capture traffic travelling to the server.

The capture filter in Wireshark would be `dst host xxx.xxx.xxx.xxx` (the xs are the server's IP address). Before leaving the sniffer running unattended for lengthy periods of time, test to see how big this file grows over the course of an hour or two, and make sure you have enough storage space for the resulting file. You can use the frame contains display filter frame

contains "homePhone" if you know one of the input fields on a page you're looking at is labelled homePhone. Any packets with data flowing to the input field will be displayed, and their contents can be checked for proper or malicious content.

Access logs and transaction data are two other places where evidence can be found. Don't forget to consider transaction times. You may be noticing symptoms of an attack if you notice a huge volume of transactions in a short period of time or at strange hours.

Command Injection Attacks

The type of payload provided and the access level used distinguish command injection attacks from other injection attacks. Command attacks will largely target trusted interfaces, such as CGIs, as well as deeper-level scripts or programmes run by administrators. The passing and execution of system commands at or just above the operating system level is known as command injection. Microsoft Internet Explorer has been the target of multiple successful command injection attacks, thanks in part to helpful code that attempted to repair faulty Web sites. For several years, these assaults were the scourge of Microsoft Internet Explorer coders.

Parameter Tampering

Parameter tampering, which is the alteration of unprotected data in the URL or a hidden field of a Web page, is one of the oldest types of Web-based assaults. This type of attack is usually directed at a business website that has prices or other data tied to a Web page.

For example, if the attacker is at a sporting goods Web site and is thinking of buying a tennis racket that costs \$80, he might see the price reflected in the URL in this way:

`http://sales.sportswidget.com/order.htm?SKU="4321A"&price=80.00`

If the attacker changes the price in the URL line before pressing Enter, and the site does not verify the price, he could buy the racket for \$30 this way:

`http://sales.sportswidget.com/order.htm?SKU="4321A"&price=30.00`

Another popular form of parameter tampering is the changing of hidden fields within theHTML itself. Here, again, if the attacker views the source of the Web page and sees the price of the racket being held in a hidden field, he could save the source code, make the modification, and then load the file and send the new price, hoping it won't be caught later. In this way, the following:

```
<input type="hidden" name="price" value="80.00">
```

could be changed to:

```
<input type="hidden" name="price" value="30.00">
```

Newer solutions, such as Paros Proxy, are great for both investigators and attackers since they allow you to change the HTML code that is received and delivered on your computer.

This makes parameter tinkering a breeze, and it also makes testing Web form pages a breeze. Unfortunately, like with many security solutions, those that are beneficial to security professionals are also beneficial to attackers.

Cookie Poisoning

Cookie poisoning is a particular form of parameter tampering in which the attacker obtains the contents of a cookie saved on the victim's machine. The attacker can either get sensitive information about the victim or update information for any purpose he wants by reading the information in these cookies. Cookies are used by many websites to store session information or short-term variables that are used to track a user's travel across a site. In principle, these cookies are invisible to the end user, and while the Web site may encrypt cookies in some situations, many are not and are extremely easy to read. As a result, attackers value the information stored in these cookies. It would be as simple as looking for the cookie from the sports store in the previous example and modifying the victim's cookie so that the list price of a racket is \$90 instead of \$80 when he checks out to induce anger and unhappiness.

Investigating Cookie Poisoning

To identify and investigate cookie poisoning, have the cookie issuing server save session variables and cookie contents to a log file, and then compare those cookies to the transaction logs to make sure the transaction finished with the identical data saved in the original cookie. If you go the extra step of watching referrer information during transactions, you can discover that the attack was not only caused by a poisoned cookie, but also by an XSS assault.

Buffer Overflows/Cookie Snooping

One of the side benefits to an attacker who performs a buffer overflow attack on a Web page is the direct reading of cookie data that is currently stored in memory. Many apps save cookies right with the browser's other variables. This is logical because the cookie is a variable. The attacker can read the unencrypted cookie data by executing a buffer overflow and having the payload read the working storage area of memory. This information can range from session information to Social Security numbers or bank codes.

Investigating Buffer Overflows

Depending on the type of buffer overflow and the error recovery strategy employed by the programmers, evidence of buffer overflows can be found in system logs, event logs, and programme logs. A buffer overflow can usually be observed reasonably quickly if you use a traffic sniffer or

intrusion detection system and filter the Web page traffic and look at the input data. Buffer overflows are usually huge files with repeating data strings that pop out at you when you see them. Test field input procedures to see if they trim or reject entries that are too large while studying a website that you suspect may be vulnerable to a buffer overflow attack.

DMZ Protocol Attacks, Zero Day Attacks

One of the best practices network administrators employ to shield the remainder of the network from the portions that need to be open to the Internet is to place Internet-facing equipment in a separate "Demilitarized Zone," or DMZ. Internal and external DMZ protocol attacks are the most common. Internal assaults take advantage of the protocols used by systems in the DMZ. The protocols that the DMZ utilises to communicate with the internal network systems are used by external assaults. If an attacker gains access to a DMZ Web server, he may discover that the Web server uses a trusted Internet work Packet Exchange (IPX) channel to communicate with a database server, which is also in the DMZ. This URL can be exploited to exploit the database by abusing the Web server. This is the best example of an internal attack.

Once within the DMZ, the attacker can utilise any protocol to get access to the company's internal network or intranet. It can be perplexing to think of an external attack as a word for attacking an interior network. Consider the attack from the perspective of being inside the DMZ and attacking outside the DMZ into the rest of the corporation if it helps. When these assaults deliver a malicious payload that isn't in the signature database of the network's antivirus or intrusion detection/prevention systems, it is referred to as a Zero Day attack. If the attack or vulnerability hasn't been made public yet, it's also referred to as a Zero Day attack.

Example of an FTP Compromise: Attacks against FTP servers have been popular among attackers for quite a few years now. These attacks allow the attacker to transfer large amounts of data in either direction faster than other methods, and they allow attackers to steal information masked as other normal FTP traffic.

A classic example of the FTP Bounce attack is shown in the Figure 8.1. The attack uses the following steps:

1. The attacker creates a script that logs into the victim's FTP site and either requests or transmits a file to an intermediate FTP server, which is usually an open server in a public place like a school or library.
2. The attacker then creates a port between the attacker's system (which is usually operating an FTP server as well) and the intermediate FTP server using a script for the intermediate FTP server. After that, the attacker logs into the intermediary server and runs the two scripts.
3. When the attacker runs the scripts, an FTP link is established between his system and the intermediary system, and then a link is established between the intermediate system and the victim machine.

4. The attacker can send or request FTP files or data from the victim server after the connections are established, and all logs on the victim server demonstrate that the attack originated from the intermediate machine.

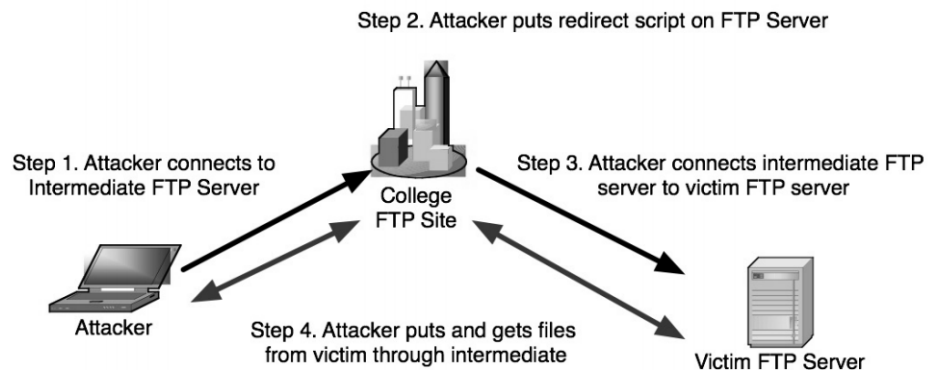


Figure 8.1 An Example of FTP Bounce Attack Methods

FTP-based assaults come in a variety of forms today. Even some of the older techniques can still work depending on the age of the FTP software and the security settings on the server!

Intrusion Detection

People who believe that intrusion detection systems prevent intrusions are making the most common mistake. They don't stop or deter invasions in any manner; all they do is report when one happens or is attempted. Snort is an open source intrusion detection system that has become a benchmark against which commercial intrusion detection systems are measured. Snort, which is available at www.snort.org, can be used to capture network traffic and provide traffic analysis alerts. It can even be set up to act as a full intrusion prevention system, blocking malicious communications. Snort accomplishes these duties by comparing rule sets to incoming traffic. These rule sets can be downloaded from the Snort website or other security sites, and they are updated on a regular basis to reflect new attacks. If you're thinking of installing Snort, make sure you read and understand the documentation beforehand. Advanced rule sets can be rather complicated, and they may or may not apply to your network architecture. It's customary to utilise Snort as a live traffic analysis tool, but you can alternatively employ a known good. Snort installation to evaluate captured traffic files. You can tell Snort to read any .cap(TCPdump-formatted) file and generate warnings from the file. Snort will typically output any warnings or alerts to the screen unless you designate an output file in which to save them.

The following code is an example of Snort alerts. As you can see, most alerts even offer links to Web sites for more information on the suspect traffic. These external references are indicated by

Xref=>.

```
[**] [1:587:8] RPC portmap status request UDP [**]
[Classification: Decode of an RPC query] [Priority: 2]
09/15-19:06:06.81952 210.114.220.46:653 -> 192.168.1.102:111
UDP TTL:47 TOS:0x0 ID:41887 IpLen:20 DgmLen:84
Len:56
[Xref=> http://www.whitehats.com/info/IDS15]
[**] [1:1971:4] FTP SITE EXEC format string attempt [**]
[Classification: Potentially bad traffic] [Priority: 2]
09/16-15:55:52.235847 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16648 IpLen:20 DgmLen:76 DF
***AP*** Seq: 0xCF7869CC Ack: 0xEBCD7EC0 Win: 0x7D78 TcpLen:
32
TCP Options (3) => NOP NOP TS: 237391678 29673183
```

If your profession requires you to investigate significant quantities of network traffic, you may wish to put up a known good Snort environment on your examination machine so that you may compare traffic captures to your tested and validated rules. One of the most basic tools in an expert investigator's toolkit is this way of immediately evaluating network traffic for probable criminal behaviour.

8.3 SUMMARY

Attackers are no longer required to break into an office or seek to circumvent firewall measures in order to get network access. Wireless networks have been compromised at BJ's Wholesale Club, Lowe's Companies Inc., DSW, Wake Forest University School of Medicine, and TJX. This chapter covers the fundamentals of wireless networks as well as the tactics used by hackers to attack them. Because of their anonymity and the difficulties of tracing down attacks, hackers have an advantage when it comes to wireless attacks. The results are enticing. Once a hacker breaks in, they bypass many of the usual network security barriers. A wireless network that was safe last year may not be as secure this year. The best way to prevent a wireless attack is to ensure the corporate wireless access point, wireless clients, and network configuration are as secure as possibly possible. Wireless networks can be more vulnerable to attacks than those on wired networks.

8.4 REFERENCES FOR FURTHER READING

Chapter 11 - Investigating Wireless Attacks, Editor(s): Dave Kleiman, Kevin Cardwell, Timothy Clinton, Michael Cross, Michael Gregg, Jesse Var Salone, Craig Wright, The Official CHFI Study Guide (Exam 312-49), Syngress, 2007, Pages 487-509, ISBN 9781597491976, <https://doi.org/10.1016/B978-159749197-6.50012>



EMAIL TRACKING AND EMAIL CRIME EXAMINATION

Unit Structure

9.0 Objectives

9.1 Introduction

9.1.1 E-mail Anatomy

9.1.2 Working with E-mail Systems

9.1.3 Protocols Used in Email Communication

9.1.3.1 Simple Mail Transfer Protocol (SMTP)

9.1.3.2 Post Office Protocol (POP3)

9.1.3.3 Internet Mail Access Protocol (IMAP)

9.2 Email Crimes

9.2.1 Phishing:

9.2.1.1 Types of Phishing:

9.2.1.2 Case Study: Bypassing Two-Factor Authentication

9.2.2 Spamming

9.2.3 Mail Bombing

9.2.4 Mail Storm

9.2.5 Sexual Abuse of Children in Chat Rooms

9.2.6 Child Pornography

9.2.7 Harassment

9.2.8 Identity Fraud

9.2.9 Chain Letter

9.2.10 Sending Fakemail

9.2.11 Email Harvesting

9.3 Investigating E-mail Crimes

9.3.1 Examining the E-mail Message

9.3.2 Copying the E-mail Message

9.3.3 Printing the E-mail Message

9.3.4 Viewing the E-mail Headers

9.3.5 Examining the E-mail Header

9.3.5.1 Microsoft Outlook

9.3.6 Tracing an E-mail Message

9.4 Tools and Techniques to Investigate E-mail Messages

9.5 Handling Spam

9.6 Network Abuse Clearing House

9.7 Protecting Your E-mail Address from Spam

9.8 Anti-Spam Tools

9.9 Summary

9.10 Reference for additional perusing

9.0 OBJECTIVES

Targets in this section: This part would cause you to comprehend the accompanying ideas:

- Working with E-mail Systems
- E-mail Crimes
- Investigating E-mail Crimes
- Tracing an E-mail Message
- Tools and Techniques to Investigate E-mail Messages

9.1 INTRODUCTION

During the 1960s Email was imagined however was utilized to a restricted limit and in a confined way; it just got well known by 1993. Email correspondence started the business transformation since it associated the planet. Albeit numerous cutting edge kinds of correspondences are created, email actually stays the principal well known inside the corporate world. As email correspondence thrived, it turned into a significant piece of our own and expert lives. Email is a vital piece of e-disclosure and scientific examination, particularly with the increment of cybercrime.

In this section, we will investigate diverse email wrongdoings and how their examination happens, by taking a gander at various contextual analyses. Email assumed a genuine part inside the examination of the Enron embarrassment, which we will see thereafter

Email Anatomy

The email comprises of two segments: Header and subsequently the Body. Each email includes a header, which might be a segment that contains data about the wellspring of the email and along these lines the way it went to prevail in the objective. The body of the email is the thing that we read

inside the email; it contains the message as well as any connections, which the sender has sent.

Working of Email System

The email framework might be a blend of equipment and programming parts, which incorporate the sender's and collector's customer and worker PC. The working of an Email System is displayed in Figure 1.

- An email customer is a Message User Agent (MUA), which is a product that sends and gets email. It changes the message over to an email message and sends it to the Message Submission Agent (MSA).
- In the Simple Mail Transfer Protocol (SMTP), the MSA decides the objective and resolves the area name to decide the completely qualified space name of the mail worker.
- The Domain Name System (DNS) worker checks the space against the rundown of mail trade workers in light of the solicitation.
- The message is then sent to the Mail Transfer Agent (MTA), after which it is conveyed to the post box by the Mail Delivery Agent (MDA).
- The message is gotten by the beneficiary's MUA utilizing either Post Office Protocol (POP3) or Internet Message Access Protocol (IMAP).

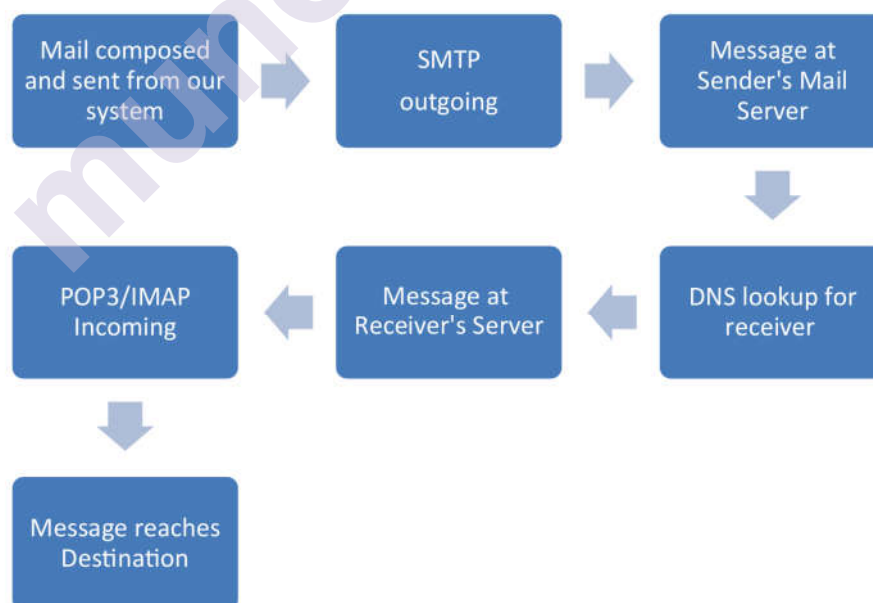


Fig.1Working of Email System

Conventions Used in Email Communication

Messages serve a major and basic part in electronic correspondence in the present advanced world. We have a bunch of conventions set up to make this electronic association conceivable and to send information between at least two associations.

1. Simple Mail Transfer Protocol (SMTP)

The Simple Mail Transfer Protocol (SMTP) is a web convention that permits you to send and get email over the web.

- The Simple Mail Transfer Protocol (SMTP) is a book based, application-level convention.
- For SMTP, the port numbers are 25 or 2525, or 587. Ports 465, 25, 587, and 2526 are utilized for secure SMTP (SSL/TLS).

2. Post Office Protocol (POP3)

This is a convention for recovering email from email workers by means of the web.

- All approaching messages are taken care of by the POP3 worker.
- Each worker is restricted to a solitary letter box.
- POP considers disconnected admittance to interchanges, decreasing the measure of time spent on the web.
- The POP3 convention is normally utilized on two ports: port 110, which is the default non-encoded POP3 port, and port 995, which is utilized when encryption is required.

3. Internet Mail Access Protocol (IMAP)

To get to the email on the mail worker, you'll need to utilize the web message access convention.

- The far off worker stores and oversees email.
- It permits clients to download and dispose of messages without understanding them.
- Support for numerous letter drops is accessible.
- Appropriate for connections.
- The IMAP convention runs on port 143, with SSL/TLS-encoded IMAP running on port 993.

9.2 EMAIL CRIMES

As the quantity of computerized residents expanded to millions, so did the quantity of violations connected to email. New clients, then again, are not

given any directions or tips on the best way to be protected on the web. Large numbers of these people in the end become obvious objectives for programmers and fraudsters who misuse their data and, much of the time, request cash. Email violations incorporate phishing messages, extortion messages, badgering messages, etc. Email has customarily been utilized to advance middle class wrongdoing, yet it is presently now being utilized to spread illegal intimidation and by stalkers to impart dangers.

Phishing

Phishing tricks are for the most part messages that lead to the assortment of fundamental and delicate data, for example, financial balance numbers, charge card numbers, and government managed retirement numbers, and the abuse or unlawful offer of such data. The assault is most ordinarily conveyed as a mock email correspondence that seems to come from an individual accountable for a definitive position or a known or individual associate, yet it can likewise seem to come from an individual responsible for a legitimate position or a notable bank, shopping entryway, inn, and so on. This happens when a cybercriminal tricks a casualty into opening an email by having all the earmarks of being a confided in association. The collector is then convinced to tap on a noxious connection or archive, which may bring about the establishment of malware (a malevolent programming), compromising all touchy information on the machine.

Phishing is every now and again utilized as a component of a more extensive attack, like a high level diligent danger (APT) occasion, to acquire admittance to business or administrative organizations by alluring and focusing on guiltless faculty. Numerous laborers are compromised in this segment to bypass security borders like firewalls, endpoint security, and email security, disseminate malware inside a shut climate, or get restricted admittance to all watched information and data.

An association that succumbs to such an assault is probably going to endure critical monetary and reputational harm. Contingent upon the broadness, a phishing endeavor may transform into a security emergency, making it hard to recuperate and recover piece of the pie.

Sorts of Phishing:

Phishing Attacks: There are a few kinds of phishing assaults:

- As the name infers, skimmer phishing by and large focuses on a particular individual or association. Phishers scour the web for any accessible data on their objective so they may assemble a conceivable and genuine looking email to extricate data (if not cash) from their planned casualties.
- Whaling is a sort of lance phishing assault focused on chiefs or other high-profile focuses inside an organization, government, or other private associations, like a COO, CEO, or another person with admittance to monetary information or resources. A typical illustration of whaling is CFO extortion. It as a rule targets high-profile focuses to

take vital and touchy information from a partnership. These are individuals who have absolute admittance to delicate data.

- Smishing is a sort of SMS phishing that happens through instant message on cell phones. Vishing, or voice phishing, is a comparative technique that utilizes the telephone.
- Deceptive Phishing: For this situation, the sender camouflages (causes it to seem bona fide) email ids as an authority and unique organization's email address, captivating and asking individuals to tap on the fake connections provided in the email. Ordinarily, cybercriminals focus on their casualties utilizing mass email systems.
- Pharming, otherwise called DNS-based phishing, is the change or altering a framework's host records or area name framework to divert URL inquiries to a counterfeit site. Thus, customers have no clue about that the site into which they are putting their own data is a falsification.
- Content-infusion phishing happens when tricksters/phishers present unsafe code or misleading substance into certified sites that demand clients' passwords or individual data. This phishing endeavor is progressing as a feature of the substance caricaturing attack.
- Search motor phishing happens when tricksters or phishers foster destructive sites with captivating stunning offers and list them in web indexes. As the aphorism goes, "Unrealistic," clueless casualties are attracted to such locales while directing their own web look and erroneously accept these destinations are genuine, incidentally uncovering the entirety of their own data.

The unforgiving the truth is that there are a great deal of phish in the ocean! A phishing attack is the beginning stage for by far most of information break endeavors. Lamentably, regardless of how protected or the number of various assurances an organization takes, some phishing messages will consistently crawl and advance into a casualty's inbox. Also, those messages are exceptionally effective — by far most of people on earth can't recognize a shrewd phishing email. This is the place where client mindfulness and representative instruction become an integral factor and are basic.

Contextual analysis: Bypassing Two-Factor Authentication

Programmers effectively bypassed Google's two-factor validation (2FA) and accessed Gmail accounts. Programmers utilized this astute mission to acquire admittance to many Google and Yahoo accounts to bypass two-factor validation. Here's the means by which the attack worked (the time is significant):

1. A programmer makes a sham Gmail login page.
2. The programmer sends the casualty a phishing Gmail security cautioning (Your Gmail account has been restricted for security reasons. To reactivate the record, you should login (blah, blah, blah,)
3. The casualty taps the phishing join and is shipped off a sham Gmail confirmation screen.
4. The casualty enters a login and secret word.
5. The programmer acknowledges the login and the casualty is then furnished with a 'Kindly info 2-Factor Authentication code:' brief.
6. Hackers in a far off area open a genuine Gmail page and sign in with the casualty's seized login and secret phrase.
7. A real Gmail acknowledges the login and sends a SMS message with two-factor verification to the casualty's telephone.
8. The casualty enters the 2FA code from the SMS onto the phishing site.
9. The programmer acquires the 2FA code and transfers it to a real Gmail account.
10. The programmer acquired admittance to the casualty's Gmail account. Source: motherboard.vice.com/en_us/article/bje3kw/how-programmers-sidestep-gmail-two-factor-validation.

Spamming

Spamming is the demonstration of sending spontaneous business email correspondences (UCE). Garbage mail is a more continuous word for spam. Spammers gather email addresses from Usenet, bots, posts, DNS postings, or potentially Web pages.

Spammers are shrewd, persuaded hooligans who are knowledgeable in innovation.

They will go to any length to access email records, unstable workers, and unreliable switches. Spammers bring in cash while staying mysterious by utilizing their insight and all around made instruments.

Spam is ordinarily shipped off countless email addresses simultaneously.

Much of the time, the e-sender letters' location is faked, permitting spammers to hide their personality. The From and Reply To fields in an Internet email header empower the spammer to give mistaken or deceiving data to urge the beneficiary to open the email.

Spam might be ordered into two classes dependent on its substance: spontaneous mass email (UBE) and spontaneous business email (UCE)

(UCE). Spam is sent by means of a faked email address or through business mass-mailing programming.

A spammer is an individual or element who conveys spam messages.

Mail Bombing

Mail bombarding is a clear assault that has been drilled for quite a while. It involves sending various duplicates of an email to a beneficiary with the aim of doing as such. The objective is simply to overpower the email worker. This is refined by either flooding the worker associations or spilling over the client's inbox to where the person in question can't get to additional messages. Flooding worker associations would be aimed at the general framework, while flooding an inbox would be aimed at a particular person. Mail bombarding is unsafe and oppressive, regardless of whether it is aimed at a particular individual to keep different clients from getting to the mail worker.

Mail Storm

A mail storm is a circumstance that emerges when PCs start to impart all alone. This system produces a lot of garbage mail. This may happen accidentally because of email message auto-sending when arranged to countless mailing records, the utilization of programmed answers, and the utilization of various email accounts. Pernicious programming, for example, the Melissa and IloveYou infections, can likewise cause mail storms. Mail storms upset an email framework's typical correspondence.

Sexual Abuse of Children in Chat Rooms

The developing utilization of texting, Web discussions like Facebook, and talk rooms has expanded the chance of rape. It is ordinary for pedophiles to use web visit rooms to physically mishandle young people by starting associations with them. This normally involves become a close acquaintance with the youth, fabricating a steady association, and afterward progressively acquainting the kid with porn through photographs or recordings that may contain physically unequivocal material. Kids might be misused for cybersex from the outset, and after trust is set up, this may develop to actual maltreatment.

Kid Pornography

Kid porn is characterized as any material that shows youngsters' sexual action. The obscurity and simplicity of move managed by the Internet have brought about a worldwide issue with kid porn. Kid porn misuse can bring about long haul torment and other unsafe outcomes. Those in the kid porn business some of the time target impeded youths by promising money or different motivators. Youngsters who are casualties of sexual abuse may experience the ill effects of trouble, enthusiastic brokenness, fear, and uneasiness for the remainder of their lives.

Badgering

Badgering may happen in numerous sorts of media, including the Internet. Garbage mail, physically unseemly email correspondences, and dangers passed on the web (through email and texting) are generally instances of provocation. Provocation of this nature is a criminal offense. Another kind of badgering is the unseemly admittance to physically express, bigot, or in any case shocking data at work. This incorporates sending undesirable interchanges to an associate that may contain unseemly data.

Character Fraud

Data fraud is developing progressively normal because of its effortlessness and benefit. This lead involves taking somebody's personality to get unscrupulous monetary advantage. It is, truth be told, burglary. To take a personality, email correspondences with unrealistic offers, fake Web locales, and different kinds of phishing are utilized. Numerous gatherings have some expertise in data catch and monetary gaming by offering this data to parties that will direct unapproved buys or monetary exchanges.

Networking Letter

Another sort of misuse that has easily moved from the actual world to web is junk letters. A networking letter is an email that was sent consecutively starting with one email client then onto the next. It will typically encourage the beneficiary to advance further duplicates of the email to various beneficiaries. These junk letters every now and again offer prizes or otherworldly advantage for sending the email and may likewise undermine misfortune or harm if the recipient doesn't communicate it. The authenticity of a networking letter is now and again obscure since the first sender's header data is lost during retransmission.

Sending Fakemail

Fakemail is any email that has been manufactured or controlled here and there. It is oftentimes utilized in spamming to hide the beginning location. Email caricaturing is a technique for sending adulterated or fake mail. Entering another person's email address in the `to` or `cc` boxes permits you to send a phony email. These may likewise incorporate data about the message's starting point.

Fakemail might be effectively produced by interfacing with TCP port 25 with any telnet customer. At the point when this is finished, the PC is quickly associated with the SMTP (Simple Mail Transfer Protocol) daemon working on that host. Fakemail would then be able to be sent by sending SMTP guidelines to the SMTP daemon. For instance, you send a fake email to

Enter the accompanying message into `Bill.Gates@Microsoft.com`:

Username HELO

EMAIL: `president@Whitehouse.gov`>

TO: Bill.Gates@Microsoft.com> RCPT TO: Bill.Gates@Microsoft.com>

Information

This is a note to thank you for your help with assisting me with winning the political decision.

President Bush surrendered.

Fakemail might be shipped off anybody and will hope to have come from the location determined via the "Post office FROM:" box. Fundamentally, fakemail is utilized to perpetrate criminal misrepresentation.

Email Harvesting

The obscure and generally criminal behavior utilizes a mechanized programming to filter pages and assemble email addresses for spammers to use in sending spam messages.

9.3 INVESTIGATING EMAIL CRIMES

To explore email violations and infractions, you should make the accompanying strides: Study the email message, duplicate it, print it, see the email headers, look at the email headers, assess any connections, and follow the email.

Coming up next are the means in the insightful cycle:

1. Inspecting the email message
2. Replicating the email message
3. Printing the email message
4. Review the email headers
5. Inspecting the email headers
6. Inspecting any connections
7. Following the email

1. Inspecting the E-mail Message

At the point when it is resolved that a wrongdoing was perpetrated by means of email, gather and protect the proof expected to demonstrate the offense in a courtroom. Proof can be accumulated by investigating the casualty's PC. This may be the email that the casualty got.

Likewise with any advanced measurable work, an image of the machine's hard circle ought to be taken first.

It is helpful to get any passwords needed to open ensured or scrambled documents while investigating the casualty's framework. At the point when actual admittance to the casualty's PC is unimaginable, a printed

duplicate of the culpable email (with the whole header) ought to be made. Albeit the novel IP address of the worker that sent the message might be produced, this is troublesome and far-fetched. Much of the time, the IP address of the source post in the email will compare to the guilty party's host.

2. Replicating the E-mail Message

An email request might be dispatched when the hazardous message is duplicated and printed. Any email application, like Eudora or Outlook Express, might be utilized, and straightforward advances can be given to move the email message from the Inbox envelope to a circle or other source.

To repeat an email in Microsoft Outlook or Outlook Express, play out these means:

1. Supplement an arranged USB streak crash into the framework.
2. Explore to the USB key utilizing My Computer or Windows Explorer.
3. Start by opening Microsoft Outlook.
4. Keep the Folder List open when opening the envelope containing the tricky message.
5. Resize the Outlook window with the goal that you can see both the replicated message and the floppy plate symbol.
6. From the Outlook sheet, drag the message to the circle envelope connected with the USB key.

Replicating the email message is likewise conceivable with order line email applications like Pine. The methodology is ordinarily novel to every product.

3. Printing the E-mail Message

It is a smart thought to print the email message whenever it has been replicated. The essential benefits of printing are that a straightforward method can be distantly passed on to a client and that it produces results that might be utilized in court. The accompanying directions represent how to print an email message from Outlook Express:

1. Navigate to My Computer or Windows Explorer and save a duplicate of the casualty's email message.
2. Launch the email programming and open the message.
3. Select Print from the File menu.
4. After you've picked your printing choices in the discourse box, click Print.

5. Open the email message in an order line email customer, for example, Pine or Eudora and pick the Print alternative.

4. Review the E-mail Headers

A message header and a subject body make up an email message. The powerful catch of the email header may represent the deciding moment a request utilizing email. The email header is fundamental since it contains data about the e-beginning. mail's This will uncover the IP address from whence it began, the strategy used to communicate it, and maybe who sent it. The message is contained in the e-subject mail's body. The email header might be gotten subsequent to replicating the email message. This method varies relying upon the email application.

Recovering the E-mail Header (Microsoft Outlook)

1. Launch Outlook and explore to the replicated email message.
2. To open the Options discourse box, right-click the message and select Options.
3. Select the header text and copy it.
4. Copy and glue the header content into any word processor, then, at that point save the record as Filename.txt.
5. Press Alt-P> to catch a screen shot of the header. This picture ought to be printed.
6. Make a duplicate of the email message and save it as message. 1.msg
7. Exit the application.

Recovering the E-mail Header (Hotmail)

1. Navigate to Hotmail and sign in utilizing your Web program.
2. Open the fitting email message.
3. Select Preferences from the Options menu. Snap Mail Display Settings for variant No.8.
4. Select Advanced Header starting from the drop menu. Go to Message Headers and pick the Advanced alternative for variant No. 8.
5. Select and duplicate the message heading content.
6. Save the document as Filename.htm subsequent to choosing the message header content.
7. This can likewise be cultivated by putting away the information related with the header's "see source."
8. Press Alt-P> to catch a screen capture of the header. This picture ought to be printed.
9. Exit the application.

Recovering the E-mail Header (Yahoo)

1. Launch Yahoo.
2. On the right, select Mail Options.
3. Navigate to the General Preferences interface and pick Show All Headers On Incoming Messages prior to saving the message.
4. Save the document as Filename.htm subsequent to choosing the message header content.
5. This can likewise be cultivated by putting away the information related with the header's "see source."
6. Press Alt-P> to catch a screen shot of the header. This picture ought to be printed.
7. Exit the application.

5. Inspecting the E-mail Header

Email headers are a helpful wellspring of data. They can reveal to you the working framework and adaptation of the email sender's working framework, the email program utilized and its form, the usernames on the framework used to send and get email, just as the framework hostname and Internet Protocol (IP) addresses.

The most productive approach to get the important email for assessment is to ask the individual who got it. It is typically desirable over have somebody at the objective site send you an email message if conceivable. Frequently, programmed deals records and framework re-mail or rundown highlights are adequate to get an email header for correlation. Do this for each site that you are allowed to assess. Email headers may likewise be caught by deliberately sending an invalid email to the objective site. This will result in a "skip" returning as undeliverable.

Albeit this isn't generally the situation, the ricochet may contain some inside data. The email applications, working frameworks, inward hostnames, and inner framework sorts are uncovered by dissecting the header. The extraordinary sender's IP address gave inside the email header is the main data fundamental when examining an occasion dependent on an email. The email header likewise incorporates other data, for example, the date and time the message was sent (a timestamp), any connections and their arrangement, and the message content. The header may likewise contain data that might be utilized to recognize the customer machine remarkably.

In this part, we will walk you through the cycles needed to examine the email header. The header is caught by following the methods laid out in the former segment.

In the event that the email message header is effectively examined, it can give significant data. Figure 1 shows an illustration of an email header.

6. Inspecting any connections

Email header investigation gives us data about the aggressor, for example, SMTP worker subtleties, the assailant's and casualty's IP addresses, the timestamp when the email was sent, and connection record data. Numerous business and web programs for examination are accessible, including www.ip-adress.com, emailtracker ace, MailXmainer, MX Toolbox, and others. The ip-adress instrument will be utilized to look at an email header and fathom the different fields demonstrated in the header.

When the IP is resolved to be genuine, the entirety of the data is assembled, and the related Internet Service Provider (ISP) is called, and the client data for the IP is mentioned. The ISP hence sends the client data to the examiners, who, with the help of neighborhood law implementation specialists, track out the culprit.

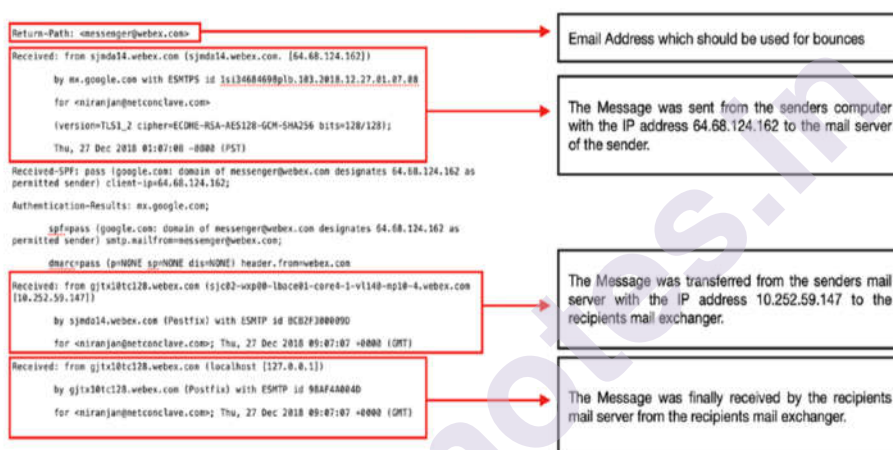


Fig.1 Sample Header with explanation 1



Fig.2 Sample Header with explanation 2

Email Tracking result as shown in the figure

IP-ADDRESS.COM	
Home	My IP
Speedtest	Stemap
Search Website, Domain, Host, or IP address	
Phony Checker	Phony List
Verify Email Address	Trace Email Address
IP to Zip Code	IP Address Distance
Email Sender	messenger@webex.com
IP Address	64.66.124.162
IP Address Country	United States of America
IP Address State	
IP Address City	
IP Address Postcode	
IP Address Latitude	37.7510
IP Address Longitude	-97.8220
ISP of this IP	Cisco Webex LLC
Organization	Cisco Webex LLC
Timezone	
Local Time of this IP country	

Contextual investigation: Email Hoax

A decent inn got an alarm when a 40-year-old miserable person composed a phony email to the inn, causing the workers to remain alert for longer than seven days. On June 1, an email with the title "Bombs in Hotel" showed up in the inbox of the lodging's email ID from an aggressor utilizing yahoo.com email. Coming up next are the email's substance (unedited):

Greetings,

3 bags loaded up with 20 Kg of RDX has been put in your lodging. In the course of the most recent 3 days, we have effectively avoided all your security frameworks. The detonator for each of the 3 explosives will be constrained by a cell phone. At the point when I call the numbers, the explosives will go off and annihilate your inn. You have 24 hours to convey Rs 5 Crores else witness the annihilation of your inn.

You will send 2 Bank DD's every one of Rs 2.5 Crores to the accompanying location:

(his significant other's Bangalore, India address referenced here)

Try not to sit around idly, the explosives will be set off at precisely 2 pm on Wednesday, June 2, 2010. This email isn't a deception. You are encouraged to view it appropriately to stay away from a great many dollars of harm and death toll. The dread alarm is genuine, this is my last admonition!

In any case, the phony email sender was captured in Bangalore after the lodging's associate security chief cautioned Cyber Crime unit authorities.

The messages and other data were provided to us by inn the board. Since the records were Yahoo's, we reached Yahoo and got data on the record, which was set up for the sake of xxxx@yahoo.com. Hurray outfitted us with the IP address data.

Utilizing ip-adress.com, we performed header investigation and found that the IP address had a place with a digital bistro in Bangalore. It was an Airtel web association, and with Airtel's assistance, we situated out the real area of the digital bistro from where the messages were sent. We then, at that point dispatched a group of experts to direct more examinations.

The culprit had sent two sham messages to the inn. His significant other had deserted him, leaving him down and out, as per examinations. This propelled him to send an email to her, so he made an email address in her name. He further mentioned that 7,000,000 USD (the Rs. 5 crores referenced in the email) be shipped off her nearby home location.

7. Following an E-mail Message

The beginning host framework's IP address can help you in deciding the proprietor of an email address that has been utilized in a presumed occurrence or wrongdoing that is being examined. This data is vulnerable to imitation. Continuously twofold check any proof you find. An assortment of sites can help with tracking down the proprietor or dependable element connected with the space name.

A portion of these are:

- www.arin.net The American Registry for Internet Numbers (ARIN) might be utilized to decide an area name dependent on an IP address. It likewise furnishes the contact data related with a space name.
- <http://www.freeality.com/> This site gives an assortment of search prospects, including email addresses, telephone numbers, and names. Clients may do invert email look on the site, which may help in deciding the subject's actual personality. This site likewise gives switch telephone number and address queries.
- www.google.com The Google web crawler might be utilized to discover practically any data. The Google Groups and Advanced Groups Search highlights empower you to look through a solitary newsgroup or all newsgroups utilizing catchphrases, message IDs, or creators. A lot of data might be recovered by putting an email address connected with the examination's theme into the "Writer" field, including any articles that the suspect has posted.
- www.internic.com This site has a similar substance as www.arin.net. These sites help examinations by following the email message and giving pivotal proof, like a presume's contact data.

9.4 TOOLS AND TECHNIQUES TO INVESTIGATE E-MAIL MESSAGES

To build up the legitimacy and get proof connected to email, the legal specialist may utilize an assortment of instruments and methods. This part goes through a couple of these instruments and approaches.

Utilizing Logs to Analyze E-mail

It is basic to check and confirm the email address, source, and way in any request including email. Framework logs are utilized to affirm the course that email has voyaged. Through their logs, switches and firewalls give fundamental approval of the email worker and the way gave inside the email header. Despite the fact that it is doable to just satire an email header, it is almost difficult to undercut all organization hardware and workers along the email's transmission way.

You may check the legitimacy of data included inside the email header by joining organization and framework logs from the source, objective, and delegate gadgets and workers along the way of the email. In the event that there are any irregularities among frameworks and logs, all things considered, the email header has been altered.

Analyzing Network Equipment Logs

It is attainable to approve the timings and IP addresses included inside the email header by investigating organization and firewall logs.

Switches and firewalls may both be arranged to screen and log approaching and departure traffic as it goes through them. Switches and firewalls regularly create log documents in this interaction. These log documents oftentimes contain email message ID data just as the source and objective locations of the workers used to convey email.

Inspecting UNIX E-mail Server Logs

Sendmail is the chief program for sending email on a Linux or UNIX framework. The logs and the arrangement record (sendmail.cf) both give significant data. Syslog is utilized by both Linux and UNIX to monitor what has occurred on the framework. The design document/and so forth/syslog.conf indicates where the syslog administration (or daemon known as Syslogd) conveys its logs.

The syslog setup document incorporates valuable data like the logging need, where logs are conveyed, and what different activities might be finished. Sendmail may create occasion messages and is regularly set up to record essential data, for example, the source and objective locations, the sender and beneficiary locations, and the message ID of the email. The syslog.conf document will legitimately show the area of the email log record.

This is frequently/var/log/maillog. This document frequently contains the source and objective IP locations, date and time stamps, and other data that might be utilized to affirm the data in an email header.

Analyzing Microsoft Exchange E-mail Server Logs

The Microsoft Extensible Storage Engine is utilized by Microsoft Exchange (ESE). While looking at email got utilizing a Microsoft Exchange worker, the agent is principally worried about the framework's

EDB documents, STM data set records, designated spot records, and transitory documents.

EDB data set documents are utilized by more established forms of Exchange. Both EDB and STM designs are utilized in late forms of Microsoft Exchange worker (2000 and past). EDB and STM data set records are utilized to create email message extra room. To safeguard the pre-arranged email, including the MAPI (Message Application Protocol Interface) metadata, an EDB document is utilized.

The STM data set contains records that are not MAPI-arranged. To monitor and execute changes to the data set document, Microsoft Exchange utilizes an exchange log. In this way, the exchange log might be used to recognize whether an email was sent or gotten by the email worker. To demonstrate the past point in time when the information base was last saved to plate, Exchange worker uses designated spot records that are composed into the exchange log.

Designated spots let the framework chairman (and hence the measurable examiner) decide whether any information misfortune has occurred since the past reinforcement was performed, permitting the framework head (and along these lines the criminological agent) to recuperate lost or erased messages.

Microsoft Exchange utilizes transitory documents (or TMP records) to store data that is gotten while the worker is too occupied to even think about dealing with it right away. RESx.logs is utilized to safeguard data set flood data. The framework doesn't erase these transitory records and they can be recovered.

A following log on the Exchange worker might be seen utilizing the Windows Event Viewer. Microsoft Exchange has a message-following capacity with a verbose mode. It is additionally conceivable to see the message content connected with the email in this mode. The occasion watcher additionally gives helpful data about email messages sent and got through the worker.

On the off chance that the Exchange investigating or symptomatic logs are empowered, they can likewise give supportive data. The Window Event Viewer is utilized to peruse these log documents. For every email letter sent or got, countless occasions are logged. Besides, the Event Properties discourse box will give additional data.

Specific E-mail Forensic Tools

Specific criminological instruments, like FINALEMAIL, Sawmill-Group Wise, and Audimation for Logging, are proposed especially to recuperate email and connections. When joined with information recuperation apparatuses (like FTK or EnCase), a system might be worked to find and recuperate any log records, email data sets, individual email stockpiling documents, and disconnected stockpiling records.

Email recuperation programming will recover information from an email worker or a customer PC. You might have the option to approve an email or set up that it is reasonable phony by looking at the gathered log and worker data with the casualty's email message.

Email Examiner

The E-mail Examiner utility aids the recuperation of erased email and different messages. After the erased things organizer has been purged, this program reestablishes erased email.

Email Examiner can assess more than 14 email data set sorts on Windows 95, 98, NT4, 2000, 2003, ME, and XP. AOL, Calypso, EML Message records, Eudora, Forte Agent, Juno 3.x, Mozilla Mail, MSN Mail, Netscape Messenger, Outlook Express, Outlook Exchange, Pegasus Mail, PocoMail, USENET Groups, and an assortment of extra organizations are upheld.

FINALEMAIL

FINALEMAIL is proposed to look through an email data set for erased email messages. It is particularly helpful for recuperating email messages when the information area data has been lost or erased. This covers cases when damage has happened because of infection contamination, cancellation, or plate reformatting. This program might be utilized to reestablish singular messages or entire data set records back to their unique state. Standpoint Express and Eudora data set configurations are upheld by FINALEMAIL.

Organization E-mail Examiner

Organization Email Examiner can dissect a wide scope of email information base arrangements. The instrument shows and cycles the entirety of the email accounts in the data store or information base, just as the entirety of the related meta-information. The program works with both Microsoft Exchange and Lotus Notes information stores, including Microsoft Exchange Information Store variants 5.0, 5.5, 2000, and 2003, and Lotus Notes Information Store renditions 4.0, 5.0, and 6.0.

Coming up next are a portion of the instrument's key highlights:

- A independent, straightforward User Interface (UI)
- Bookmarking
- Support to trade information into Paraben's email inspector
- An progressed search work

Organization E-mail Examiner is intended to work pair with Paraben's E-mail Examiner, and the yield is in a similar arrangement. Organization E-mail Examiner may send out an entire mail store and even believer it to an other arrangement.

R-Mail

R-mail is an email recuperation program that can reestablish erased email correspondences. This program is expected to recuperate Outlook Express email. The program can repair.dbx documents that have been harmed by erasure. It's anything but, a licensed email reclamation procedure that can remake broken *.dbx records to recuperate lost email messages. The program stores recuperated email messages in.eml design, which might be brought into Outlook Express. This procedure is particularly valuable when a suspect has deleted email correspondences intentionally.

Following Back

Email following starts with checking the email header. Check the data included inside the email header (containing the subject, date, Sent From, and Received To addresses). The Sent From line contains the source IP address of the host that sent the email just as the sender's email address (which might be caricature without any problem). The Received To lines show to each host that the email has been prepared by finishing up with the date and time that the email was taken care of.

Continuously remember that, except for the Received segment, all lines in the email header can be faked. This is the reason the header data from different sources should be approved. On the off chance that the header data has been approved, the first email worker ought to be used as the essential source to follow back to (utilizing the procedures recorded before in this part).

Following this, it is practical to move toward the court and look for a court request to gather the log records from the source worker. This data may be utilized as proof to build up the sender's actual personality.

Following Back Web-Based E-mail

Online email suppliers (like Hotmail or AOL) may every now and again make following the sender troublesome. The administrations permit clients to send and get email from anyplace on the planet. A considerable lot of these administrations are free, and no confirmation or proof of character is required while enlisting for a record. Accordingly, coordinated criminal gatherings habitually set up fake email accounts with bogus data.

The extraordinary IP locations can in any case be recovered to find a suspect. Most Web-based email suppliers (counting Hotmail and Yahoo) track the IP address of any host that utilizes their administrations. Moreover, most Web-based email frameworks will give the exceptional IP address in the header data.

Looking through E-mail Addresses

You can use web indexes to expand the amount of data you have on the suspect. Most Internet web search tools will give additional data about the suspect by contributing contact information, (for example, email addresses, the speculate's name, telephone number, or areas).

When searching for email addresses, the accompanying web indexes are habitually utilized:

- <http://www.altavista.com> Altavista's landing page has a "Group Finder" alternative. It has two inquiry alternatives: telephone and email. By contributing the individual's initials or the entire last name, you may discover their email address, telephone number, and surprisingly a record verification.
- www.infospace.com InfoSpace gives a converse query alternative to help you in following an email way. You can utilize email registries and freely available reports to assist you with your exploration.
- <http://www.emailaddresses.com/> This site offers a free email address registry. The catalog contains a wide scope of data and empowers for looking by area just as converse queries.
- Google (www.google.com) Many people presently use Google as their essential web search tool. The utilization of the web search tool has brought forth a whole subculture known as Google Hackers.

Email Search Site

The site www.EmailChange.com offers a free email address change register and web search tool. It very well may be utilized to chase down speculates who have exchanged email addresses. By entering the suspects' earlier email addresses into the hunt site, their new email addresses are often recognized.

9.5 HANDLING SPAM

www.EmailChange.com gives a free email address change vault and web search tool. It could be utilized to find presumes who have changed their email addresses. The speculates' new email addresses are typically found by putting their past email addresses into the pursuit site.

On the off chance that you get spam from a specific location consistently, you might have the option to report the occasion to the FTC (The United States Federal Trade Commission) by messaging a duplicate of the spam message to spam@uce.gov. The FTC additionally has an online objection structure accessible at www.ftc.gov. You should incorporate the email header when recording an objection.

The email header gives the data that buyer security specialists need to react to a spam grievance. A duplicate of the spam can be given to the ISP to make them aware of the spam issue on their organization and help them in lessening future occasions.

9.6 NETWORK ABUSE CLEARING HOUSE

The Network Abuse Clearing House (www.abuse.net/) was set up to help Internet clients report harmful conduct. It is planned to help in the

administration and minimization of organization abuse. The quantity of reports of misuse has developed pair with the quick extension of Internet wrongdoing. The Network Abuse Clearing House has a complete data set of all objections got.

This data set might be gotten to utilizing the accompanying techniques:

- Using a mail sending administration
- Using a web index
- Through the utilization of a space name query
- Using a WHOIS worker

Abuse.net is neither a boycott or obstructing rundown, and it doesn't reject or boycott email.

9.7 PROTECTING YOUR E-MAIL ADDRESS FROM SPAM

Email spammers utilize a data set of email addresses assembled by means of address reaping on the Internet. Email locations might be acquired by means of mailing records and Internet news bunch postings, just as Web destinations, Internet talk rooms, and surprisingly the enrollment registry of an online business. To shield email addresses from spammers, limit the occasions (assuming any) they are distributed in broad daylight.

Space keys and other encoding methods can be utilized to restrict others' capacity to mishandle email accounts. These advances utilize cryptographic cycles on email interchanges (for instance, by adding a computerized signature) to help the recipient in affirming the beginning and validness of an email. They approve the area first, then, at that point match it to the space determined in the sender's "From" field. In the event that an email is genuine, it is conveyed to the client's letter box. Else, it will be returned. The whole activity happens on the worker level.

9.8 ANTI-SPAM TOOLS

In this segment, we'll examine a few apparatuses that have been created to assist you with limiting SPAM.

Enkoder Form

Enkoder Form is expected to ensure against email reaping. It permits you to scramble email addresses into JavaScript code, which is apparent to real programs however undetectable to many robotized spam programs. It aids the insurance of email tends to displayed on HTML-coded Web pages.

Email locations can be encoded utilizing the essential structure accessible at <http://hivelogic.com/enkoder/structure>. Round out the structure with your data and afterward click the Encode It button. A JavaScript code is created that might be promptly embedded into the HTML code of a Web

page where the email address will be shown. A Web program may see the recently created interface.

eMailTrackerPro

eMailTrackerPro looks at the email header to decide the IP address of the PC that sent the email. It will likewise give data about the sender's geological area. In light of this usefulness, this device is particularly significant for abstaining from spamming and mocking. This program is available at www.emailtrackerpro.com.

By sending a manufactured message to the recipient, an email falsifier (spoofers) might be planning to cause trouble, start a monetary wrongdoing, or even slander the individual being caricature. eMailTrackerPro Advanced Edition incorporates an online email checker, which permits you to see all email messages on the worker before they are communicated to your PC.

The underlying area data set of the product tracks email interchanges to a specific country or space of the world. eMailTrackerPro additionally upholds hyperlink osmosis through VisualRoute.

Aggressors can in any case evade this by utilizing a Web-based email anonymizer administration. For standard email correspondences, open mail transfer workers can be used. The IP address of the anonymizer firm, not the presume's location, will be shown.

SPAM Punisher

SPAM Punisher is an enemy of spam program that assists you with discovering a spammer's ISP address. It recognizes counterfeit locations consequently and works with various email customers (counting AOL, Hotmail, Microsoft Outlook, and Eudora).

SPAM Punisher parses email headers for IP locations and afterward endeavors to figure out which IP addresses are phony. It then, at that point permits you to handily email a protest to the pertinent maltreatment address. Spam Punisher's protest formats are completely adaptable. Spam Punisher is viable with Windows 9x/ME/NT/2000/XP.

9.9 SUMMARY

In this section we took in the accompanying:

- Phishing tricks are by and large messages that lead to the assortment of basic and delicate data, for example, Visa numbers, government managed retirement numbers, and financial balance subtleties, which are then abused or sold unlawfully.
- Spam is spontaneous and undesired email that enters our inbox. Spammers send 'Garbage Mail' to a great many beneficiaries' inboxes.

Greylisting, Content Filtering, and DNS Blacklisting are some enemy of spam strategies.

- Email bombarding is a procedure where the assailant fills the casualty's letter drop with an enormous number of messages in a brief timeframe. The's aggressor will probably overpower the post box with traffic.
- Email legal sciences is the part of digital crime scene investigation that examinations and looks at the substance and segments of messages utilizing apparatuses and systems.
- Email headers are a significant wellspring of data since they incorporate the metadata that is joined to each email and help the legal sciences specialist break down and look at the email ancient rarities.
- Email header investigation furnishes us with data about the assailant, for example, SMTP worker subtleties, the aggressor's and casualty's IP addresses, the timestamp when the email was sent, and connection document data.
- If the evidence email is demonstrated to be spam, the experts will mastermind snare to capture the culprit. This is alluded to as the snare technique.

9.10 REFERENCE FOR FURTHER READING

1. Practical Cyber Forensics_An Incident based Approach to Forensic Investigation, Niranjana Reddy, Apress Publisher, 2019.
2. The official CHFI Exam 312-49 study Guide, Dave Kleiman, SYNGRESS Publisher, 2007.
3. Digital Forensics and Incident Response, Gerard Johansen, Packt Publishing, 2020.
4. EC-Council CHFI v10 Study Guide, EC-Council Publisher, 2018.
5. <https://emailheaders.net/forensic-email-search.html>
6. <https://pdfs.semanticscholar.org/8625/a3b17d199e5cabb796bad0df56a7979c77c.pdf>
7. <http://jpsra.am.gdynia.pl/upload/SSARS2016PDF/Vol1/SSARS2016-Charalambous.pdf>
8. <https://cyberforensicator.com/wp-content/uploads/2017/01/SSARS2016-Charalambous.pdf>



MOBILE FORENSICS, REPORTS OF INVESTIGATION, BECOME A PROFESSIONAL WITNESS

Unit structure

10.0 Objectives

10.1 Introduction Mobile Forensics

10.1.1 Acquisition Protocol

10.1.1.1 Case Study: Unlocking with Face ID or Touch ID

10.1.2 Android OS

10.1.2.1 Rooting an Android Device

10.1.2.2 Android Debug Bridge

10.1.2.3 Methods for Screen Lock Bypass

10.1.3 Manual Extraction

10.1.4 Physical Acquisition

10.1.4.1 Tools for Image Extraction

10.1.4.2 Case Study: Image Extraction of an Android Device

10.2.4.3 JTAG

10.1.5 Chip-Off

10.1.6 Micro-read

10.1.7 Challenges in Mobile Forensics

10.1.8 iOS OS

10.1.8.1 iOS Device Boot Process

10.1.8.2 Jailbreak vs. No Jailbreak

10.1.8.3 iOS file system and Architecture

10.8.3.4 iTunes iPhone Backup

10.1.9 Case Study: iPhone Backup Extractor

10.1.10 Case Study: Dr. Fone iPhone Backup Viewer

10.2 Writing Investigative Reports

10.2.1 Understanding the Importance of Reports

10.2.2 The Requirement of an Investigative Report

10.2.3 Report Classification

10.2.4 A Sample Investigative Report Format

10.2.5 Report Writing Guidelines

10.2.6 Consistency and Other Important Aspects of an Good Report

10.2.7 The Dos and Don'ts of Forensic Computer Investigations

10.2.8 Best Practice for Investigation and Reporting

10.3 Becoming an witness

10.3.1 Introduction

10.3.2 Understanding the witness

10.3.2.1 Qualifying As an witness

10.3.2.2 Types of Expert Witnesses

10.3.2.3 Testimony and Evidence

10.3.3 Testifying As an witness

10.3.3.1 Layout of a Courtroom

10.3.3.2 Order of Trial Proceedings

10.4 Summary

10.5 Reference for further reading

10.6 Frequently Asked Questions

10.0 OBJECTIVES

Objectives in this chapter: This chapter would make you understand the following concepts:

- Stages of Mobile Forensics
- Android Operating Systems
- Challenges
- iOS OS
- Writing Investigative Reports
- Becoming an witness

10.1 INTRODUCTION MOBILE FORENSICS

Mobile Forensics could also be a department of Digital Forensics. It's set the acquisition and evaluation of cell gadgets to urge better virtual proof for forensics investigations.

Acquisition Protocol

There are a few of unique issues for cell acquisition:

- Always lookout of cell gadgets with gloves as fingerprint could even be amassed from it.
- Make a remember of all open packages walking at the tool and examine the documents/textual content with inside the clipboard.
- Use a Faraday bag to accumulate the cell tool.
- All information inclusive of tool call, IMEI range, serial range etc., got to be mentioned with inside the chain of custody shape.

A vital component in recent times is tool encryption; if the proprietor of the tool is gift on the time of acquisition, the tool passcode/sample lock information must be received. There had been some information memories approximately producers not cooperating with regulation enforcement while the passcode isn't to be had. The producers refuse to release gadgets, mentioning confidentiality then on. Apple has been with inside the knowledge for this, and it's been observed that even the Apple representatives cannot release an iPhone for everybody without restoring the iPhone.

Android OS

Android is an open supply working device based totally on Linux Kernel, advanced through Google for cell gadgets. The T-Mobile G1 become the first Android handset the world noticed and once you consider that then Android has come a protracted manner. Its releases are codenamed on famous confection gadgets inclusive of Kit Kats, lollipops, frozen dessert sandwiches, etc. The lower back cease of Android programming is administered in Java and packages are run during a Dalvik digital device. Further, a totally unique identification secret's furnished to enforce protection measures, and packages can get entry to tool garage best if legal through the buyer. User-granted permissions are wont to limitation get entry to to device capabilities and consumer information. Albeit the protocols of Android Forensics are very similar to Computer Forensics, there are numerous variations with inside the strategies hired, particularly as Android helps extraordinary document structures. From an Android tool, we attain information inclusive of Call Data Records (CDR), Contacts, Messages, Apps statistics, GPS locations, passwords, Wi-Fi networks, etc.

The Android listing could also be explored through the 'adb shell' that we will use and reveal. Android's principal partition is usually partitioned as YAFFS2 (Yet Another Flash File System), which is meant maintaining in thoughts embedded structures are usually smartphones. Android helps ext2, ext3, and ext4 document structures which could be synonymous to Linux; and it additionally helps vfat, that's utilized by Windows structures.

Rooting an Android Device

Android may be a Linux-primarily based totally OS this is often tweaked to optimize it for contact display gadgets. Rooting Android unlocks its middle module to a consumer, which allows get entry to to the covered regions of the tool. Earlier, rooting become a commonplace place exercise with Android builders who desired to seek out out all of the capabilities of the tool. Over the years, rooting has find yourself a famous exercise with numerous tech savvy Android customers who want to personalize their tool with custom ROMs, attain updates, and found out third-celebration packages.

Rooting permits the forensic investigator to profit root privileges at the tool. But rooting an Android tool involves that the examiner installs a third-celebration software program to the telecel smartphone that would purpose adjustments to the tool country, and there could also be a threat of an flawed rooting approach like accidentally deleting or editing information at the tool, which will cause unreadable information codecs. albeit rooting an Android tool to accumulate proof offers an investigator root privileges, it can't be taken into consideration a legitimate technique for proof acquisition, and therefore the proof amassed through rooting the tool isn't admissible during a courtroom docket of regulation. Rooting an Android tool to make an photograph of an Android tool is proven with inside the bodily acquisition segment afterward this bankruptcy.

Advantages of Rooting:

- Access to middle device documents.
- Ability to require away bloatware.
- Enhances battery performance.
- Special apps could also be established.

Disadvantages of Rooting:

- If rooting isn't administered well, there could also be the threat of bricking the tool.
- Security of the tool is compromised.
- Warranty is void.

If the investigator roots the tool and later reveals the suspect to be harmless, that individual will now not be capable of avail any offerings for the tool if the tool is below the reassurance . So, the investigator wishes to form amends for any claims now not supported through a legitimate assurance once you consider that he had changed the tool.

Android Debug Bridge

This is a command-line device that permits us to connect an Android tool to a pc host device through a USB cable. it's a completely flexible device because it permits the buyer to hold out numerous duties inclusive of putting in , debugging, and getting obviate apps, etc. Also, through the utilization of the adb instructions, we'll flash a custom recuperation' after which thru recuperation, we'll found out root documents to root an Android tool. Adb is a component of the Android Software Development Kit (SDK) platform equipment package.

ADB includes 3 additives:

- Client – which sends out instructions. Client could also be invoked through issuing an adb command the utilization of a command-line terminal.
- Daemon (adbd) – runs instructions at the tool, and it runs as a history manner.
- Server – manages conversation among the patron and daemon. It runs as a history manner on a pc device.

Adb comes with many beneficial instructions that assist the examiner to talk with the tool. as an example , to listing the gadgets linked at the device, kind 'adb gadgets' to place in an utility in an Android tool thru device shell kind 'adb found out filename.apk'; similarly, to uninstall an utility from the tool, kind 'adb uninstall filename.apk'.

Methods for Screen Lock Bypass

If the Android tool is locked, its photograph acquisition turns into a nightmare for forensic examiners. With protection requirements stronger than ever, the want for higher practices to pass the display lock is required. Newer Android variations are proof against beforehand successful display lock pass techniques. However, there are a couple of techniques a forensic examiner can utilize.

- Commercial display lock pass equipment – Offer maximum fulfillment price amongst with rock bottom threat of data loss. There are many equipment which will be used for every Android and iOS, as an example, dr.fone – release, iSkysoftToolBox, Pangu FPR Unlocker Tool, etc., which supply software program offerings that pass display lock. It helps many fashions and is simple to use .

- Flashing Custom Recovery/ROM – this system is extra famous amongst builders for Android phones. It entails flashing the tool with a custom recuperation. It might be very vital to flash the tool with an appropriate custom recuperation this is often precise to the tool version.

However, it is vital to recognise the threat concerning this technique; flashing with a no compliant recuperation mode can smash the knowledge or even brick the tool. Team Win Recovery Project (TWRP) and Clockwork are famous recuperation techniques. Also, right here we're flashing ROM information, and not like disk forensics, we in no way use a write blocking tool in cell forensics.

Manual Extraction

Manual extraction could also be taken into consideration because the primary line of strategies utilized in forensic exam and stays the utmost noninvasive one. this is often likewise a completely fundamental approach, which can be followed through regulation enforcement officials or professionals who aren't tech savvy.

Experts can detect what information they need and extract it as in line with will, because it saves time and therefore the complexity of imaging.

AF Logical OSE through NowSecure may be a superb device for this. The fashionable steps worried are those:

1. Push AFLogical-OSE_1.five.2.apk through adb/USB connection/ OTG force on cell tool.
2. Install AF Logical OSE.
3. Open app and detect parameters for extraction and detect 'OK.'
4. Find documents in 'forensics' folder and export them on pc device for evaluation.

Call statistics, Contacts, and Messages exports are created in .csv layout, which is on the market through many packages. An data document can also be retrieved, that's in .xml layout and includes information approximately the tool and therefore the packages saved in it.

Here we are the use of the Santoku Operating device. Santoku is an open supply working device for cell forensics, evaluation, and protection. And right here we've used a Sony Xperia telcel smartphone walking on jelly egg four.2 apk for demonstration.

1. Use adb gadgets command to listing all of the linked gadgets. ADB drivers are constructed into the Santoku OS .
2. Download AFLogical OSE apk from <https://github.com/nowsecure/android-forensics/downloads>. Push the apk onto the tool to place in it at the tool. to try to to that, kind the command:

```
adb -d found out AFLogical-OSE_1.five.2.apk
```

3. we will see that AF Logical is established at the Android tool
4. Open the utility and detect the parameters for extraction. Click on seize after choosing all of the parameters
5. Once information extraction is administered , name statistics, Contacts, and Messages exports are created in .csv layout, which is on the market through many packages. An data document can also be retrieved, that's during a .xml layout and includes information approximately the tool and therefore the packages saved in it. These documents could also be discovered withinside the File Manager ➤sdcard➤ forensics folder

We can use those csv documents for evaluation.

Physical Acquisition

This is the other line of a forensic approach utilized in cell forensics. The forensics investigators use equipment to accumulate a forensic photograph of the cell tool. center635

Tools for Image Extraction

Various equipment which could be getting used for photograph extraction of an Android tool are as follows:

- BusyBox – frequently referred because the “Swiss navy knife of Embedded Linux.” BusyBox may be a software program utility that applications many Unix equipment. it's composed over 300 instructions and may be a nifty little device ready to many operations.
- Ncat – Ncat may be a networking software that allows information switch the community from the instruction . it's a part of the Nmap mission and is meant to be a dependable lower back-cease device.
- dd – Data Definition (dd) is one the oldest imaging equipment, that's a command-line device in most cases utilized in Unix Operating Systems. it's a easy software beneficial in copying information from one place to the other . It comes as a neighborhood of the GNU/Linux ‘coreutils’ package. It can accumulate information withinside the RAW layout, which can be additionally analyzed in many extraordinary forensic suites.
- Kingoroot – Kingoroot is an Android utility used for rooting of the Android tool.

Case Study: Image Extraction of an Android Device

We have amassed a cell tool from against the law scene, and as a Forensic Investigator we're getting to root the tool to urge tremendous consumer get entry to and accumulate dd snap shots of the tool for additionally evaluation. We are the utilization of an Ubuntu working device model 16.five for obtaining the photograph of the tool Sony Xperia telecellsmartphone.

Before beginning ensure you've got following equipment and apk established in your device:

- Adb drivers: you'll down load those from [HYPERLINK](#)

"<https://developer.android.com/studio/releases/platform-equipment>" |
"downloads"<https://developer.android.com/studio/releases/platform-equipment#downloads>

- Kingoroot: you'll down load this apk from <https://root-apk.kingoapp.com/>

- BusyBox: you'll down load this apk from <https://www.appsapk.com/busybox-app/>

- Netcat: you'll down load this from <https://nmap.org/ncat/>

1. Here we've created directories /Android/sdk/device and saved our KingoRoot.apk and BusyBox.apk therein .
2. After successful found out of adb drivers, join your Android tool in your device and start terminal. Type the next command within side the terminal to listing linked Android gadgets. adb gadgets
3. To root the tool, we will found out KingoRoot.apk on our Android tool. Type the command: adb -d found out KingoRoot.apk
4. Similarly, to place within the BusyBox app in your tool, kind the command: adb -d found out BusyBox.apk
5. Once all of the packages are at the tool, we test if found out become successful through establishing them
6. Open KingoRoot app and click on onon One Click Root and wait till the rooting manner completes.
7. After successful rooting of the tool, the SuperUser app might be established in your tool
8. Start the BusyBox app and provide it root get entry to after which click on at the Install alternative
9. Now to start the adb shell, kind the next instructions to urge root get entry to: adb -d shell su
10. To listing directories, kind ls /information. we will best get entry to those directories with root privileges
11. to ascertain an inventory of walls, kind the next command. Here we will create a dd photograph of mmcblk0 partition as it is the bodily disk withinside the tool and carries all of the specified information cat /proc/walls

12. Now we would like to line up a connection among the tool and therefore the pc device. we'll use port 8888 right here to modify information among those . We then run the next command at the pc device:

adb ahead tcp:8888 tcp:8888 The cell tool will examine the command and ship information. To concentrate to the conversation, we use netcat on port 8888.

13. to make the dd photograph of mmcblk0 partition:

Type command `dd if=/dev/block/mmcblk0 | busyboxnc -l -p 8888`

Here if is that the enter interface that reads the disk after which we will pipe that information into busybox. nc is netcat command that's wont to switch information at the community. -p command denotes the port range wont to switch information. -l command is employed to form the Android tool concentrate for a connection coming at the telecellsmartphone on port range 8888.

14. After a connection has been activated, the knowledge from the tool might be piped right into a document android.dd. to undertake this, kind command:

`nc 127.zero.zero.1 8888 > android.dd`

It will take time to achieve the photograph; it relies upon upon the reminiscence of the tool. Once the imaging is whole, the photograph document could also be analyzed in extraordinary software program; right here we used the Autopsy device for evaluation.

Physical Acquisition

This is the other line of a forensic approach utilized in cell forensics. The forensics investigators use equipment to accumulate a forensic photograph of the cell tool. center635

Tools for Image Extraction

Various equipment which could be getting used for photograph extraction of an Android tool are as follows:

- BusyBox – frequently referred because the “Swiss navy knife of Embedded Linux.” BusyBox may be a software program utility that applications many Unix equipment. it's composed over 300 instructions and may be a nifty little device ready to many operations.
- Ncat – Ncat may be a networking software that allows information switch the community from the instruction . it's a part of the Nmap mission and is meant to be a dependable lower back-cease device.
- dd – Data Definition (dd) is one the oldest imaging equipment, that's a command-line device in most cases utilized in Unix Operating Systems. it's a easy software beneficial in copying information from

one place to the other . It comes as a part of the GNU/Linux 'coreutils' package. It can accumulate information within the RAW layout, which can be additionally analyzed in many extraordinary forensic suites.

- Kingoroot – Kingoroot is an Android utility used for rooting of the Android tool.

Case Study: Image Extraction of an Android Device

We have amassed a cell tool from against the law scene, and as a Forensic Investigator we're getting to root the tool to urge tremendous consumer get entry to and accumulate dd snap shots of the tool for additionally evaluation. We are the utilization of an Ubuntu working device model 16.five for obtaining the photograph of the tool Sony Xperia telecellsmartphone.

Before beginning ensure you've got following equipment and apk established in your device:

- Adb drivers: you'll down load those from [HYPERLINK](https://developer.android.com/studio/releases/platform-equipment)

"<https://developer.android.com/studio/releases/platform-equipment>"
"downloads"<https://developer.android.com/studio/releases/platform-equipment#downloads>

- Kingoroot: you'll down load this apk from <https://root-apk.kingoapp.com/>

- BusyBox: you'll down load this apk from <https://www.appsapk.com/busybox-app/>

- Netcat: you'll down load this from <https://nmap.org/ncat/>

1. Here we've created directories /Android/sdk/device and saved our KingoRoot.apk and BusyBox.apk therein .

2. After successful found out of adb drivers, join your Android tool in your device and start terminal. Type the next command within the terminal to listing linked Android gadgets. adb gadgets

3. To root the tool, we will found out KingoRoot.apk on our Android tool. Type the command: adb -d found out KingoRoot.apk

4. Similarly, to place within the BusyBox app in your tool, kind the command: adb -d found out BusyBox.apk

5. Once all of the packages are at the tool, we test if found out become successful through establishing them

6. Open KingoRoot app and click on onon One Click Root and wait till the rooting manner completes.

7. After successful rooting of the tool, the SuperUser app might be established in your tool
8. Start the BusyBox app and provide it root get entry to after which click on at the Install alternative
9. Now to start the adb shell, kind the next instructions to urge root get entry to: `adb -d shell su`
10. To listing directories, kind `ls /information`. we will best get entry to those directories with root privileges
11. to ascertain an inventory of walls, kind the next command. Here we will create a dd photograph of mmcblk0 partition as it is the bodily disk withinside the tool and carries all of the specified information `cat /proc/walls`
12. Now we would like to line up a connection among the tool and therefore the pc device. we'll use port 8888 right here to modify information among those . We then run the next command at the pc device:

`adb ahead tcp:8888 tcp:8888` The cell tool will examine the command and ship information. To concentrate to the conversation, we use netcat on port 8888.

13. to make the dd photograph of mmcblk0 partition:

Type command `dd if=/dev/block/mmcblk0 | busyboxnc -l -p 8888`

Here if is that the enter interface that reads the disk after which we will pipe that information into busybox. nc is netcat command that's wont to switch information at the community. -p command denotes the port range wont to switch information. -l command is employed to form the Android tool concentrate for a connection coming at the telecellsmartphone on port range 8888.

14. After a connection has been activated, the knowledge from the tool might be piped right into a document android.dd. to undertake this, kind command:

`nc 127.zero.zero.1 8888 > android.dd`

It will take time to achieve the photograph; it relies upon upon the reminiscence of the tool. Once the imaging is whole, the photograph document could also be analyzed in extraordinary software program; right here we used the Autopsy device for evaluation.

JTAG

Joint take a glance at motion organization or JTAG may be a complicated information extraction technique utilized in cell forensics. JTAG within the beginning become created through the electronics enterprise as how of finding out and verifying designs and published circuit forums. JTAG is

that the acronym that acquired reputation as an IEEE widespread entitled Standard Test Access Port and Boundary –Scan Architecture. JTAG offers an interface through which a pc can speak directly with the chipboard. It entails connecting the proof cell tool's Test Access Port (TAP) to a JTAG emulator to urge entry to uncooked information.

Steps included in JTAG forensic exam are the subsequent:

1. Identification of TAPs: you'll become conscious of TAPs through studying documented gadgets. If the TAPs are unknown, check out the tool PCB for capacity TAPs, after which manually hint or probe to pinpoint suitable connector pins.
2. Solder wires to TAPs: this ends in an appropriate connector pins or makes use of a solderless jig.
3. Connect suitable JTAG emulator with twine leads for the boast tool.
4. Acquire bodily photograph dump.
5. Disconnect the wires and reassemble the tool.
6. Analyze photograph with forensic software program. JTAG emulators are the twine among PC's software program equipment and DSP forums at some point of improvement. It connects the host PC through parallel interface or USB port. The JTAG emulator offers a easy manner to supply the development device software program an instantaneous connection to a minimum of one or extra DSP gadgets at the goal board. a couple of JTAG emulators are XDS110, XDS200, XDS560, etc., for a C2000 microcontroller.

Advantages:

- JTAG may be a complicated, but non-invasive, technique of forensic exam.
- It could also be used with many sorts of cell gadgets a bit like the Windows phones.
- The method is far less complex than Chip-Off (see subsequent segment).

Disadvantages:

- In case of tool encryption, the fulfillment price is far less.
- JTAG assets are tough to locate over internet .

Chip-Off

Chip-Off is taken into consideration the ultimate resort. because the call suggests, it entails getting obviate the reminiscence chip of the cell tool and planting it onto a specific hardware for information acquisition and reading its contents. With the Chip-Off approach, examiners attain a binary photograph of the reminiscence chip, that's analyzed through

specialised software program. this is often a sophisticated forensic technique that even works for bricked and/or broken gadgets. The nonvolatile reminiscence issue is eliminated and positioned on a hardware reader through which information is received.

Here are the steps involved in Chip-Off forensic exam:

1. The reminiscence chip is eliminated through de-soldering it.
2. The chip is cleaned and repaired (if important).
3. chip is established on unique hardware apparatus, and knowledge is received.

Advantages:

- Useful for exam of gadgets in broken situation.
- High chance of data acquisition if tool is locked.
- Gives forensics investigators the freedom to craft information acquisition manner.

Disadvantages:

- Heat and adhesive wont to deduct the reminiscence chips also can additionally harm the circuit card .
- Reassembly of the tool after exam might be very tough and typically unsuccessful.

Micro-read

Micro-read exam entails the usage of a excessive-powered microscope and observes output on the gate stage. The tool reminiscence chip is shaved in extraordinarily skinny layers, and then the knowledge is examine little by little from the availability the utilization of an microscope or different tool. it's a fantastically state-of-the-art approach, and only a couple of entities provide Micro-examine exam offerings. Use of this system is for excessive-price gadgets or broken reminiscence chips. Being this type of complex, and expansive approach, it is reserved for best excessive-profile instances. It might be very tough to locate industrial equipment for Micro-examine. this is often probably a extra approachable approach withinside the on the brink of destiny.

Challenges in Mobile Forensics

With smartphones evolving at a mind-blowing price cell forensics is extra difficult than ever. Every Android model launch comes with up so far capabilities and protection improvements, which normally hinder with the forensic manner. As a fresh Android model is launched, the forensic equipment utilized in forensic exam frequently find yourself redundant.

Apart from the software program, with this type of great range of gamers withinside the marketplace, a forensics examiner also can additionally encounter extraordinary sorts of hardware. Device specs have find yourself complicated and range amongst groups. This provides to the prep paintings of a forensic examiner as they need right equipment to urge entry to the hardware. as an example , we've visible the upward thrust of USB Type-C connectors now being utilized by producers with many gadgets.

Encryption in gadgets has received essential momentum after information leak scandals around the sector. People have find yourself aware of their privateness rights and knowledge a want to shield their information. Manufacturers have began bent bolster their protection modules, that's preferred through the client. Such a excessive stage of protection has find yourself an enormous impediment for forensic examiners because it turns into very tough to pass protection of the tool. While cell gadgets walking older Android model are nonetheless available through a gaggle of strategies, more moderen gadgets frequently do not have any assist from even industrial equipment. Not all of the knowledge is at the tool, as cloud garage has find yourself a famous and favored alternative for telecellsmartphone customers. Manufacturers provide very tempting applications so as that customers save their information at the cloud, and customers locate it maximum convenient, too. All this another time may be a hurdle on the time of data extraction; if account credentials are gift with the forensic professionals, then information could also be received otherwise there could also be no get entry to thereto .

Apart from Logical and Physical Acquisition, the superior forensics strategies inclusive of JTAG, Chip-Off and Micro-examine are fantastically invasive and need meticulous expertise and specialized schooling. These techniques are also very pricey and are not available to all or any and varied as only a couple of groups provide those offerings. Researchers have expressed their problem approximately the developing complexities of breaking thru the encryption of the gadgets. Chip-off gives a 90% fulfillment price as many hardware producers are making it tough for examiners to hold out an intensive exam. But if records has taught us something, it is that answers are created as troubles seem: the destiny is complete of obligations and possibilities.

iOS OS

iOS may be a cell working device created and advanced through Apple Inc. that currently powers among the business enterprise's cell gadgets, inclusive of iPhone, iPad, and iWatch. The iPhone firmware working device is based totally on Mac OS X. Every iOS tool combines hardware, software program, and offerings designed to paintings collectively for optimum protection. iOS protects the tool and its information at rest (i.e., information isn't shifting from tool to tool or community to community), inclusive of the entire thing customers do locally, on networks, and with key net offerings.

iOS gadgets offer superior protection capabilities and they are clean to use. Many of these capabilities are enabled through default, and key protection capabilities like tool encryption aren't configurable, so as that customers can't disable them through mistake. Other capabilities, inclusive of Face ID and Touch ID, beautify the buyer enjoy through making it more easy and additional intuitive to steady the tool.

iOS Device Boot Process

Bootrom permits the tool also and initialize all of the peripherals of iOS and a couple of hardware additives. There are 3 extraordinary modes for the boot procedures for iOS gadgets:

- Normal boot manner
- Recovery mode
- DFU mode

Normal Boot Process

In a regular boot manner, the Bootrom will run and test the signature of the Low-Level Bootloader (LLB) and executes it if the signature is matched. After executing LLB, it'll test the signature of iBoot (Apple degree 2 bootloader for all iOS gadgets) before handing it over to the iBoot, which in flip exams the kernel signature and executes it. The kernel is signed which can prevent any unsigned code to be completed.

Recovery Mode

When the iOS tool is close to the "Recovery Mode," the Bootrom is completed first; it exams the iBoot signature and if it suits, it'll execute it. then, iTunes sends Apple's signed "kernel" and "Ramdisk" to the tool, after which the repair manner is initiated. Process no unsigned code could also be completed at some point of any a neighborhood of the "Recovery Mode."

DFU Mode

In Device Firmware Upgrade (DFU) Mode, the Bootrom is loaded after which the iBSS (a stripped-down model of iBoot) is despatched to the iOS tool. Then the iBSS signature is checked and completed through the Bootrom. then, Apple's signed kernel and repair disk are despatched to the tool and completed through iBSS after a signature test. Once that's administered, the repair manner is initiated. Process no unsigned code could also be completed at some point of any a neighborhood of the "DFU Mode."

Jailbreak vs. No Jailbreak

iOS jailbreaking is beneficial for the motive of getting obviate software program regulations imposed through Apple on iOS through the utilization of a sequence of kernel patches. Jailbreaking permits root get entry to to iOS, permitting the downloading and found out of additional packages,

extensions, and topics which could be unavailable thru the authentic Apple App Store. Additionally, it is feasible to use different SIM playing cards apart from the certified issuer. A jailbreak is best feasible withinside the DFU mode, that's a standing of the iPhone working device. The device could also be overwritten on this mode, with changed iPhone firmware like Cydia utility. it's feasible to down load packages with Cydia (it isn't a licensed AppStore), which are not legal through Apple, as an example , OpenSSH, Netcat, or Terminal.

A jailed iPhone may be a tool with out changed software program and altered working device. Apple permits the found out of packages which could be legal best from Apple over the AppStore on a jailed iPhone. A Jailbroken iPhone is above a jailed iPhone from the attitude of a forensic examiner, because it isn't feasible to place in OpenSSH and Netcat to form a connection over Wi-Fi/WLAN during a jailed iPhone.

iOS file system and Architecture

All Apple cell gadgets use the HFSX document device. HFSX is case touchy, due to this that that if there are documents with equal out in the device, due to their case sensitivity, the document device will differentiate among the two documents. this is often the foremost distinction with HFSX and HFS+ document structures. Logically, iPhone has walls. One is for storing the iOS precise documents, accountable to load the working device inclusive of kernel snap shots and configuration documents.

The different partition is employed for the garage of consumer-precise settings and packages inclusive of flicks , music, photos, contacts, and extra. The 2nd partition is extra vital from a forensic factor of view because it carries all of the capabilities a consumer can perform on an iPhone and therefore the information for those capabilities, as an example , name records, touch listing, quick messaging provider (SMS) messages, emails, audio and video, and photos. Since iPhones' hardware and dealing structures are closed supply and proprietary, fashionable motive forensic strategies and equipment will now not paintings thereon .

iTunes iPhone Backup

iOS tool backups could also be controlled with the Apple iTunes software program. If the iOS gadgets are synchronized, iTunes creates a backup. All the knowledge of the gadgets is saved withinside the backup, and it is also feasible to encrypt the backup. it's straightforward for an examiner to locate and use the iPhone backup if the backup isn't encrypted.

Case Study: iPhone Backup Extractor

As a forensic investigator, we're getting to decrypt an iOS tool backup taken through iTunes. This device is understood as iPhone Backup Extractor. iPhone Backup Extractor may be a industrial device, however we'll use its 30-day trial model for recuperation of photos, messages, motion pictures, name records, notes, contacts, Screen Time passcode,

WhatsApp messages, and different app information from iTunes and iCloud Backups.

We have taken an encrypted backup through iTunes for demonstration. Encrypted backup additionally backs up numerous account passwords used at the iOS tool.

1. Start iPhone backup extractor device, and it will show an inventory of backup to be had thereon tool, and detect the backup of your iOS tool. If the tool's backup is encrypted, a forensic investigator can use numerous password-cracking equipment to retrieve the password. Additionally, you'll upload your iCloud account to look at your iCloud backup.
2. Here we'll see that iPhone Backup Extractor equipment has fetched photos, contacts, messages, WhatsApp messages, name records, etc., efficiently
3. Here we'll see Decrypted WhatsApp chats withinside the Preview segment. This device become capable of fetch snap shots and attachments withinside the chats as properly Similarly, we view Photos, Messages, Contacts, etc., withinside the Preview segment. Here we'll see that the Snapchat app is likewise established at the tool. The paid model of this device offers information approximately different apps inclusive of Snapchat, Instagram, etc., which had been established at the iOS tool at some point of backup.

Last, withinside the info segment, we'll see information about the iOS tool inclusive of Backup information, hardware statistics, Mobile tool identifiers, account statistics, production information, and SIM issuer information

10.2 WRITING INVESTIGATION REPORTS

One of the utmost essential elements of any forensic engagement is that the manufacturing of an investigative document. This record is written to talk the ultimate results of virtual forensic evaluation and exam. If you can't document your findings, nobody will recognize or recognize what you've got discovered or its significance.

Understanding the Importance of Reports

In forensic investigations, the investigative document is of critical significance. In maximum instances, document writing capabilities are overlooked. Producing a properly-established and logical investigative document improves the possibilities that a jury might be satisfied which you recognize what you're doing which the proof is legitimate. A document must now not best speak the knowledge, however additionally gift professional opinion. During a crook research, the reviews additionally find yourself the availability for the practise and presentation of the research for trial. The goal of any investigative document is to record the knowledge and proof. If you find proof that does not assist your

case you still want to document it. Related reveals inclusive of diagrams and photos need to be protected for the document to be powerful.

Investigative reviews need to stipulate the fees purchased the professional's offerings and listing all of the civil or crook instances wherein the professional has testified for the previous 4 years. The document must now not contains the instances wherein the professional acted as a witness . A witness may be a witness who isn't attesting withinside the potential of an professional witness. Always contains reveals inclusive of the CV of the investigator performing as a witness that lists all courses that the witness has written at some point of the previous 10 years. Ensure which you retain the simplest requirements for writing and attesting. Not best will reviews be saved during a deposition financial organization or library or maybe be to be had at the web , however additionally your testimony is usually administered below oath.

The Requirements of an Investigative Report

An investigative document is made with the motive that it are often utilized during a courtroom docket of regulation. It must be succinct and recognition at the venture or purpose of the research. The investigator's favorite motive is to get statistics and, as a result, proof on a selected count, to urge better widespread files, or recover sure document sorts and any date and timestamps. The purpose of the research might be described through your patron. Your patron are going to be inner to the corporation you work for or the other investigator or legal professional. Spending time documenting the goal will typically shop time and reduce the worth of the exam. Always confirm that the investigative document specifies the venture of an research.

Your document must float in a uniform order, reflecting that of the knowledge as that they had been determined at some point of the research. An define or an association based totally on appendices and an boast is suggested to assist in assembling substance for the document. The document must be written during a logical way that states the effort , gives the outcomes of the research, and units forth the conclusions and proposals. A coherent presentation must be wont to collect the knowledge and proof.

Report Classification

Your initiative in writing a document must be to become conscious of the document's supposed target market and purpose. The investigative document must be established so as that individuals who don't have a excessive stage of technical expertise can recognize it. When studying this record a nontechnical reader must be capable of recognize the findings and lawsuits of the case.

Reports are typically classified into:

- Verbal reviews
- Written reviews

Reports also will be classified as being:

- Formal in nature
- Informal

When you supply a correct document verbally it must be established for presentation orally to a board of directors, managers, or a jury. Always arrange the document to suit within the time body given. A supplementary record that carries predicted questions and applicable solutions wishes to be organized for the humans to whom you're offering and to resource your presentation.

This record is understood because the exam plan and is made through the legal professional for the investigator's advantage. Changes to the exam plan inclusive of those concerning explanation or definition could also be asked through the investigator for motion through the legal professional if an expression or period of time is misused.

Do not contains gadgets that are not related to the testimony. An casual verbal document is far less established than a correct document and is brought in individual (most usually in an legal professional's office). This document is meant to be a initial document and it wishes to be strictly managed to stop inadvertent launch. It must comprise the weather of the research which have now not been finished, inclusive of any assessments or evaluation that has now not been concluded, interrogatories, record manufacturing, and depositions.

An casual document is likewise a initial document. This form of document may be a excessive-threat record that carries touchy statistics which may show useful for the opposing celebration. The opposing celebration also can additionally acquire the record in discovery. Discovery is that the strive made to achieve proof previous to an ordeal. The statistics are often a written request for admissions of reality, deposition, or questions and solutions written below oath.

A formal document may be a document sworn below oath (inclusive of a sworn statement or declaration). Always confirm that your phrase utilization, grammar, spelling, and knowledge are accurate while writing formal reviews. As this document is formal in nature, the favored fashion will use first-individual narratives with a herbal language fashion. An affidavit are often wont to preserve the issuing of a warrant or be offered as proof during a proper courtroom docket taking note of. Always supply your complete interest to writing a record withinside the formal written fashion.

It is prudent to incorporate the substance of written, casual reviews in an casual, verbal document. Summarize the way and method inclusive of the matter device, device used, and findings, with inside the verbal, casual document. Never smash a written, casual document with out formal written steering from an legal professional, as this motion are often taken into consideration because the destruction or concealing of proof.

A Sample Investigative Report Format

The following segment gives a possible format of an investigative document. The presentation of correct textual content is adequate to having the power to speak definitely. As such, continually supply your complete interest to format and presentation of statistics during a document whilst you're writing. it's additionally really helpful to constantly adhere to a unmarried format at some point of the document. This creates consistency.

Two principal techniques exist for developing a format shape: decimal numbering and felony-sequential numbering.

Here is an instance of the decimal numbering device:

1.0 Introduction

1.1 the character of the Incident

1.1.1 the small print of the Victim

2.0 First Incident

2.1 the primary Witness

2.1.1 Witness Testimony – Witness No. 1

3.0 Location of Evidence

3.1 Seizure of Evidence

3.1.1 Transportation of Evidence

4.0 Analysis of Evidence

4.1 Chain of Evidence

4.1.1 Extraction of knowledge

5.0 Conclusion

5.1 Results

5.1.1 Expert Opinion

Legal-sequential numbering makes use of this layout:

I. Introduction

1. Nature of the Incident

2. The Victim

3. Witness to the Event

4. Location of Evidence

II. Examination

5. Chain of evidence

6. Extraction of Evidence

7. The Analysis of Evidence

The felony-sequential numbering device is employed in pleadings and is legendary amongst attorneys. Roman numerals are used for the foremost thing of the document and Arabic numbering helps the statistics element.

The maximum critical issue of any investigative document is that the usage of powerful language to talk the statistics definitely. To try this, signposts must be protected within the document. A signpost is a manual to the readers of the record that focuses their concept on an element or series of a fashion. Signposts spotlight the first factors which you would like to hold through developing a logical improvement of the statistics within the document. This makes it more easy for the reader to know the record.

For instance, the steps within the record are going to be added the utilization of a signpost inclusive of “The initiative on this segment,” or “The 2nd step withinside the exam”. These act because the signposts for the series of statistics.

Try to influence clean of redundant statements inclusive of “This document is submitted”, or “As the top results of the research, I need to document as follows”. The use of right fashion and tone and concept regarding the usage of accurate layout, punctuation, vocabulary, and grammar is critical whilst you’re writing a document.

Report Writing Guidelines

Whatever you write for your document, you want to do not forget that its presentation wishes to float during a logical order if it is to hold the statistics you've got amassed withinside the way which you desire. To reap this it is important to plot the document before writing it. This allows you to make your argument piece through piece.

The document must comprise a right float of sentences which may be organized to resource the event of concept during a clean and unambiguous way from the begin to the cease of the record. Each paragraph must be correlated to mirror the ambitions of the entire record and offers the reader with an impression of precise relation.

The use of headings with information beneath Neath is suggested. These information must be set in paragraphs, every limited to a specific material. Any use of jargon, slang, or technical phrases must be prevented during which feasible. If important, put together a thesaurus containing slang or technical phrases. When writing, hire lively voice in situ of passive. active encourages conciseness and accuracy in writing and comes

throughout as being extra forceful. Always prevent from trite and superlative phrases.

When a specific abbreviation is employed for the first time with inside the document it is really helpful to place in writing the entire shape of the equal. Comprise acronyms withinside the Glossary protected on the cease of the document. Most attorneys do now not have an thorough technical expertise. As a outcome, it is feasible to confuse them while the utilization of of acronyms.

Using Supporting Material

A properly-written investigative document tells a tale wherein one has got to reply numerous questions inclusive of who, while, in which, why, and therefore the way. While answering those questions, helping substances inclusive of figures, tables, information, and equations are required within the event that they assist the story spread in an powerful shape.

The helping fabric could also be noted directly withinside the textual content and included withinside the writing to beautify the effect. it's really helpful to range figures and tables withinside the equal order as they're added withinside the document. as an example , tables could also be numbered as Table 1, Table 2, and so on. within the equal manner, figures could also be categorized as Figure 1, Figure 2, and so on. Numbering the material avoids confusion and makes it more easy to acknowledge .

To lessen narration and emphasize vital information, positioned tables and schedules in appendices. Captions are favored over easy titles, because the entire statistics provides to the conciseness of the presentation. If charts are used, they need to be categorized, inclusive of axes and units. during a paragraph, if any desk or determine is cited, that determine or desk must be inserted after the paragraph. One can also accumulate all helping fabric after the reference segment.

Consistency and Other Important Aspects of an Good Report

Whenever you're writing a document do not forget that consistency is significant. Create and keep record templates to resource you. an appropriate investigative document layout must contains the next sections:

- Abstract or precis
- Table of contents
- Body of document
- Conclusions
- References
- Glossary
- Acknowledgments

These sections are often adjusted to in shape the motive of the document. The summary or precis must gift the essence of the document as an abbreviated or condensed shape of the research. That is, it must gift the important thing thoughts expressed within the document. A properly-designed desk of contents must offer brief reference to all vital capabilities of the research.

Any appendices protected within the document want to be indexed and defined with inside the desk of contents. The document frame must comprise the first factors which you would like to hold. It must ask the motive of the document. References and appendices listing the substance noted with inside the document, inclusive of output from equipment and interview notes. A presentation can observe any layout which you and therefore the alternative events are snug with.

The Main Features and Aspects of an honest Report

A suitable document will typically have the next capabilities:

- It will offer an thorough clarification of the techniques, exam strategies, materials, or system used. It'll additionally element any analytical or statistical strategies, information/series, or reasserts inside numerous subsections that resource the reader in growing an expertise of the research manner.
- Any suitable document offers a properly-prepared presentation of the knowledge amassed. the knowledge series manner may be a essential issue of an efficaciously administered forensic exam. In preparing the lab document, information inclusive of observations must be recorded during a laboratory pocket book for later reference. All the tables used for offering information must be categorized.
- Include any calculations which you create. It's right exercise to summarize the commonplace place call of the calculations (e.g. Secure Hashing Algorithm for SHA-1) wont to confirm the integrity of the proof and therefore the dates that those during which finished at some point of the research within the document. Briefly describe an equivalent old equipment and their mentioned supply which are used for this calculation.
- List a declaration detailing any provision for uncertainty and mistakes evaluation. There are continually obstacles of experience and there could also be no foolproof manner to shield the integrity of data. as an example, while retrieving a timestamp from a pc device you want to country that the timestamp could also be reset effortlessly which this statistics on my very own must now not be relied upon.
- Give special causes to your outcomes. These must be indexed during a logical order the utilization of subheadings containing textual content which addresses the motive of the document. Where feasible, use tables and figures within the textual content to beautify its presentation. make sure that any reader with out a expertise of the case

can recognize the research and therefore the outcomes totally during this document.

- Present a dialogue of the outcomes and end. Discussing outcomes and conclusions is critical. The importance of the studies must be mounted on this segment of the document. Provide solutions to questions inclusive of how the case progressed, what troubles happened, and any troubles that had been addressed.
- List your references. Include the humans and courses mentioned with inside the document. Plagiarism will smash the credibility of your document. Site all supply fabric, Web webweb sites, the reviews of others, and any works that are not your very own.
- Include any required appendices. An appendix must be wont to reference any longer fabric this is often referenced with inside the document. you want to contains charts, diagrams, graphs, transcripts, and copies of device output. Arrange the appendices withinside the order that they appear within side the document
- Provide acknowledgment during which it is warranted. Thanking those individuals who helped at some point of the introduction of a document will make it far more likely that they will assist you within side the destiny. List humans who've contributed to the evaluation of data , proofreading, or another beneficial hobby. Acknowledgment is optional, however recommended.

The Investigative Report Format

There are as many document writing codecs as there are groups or agencies. When a previous document is to be had this is often desirable to the events, observe the layout it utilized in place of re-developing one. Review the knowledge to make a decision the relevancy and as a result what information to contains and which to get rid of previous to writing the document. Carefully study any information and confirm that they are applicable. The document need to contains all of the applicable proof. This consists of proof that does not assist the document's end. you want to keep your objectivity within side the document and record the findings in an independent and proper way. attempt to locate flaws in questioning or exam, as it is probable that just in case you don't, an individual else will. Do now not broaden an schedule besides for locating the truth at some point of document writing.

There are essentially 4 sections to an investigative document. These are:

- Section 1 This segment consists of the chief information inclusive of the investigating officials, the thanks to touch them, and therefore the place of the operating papers.
- Section 2 This segment covers the history and precis of the document. It includes a precis of the complainant's allegations, discretionary

statistics which may resource the reader in expertise the case, the ultimate results of the case, and therefore the listing of allegations.

- Section 3 This segment introduces the first allegation. It gives the knowledge, offers an evaluation and dialogue of the knowledge, and, during which suitable, offers a recommendation. Conclusions could also be declared on this segment, and this segment also can additionally contain the disposition to record any remedial movements that the accountable authority took regarding any substantiated allegations. During this segment, you want to attend to each allegation within the equal layout if one exists. Further sections could also be added to the record at this factor, relying at the allegations.
- Section 4 The concluding segment lists and describes the interviewees, the files reviewed, and every one different proof that has been amassed. Before writing the document, do not forget that numerous forensic software program equipment, inclusive of Forensic Toolkit (FTK), DriveSpy, ILook, and EnCase, can generate reviews. These equipment can create reviews in textual content layout, a phrase processor layout, or HTML layout. The previous record is that the aggregate of the document generated the utilization of forensic equipment and therefore the authentic investigative document.

The “Do’s” and “Don’ts” of Forensic Computer Investigations

The seven maximum essential dos and don’ts so one can follow to any forensic research are:

1. Ask questions Inquire on the character of the request. The extra expertise you’ve got concerning the research, the additional powerful you’ll be.
2. Document methodically No count how easy the decision for, write it down—even just in case you experience that you simply may now not perform that a part of paintings.
3. Operate in suitable religion Generally, you want to observe commands out of your advanced or felony recommend within the direction of an research. It are often feasible that a couple of investigative movements are going to be unlawful. Bring this to the choice events’ interest.
4. Don’t get in too deep If any of the next situations are authentic, you’ll want to form an vital willpower on whether or to not maintain in your very own or to call in several events (inclusive of regulation enforcement):
 - a. The research entails against the law.
 - b. The research is anticipated to cause extreme subject or termination of an worker.

- c. The research involves that files are organized and maintained for a courtroom docket or a central authority investigative frame, and observe felony discovery regulations.
- d. Large-scale investigations over quite one jurisdictions must be administered through skilled investigators.
5. plan to analyze Involve individuals who are important to the research and don't make all of the alternatives your self.
6. Treat the entire thing as personal no matter who is aware of—or the rumors that sur- face—maintain all statistics personal and reveal the statistics best to parents who want to acknowledge .
7. File it Keep your documentation and reserve it safely. Always document it during a managed way.

Best Practice for Investigation and Reporting

Any suitable document will solution the 5 Ws: who, what, why, while, and during which . Remember to record who become worried within side the case and who asked it. Document what become administered and why. When and during which did it arise? an appropriate document must provide an evidence for the pc and community procedures and record all salient elements of the device.

A properly-carried out research must additionally observe the SMART method. This is:

- Specific Detail every issue.
- Measurable Ensure which you log file sizes, instances, and different applicable fabric.
- Achievable Ensure which you've got the assets to reap your objectives.
- Realistic Report the knowledge , don't speculate.
- Time-primarily based totally Work to time constraints and deadlines, and confirm which you recorded all of the activities as they've happened at the device.

Reports are essential to a search as they provide the way to alternate the findings and different proof to the important humans. A document are often formal or casual, verbal or written, however it continually wishes to be grammatically sound, so confirm which you employ an appropriate spelling and prevent from any grammatical mistakes. When writing the document, prevent from the utilization of jargon, slang, or colloquial phrases and confirm the readability of writing, as that's essential to the fulfillment of a document.

Writing a document is like questioning. The presentation of the document need to float logically to hold the statistics during a established shape. Discuss the outcomes and conclusions. Remember that the previous record

may be a aggregate generated the utilization of forensic equipment and therefore the authentic investigative document. Also, while engaging within the research, don't forget: Document the entire thing! In virtual investigations, the utmost essential component to do not forget is documentation, or keeping chain of custody. Documentation need to be maintained from the beginning to the cease of the enagement. Having an flawed chain of proof is worse than having no proof in any respect Document the device's hardware configuration. After you've got moved the device to a gentle place during which the proper chain of custody could also be maintained, it is essential to require as documentation photos of the device hardware additives and therefore the way the connections and cables are organized.

Also, record the device date and time. this is often extraordinarily vital. An wrong date and timestamp can permit the refuting of proof and obtain in-tuned with into query the integrity of the findings. albeit the entire thing else takes place perfectly, the mere reality that it got up to now will effect the entire research.

Document filenames, dates, and instances at the device and make a timeline. The filename, introduction date, and final changed date and time are of critical significance from an evidentiary point of view while admitting virtual proof. The filename, length, content material, and introduction and altered dates need to be documented.

Finally, you want to record all the findings. it's vital to record the findings sequentially because the issues are recognized and proof is discovered. A right file of all of the software program hired in assessment of the proof must be organized. One must be legally certified to use the software program thanks to the very fact pirated software program is of no use during a tribulation of the case. Document can also contains the software program license and display pictures to reveal how software program become used within side the proof series manner.

10.3 BECOMING AN WITNESS

Introduction

A cybercrime research and constructing of the case document is aimed closer to at least one cease end result: acquiring a conviction of the cyber crook during a courtroom docket of regulation. No count how suitable the proof you attain—log documents displaying unauthorized get entry to to the community, difficult disks seized from the suspect's pc containing simple warning signs of the crook hobby, community statistics monitoring the intruder lower back thru Internet servers to his or her pc—none of this proof can stand on my very own . Under maximum judicial structures, bodily and intangible proof need to be supported through testimony. Someone need to testify on while, in which, and therefore the way the proof become received and affirm that it is the equal while it is offered in courtroom docket because it become while it become amassed.

Even though you want to affect each case as a level though you had been looking forward thereto to go to courtroom docket, actually attesting in courtroom docket could also be a disturbing enjoy. If you've in no way been during a court docket before, it's ready to experience very similar to your first day at a fresh college. You're unusual with the environment, don't recognise the strategies, and may even make errors so one can purpose you to balk later. Even whilst you recognise what to assume, it's ready to nonetheless experience like you're strolling into the principal's office (or at instances like you're strolling onto the playground to be crushed up). Testifying typically isn't a pleasant enjoy, albeit it's ready to be made more easy thru expertise and luxuriate in. With sufficient practise, the event may even be some thing you'll do not forget proudly.

Understanding the witness

Testimony in courtroom docket is furnished through witnesses, which may be humans who've first hand expertise of against the law or incident, or whom provide proof at some point of an ordeal, tribunal, or taking note of. When proof is technical in nature and hard for laypeople to acknowledge, professionals are often required to testify to supply an evidence for the character of the proof and what it manner to the case. during a cybercrime case, police investigators and IT employees are often required to require the witness box. Two sorts of witnesses could also be referred to as to testify in crook movements:

- Evidentiary witnesses
- Expert witnesses

An evidentiary witness may be a one that has direct expertise of the case. As an example, a community administrator is perhaps referred to as to testify on what she or he located at some point of an assault at the community, or an investigator is perhaps referred to as to testify on the proof that she or he located on a pc that became seized pursuant to a seek warrant. An evidentiary witness can best testify on information (what she or he noticed, heard, or did) however cannot supply authoritative reviews or draw conclusions.

A professional witness is not the same as an evidentiary witness therein he or she is going to supply opinions and draw conclusions approximately information within side the case. The professional witness also can additionally do not have any direct involvement within side the case however has unique technical expertise or know-how that qualifies her or him to supply expert reviews on technical subjects. Expert witnesses from time to time put together reviews that outline their reviews and provide motives for each opinion.

Even though knowledgeable witness can gift conclusions, she or he's constrained within side the reviews which will be expressed. as an example, knowledgeable in pc generation also can additionally testify that a threatening e mail become traced to an account that become owned through the defendant, and therefore the way evaluation of the defendant's

pc confirmed that it become actually dispatched from that device. The witness cannot gift a end that the defendant is thereby responsible as sin. After all, someone is taken into consideration harmless till demonstrated responsible, and therefore the neutrality of the professional witness must observe that philosophy. The professional in computer systems additionally couldn't communicate approximately the mind-set of the defendant because it become being dispatched, as psychology isn't the witness's know-how. A witness is constrained to attesting approximately what she or he noticed, heard, or did, and professional witnesses can communicate best to the present and/or approximately statistics this is often within the scope in their expertise and luxuriate in .

The prosecution and protection legal professionals are accredited to possess professional witnesses testify during a case, albeit they aren't continually deemed important through one or both facet. As such, professionals aren't utilized in maximum trials. In many instances, the burden of proof is evaluated and a plea bargain is reached. A plea bargain is an settlement wherein the defendant pleads responsible to a lesser crime to possess extra extreme expenses dropped. Even while a case does visit trial, frequently the evidentiary testimony is all that a prosecutor or protection legal professional wishes to argue the guilt or innocence of a defendant. for each case getting to trial, a legal professional need to decide whether or not the knowledge might advantage from knowledgeable opinion, or whether or not the evidentiary testimony and proof can stand on its very own.

The professional witness must additionally now not be pressured with professionals that function consultants, which each facts also can additionally use to acknowledge extraordinary sorts of proof. as an example , during a tribulation concerning a automobile twist of fate, the protection legal professional also can additionally touch knowledgeable in protection requirements to acknowledge problems related to the air baggage utilized during a selected make and version of automobile. Although the professional offers readability in expertise elements of the case, she or he isn't knowledgeable witness thanks to the fact:

- The individual hasn't been subpoenaed or sworn in as a witness.
- No testimony has been given in courtroom docket.
- The courtroom docket hasn't identified the individual as knowledgeable .

As we'll see within side the next segment, whether or not an individual is targeted as knowledgeable witness is in most cases on the discretion of the decide taking note of the case. The professional witness offers statistics approximately his or her qualifications, and every the prosecution and therefore the protection evaluation the individual's training, enjoy, and different credentials. Either facet also can additionally project the individual's qualifications in courtroom docket, or they'll each agree that the individual may be a professional during a selected area. Ultimately,

however, it is the maximum amount because the plan to apprehend the individual as knowledgeable .

Qualifying As an Expert Witness

The requirements for qualifying as knowledgeable witness range around the sector. during a few countries, professional witnesses need to be registered as professionals during a selected area. within the USA and Canada, professionals need to typically show their know-how through offering their credentials in courtroom docket.

To decide whether or not someone qualifies as knowledgeable witness, and whether or not their testimony is admissible, entails a fashion of exam, cross-exam, and being identified through the courtroom docket. The legal professional calling the capacity professional witness will typically examine his or her qualifications into the file, and/or also can additionally ask a sequence of questions. These questions are designed to reveal the individual's credentials as knowledgeable . Such questions may consist of:

- What ranges, diplomas, or certificate do you've got?
- What positions have you ever ever held within side the area?
- What lectures or publications have you ever ever taught on this area?
- What extra schooling or publications related to this area have you ever ever taken?
- What memberships in agencies related to this area do you've got?
- What books or papers have you ever ever written pertaining to the area?
- What is your beyond enjoy as knowledgeable witness on this area?

The high-satisfactory of your solutions to those questions will assist to make a decision whether or not you'll be identified as knowledgeable during a selected vicinity. However, in searching at those questions, don't experience that you simply got to have an outstanding solution to every one. as an example , just in case you had training and luxuriate in however didn't have any coaching enjoy, you'll nonetheless be declared knowledgeable . The key component is that the general know-how, now not whether or not you've an impressive solution to each and every this type of questions. After all, the first time every one testifies in courtroom docket, the answer as to if or not you've got testified before may be a resounding "no."

Once the witness has been referred to as to the stand and tested, the courtroom docket might be requested to easily accept her or him as knowledgeable . The opposing facet will then have the likelihood to easily accept the witness as knowledgeable or project its admissibility. If a project is formed , the opposing facet can cross-study the witness on his or her qualifications.

The opposing facet also can additionally project the professional witness's credentials in an attempt to have that individual's testimony deemed inadmissible, or prevent her or him from declaring reviews and conclusions approximately the proof. The legal professional making this project features a heavy burden in trying to exclude proof or testimony at any degree of litigation. Not best need to she or he assault the credibility of such witnesses, their testimony, and any proof they've furnished, however additionally need to achieve this with constrained expertise. The legal professional are often knowledgeable in regulation, however have minimum or no know-how within side the world of the witness.

As we'll see in later sections of this appendix, an legal professional also can additionally use a number of procedures and assets while cross-inspecting a witness and difficult her or him as knowledgeable . Such procedures can contains approaches of asking questions, and hints which could be frequently successful in tripping up a witness's testimony. To recognize technical elements of the case and ask extra powerful questions, the legal professional also can additionally rent his or her very own professional, who could also be consulted before the trial and/or at some point of the lawsuits. Because the difficult facet's professional is in no way sworn in as a witness, the identification of the professional also can additionally in no way be regarded to the opposing facet, and will in no way be cross-tested. Although this might assist a legal professional's case a extraordinary deal, charges worried with hiring knowledgeable could also be prohibitive, so as that they aren't utilized in maximum instances.

Once the opposing facet has cross-tested the witness, the courtroom docket can pay attention arguments from each facets on the matter of whether or not the individual must be identified as knowledgeable . additionally to difficult that the know-how of a witness hasn't been mounted, which the individual is thereby unqualified to supply reviews on problem count, arguments are often made that the individual's know-how is constrained. Challenging the constrained know-how of a witness could also be administered at some point of cross-exam. If the individual's know-how is deemed constrained, she or he also can additionally nonetheless be capable of supply reviews, however the individual's testimony might be given little weight.

Regardless of whether or not the witness's qualifications are challenged, the previous selection rests with the decide. If the decide is happy that the witness has enough training and luxuriate in to testify and shape reviews on problem count related to the case, the courtroom docket will apprehend that the individual may be a professional. The vicinity of know-how that's identified are often wide (inclusive of being knowledgeable in pc generation) or constrained to a slim area of experience (inclusive of being knowledgeable on a specific piece of software program).

Just thanks to the very fact someone may be a professional during a single trial, doesn't always imply that she or he might be identified in the other trial. Being declared knowledgeable applies best thereto unique case, and doesn't convey ahead to another instances therein you'll testify within side

the destiny. for each trial, the way of being identified as knowledgeable need to start another time .

Experts Who aren't Witnesses

Lawyers are taught in no thanks to invite a question that they don't recognise the answer to. However, despite the very fact that she or he has know-how in practising regulation, the legal professional could have constrained expertise of generation or different specialised fields. To make amends for this loss of experience, professionals are often used as consultants.

Regardless of whether or not a consultant consulting with the legal professional testifies in courtroom docket, the prosecution or protection legal professionals also can additionally use her or him to supply extra perception to a case at some point of the direction of an ordeal .The legal professional also can additionally visit professionals previous to an ordeal and/or at some point of lawsuits. In many instances, the professional will write reviews that designate technical elements of a case in layman's phrases, and document any errors obvious in witness statements that comprise technical statistics or within side the processing of proof. due to the statistics furnished through the professional, the legal professional can higher put together for the capacity testimony of witnesses, and crossexamine them on technical elements of a case. Because the representative is in no way officially utilized in courtroom docket (i.e., sworn in to supply testimony), one facet may in no way recognise the decision or lifetime of a representative being utilized by the choice facet. Becoming an witness

• Appendix A

In a few instances, professionals also will be found in courtroom docket. The professional will concentrate to testimony, offer statistics on technical anomalies or different information in what a witness testifies to, and may even offer a couple of observe-up questions that the legal professional can use. When the opposing facet tries to qualify a witness as knowledgeable , the representative can help in clarifying regions of the witness testimony, and propose questions for cross-exam which may disqualify the witness as being knowledgeable .

Experts in numerous fields are also used for the motive of finding out proof so one are often used within side the case. as an example , DNA proof also can additionally play a key function during a homicide trial, or one concerning sexual attack or paternity. A DNA professional is perhaps employed to see blood or semen samples. Through the finding out , the validity of this proof could also be decided, and might display that it suits a defendant or has been tainted during a few manner. Through such assessments, the guilt or innocence of somebody are often mounted, and might assist to make a decision whether or not the case must be dismissed. Needless to say , if any of the outcomes had been utilized in courtroom docket the individual might then be referred to as a witness, and altogether likelihood undergo the way of being certified as knowledgeable witness.

Although professionals are often utilized during a case without ever acting as a witness, professional witnesses are also normally used within side the potential of a consult. The legal professional who referred to as the witness also can additionally request the individual still be within side the court docket to supply perception into technical problems, or help in several approaches. Because the courtroom docket has already identified the individual as knowledgeable, there could also be a bonus of being capable of re-name the witness to the stand to supply additionally testimony on information as they get up at some point of the trial.

Types of Expert Witnesses

A professional witness testifies with regards to problem count wherein she or he has know-how, so it must come as no wonder that thanks to the very fact there are such tons of extraordinary subjects, there are numerous extraordinary sorts of professional witnesses. Although professionals exist in many fields, variety of the additional commonplace place ones utilized in trials consist of:

- Civil litigation Experts
- Criminal litigation Experts
- Computer forensic Experts
- Medical and psychological Experts
- Construction and architecture Experts

Criminal Litigation Experts

Criminal litigation professionals are wont to help within side the prosecution and protection of individuals worried in against the law. Criminal litigation entails movements con to people who've dedicated unlawful acts, who're introduced to courtroom docket through the authorities to deal with expenses of breaking precise legal guidelines. to assist in expertise technical information of a case, examine and gift proof, and perform different capabilities that would fine be addressed through knowledgeable during a associated area of experience, professional witnesses are used.

The specialties of crook litigation professionals utilized in courtroom docket range significantly. There are professionals in nearly any area you'll believe who are often wont to provide an evidence for any sort of proof or thing of a case. In crook instances, the majority of execs utilized by the prosecution might be participants of the police, or others worried within side the research. As we've mentioned, the person who administered a pc forensic exam will frequently be referred to as as a witness, and may be certified as knowledgeable during a selected vicinity of generation. Similarly, during a case concerning a automobile twist of fate, a policeman skilled as an twist of fate reconstructionist will acquire proof on the scene of a visitors twist of fate, and reconstruct the aim, outcomes, and different activities that caused the twist of fate from those

clues. The protection may additionally use professionals to help their function within side the trial. These professionals are often wont to perform assessments and evaluation information of the case, additionally to supply opportunity interpretations of the proof. By supplying this know-how to a case, the knowledge of the case find yourself clearer to the decide, jury, and different events worried within side the case.

As we cited formerly, professionals are also wont to offer technical consulting to felony recommend, which they function a aid for explaining technical information. This perception will show beneficial now not best at some point of the trial, however additionally at some point of discovery and depositions, Civil Litigation Experts

In addition to crook instances, professionals are utilized in civil litigation wherein one celebration sues the other to reclaim what they experience is owed them. In doing so, civil litigation courts offer a discussion board for resolving those disputes. Different sorts of civil litigation can contains any range of lawsuits among people and/or corporations, inclusive of:

- Libel and slander
- Land disputes
- Probate of wills
- Wrongful dismissal
- Malpractice
- Personal injury
- Wrongful demise
- Contract disputes
- Other disputes among people and/or corporations

In searching on the various felony movements which may arise in civil courtroom docket, you'll see that now not all of them contain suing for economic settlements. In many instances, civil litigation tries to make a decision the rights of an man or woman, the scope of an settlement, or the goal of a contract. as an example , if someone died with out a will, the courtroom docket are often required to make a decision the requirements of the deceased, and therefore the thanks to fine divide the property among the individual's spouse, kids, and different fascinated events. To decide the knowledge of a case, and are available to an equitable selection, professional witnesses are often wont to assess and help in expertise the knowledge of the case. These professionals are frequently the equal sorts as those that are often utilized during a crook trial, inclusive of forensic accountants, clinical professionals, and different experts who consider any area which may offer perception to elements of the case.

Even though civil courtroom docket isn't the same as crook courtroom docket, the 2 frequently overlap. In addition to the use of the equal kinds of professionals in each regions of regulation, a case this is held in crook courtroom docket can also additionally later seem in civil courtroom docket. A famous instance of that is the O.J. Simpson trial wherein he changed into acquitted of the murders of humans, however changed into later discovered accountable in civil courtroom docket and ordered to pay damages in a wrongful demise in shape. Just due to the fact an man or woman is attempted in crook courtroom docket doesn't imply he or she will't be sued later in civil courtroom docket.

Computer Forensic Experts

As you properly recognise from studying this book, pc forensics is the gathering, exam, renovation, and presentation of virtual proof. Computer forensic professionals accumulate and study capacity proof at some point of an research, inclusive of information that's been deleted, encrypted, or broken. Any steps taken at some point of this manner are documented, and methodologies are used to save you the proof from being altered, corrupted, or destroyed. As we've careworn at some point of this book, any case concerning pc forensics must continually be handled as aleven though it had been going to courtroom docket, and that any documentation and proof will subsequently be grew to become over to a prosecuting legal professional.

In crook instances, the protection legal professional may additionally rent his or her very own professional to check the proof, and decide whether or not any mistakes had been made at some point of the exam of the pc. The professional will even record the movements she or he took, on the way to typically be integrated right into a very last document that's submitted to the legal professional. This professional will also be required to testify in courtroom docket, however this time on behalf of the protection legal professional.

While serving as a professional for the protection, the pc forensic professional must continue to be independent and carry out among the equal capabilities as that of the prosecution. Any examinations she or he plays might contain inspecting, maintaining, and offering proof, and may also require gathering extra proof that changed into ignored at some point of the research. In doing so, the professional might try to locate opportunity motives for the presence of information, inclusive of figuring out whether or not a Trojan horse, botnet, or different malicious software program changed into gift at the device.

Because she or he is operating on behalf of the protection, it's far vital that any patron-legal professional statistics this is inadvertently received is saved non-public and now no longer divulged with out consent of the legal professional or below order of the decide. Computer forensic professionals will also be utilized in civil litigations. Because statistics coping with a case can be saved on computer systems or different gadgets, pc forensic professionals can be used to look for information inclusive of e mail,

textual content messages, chat logs, Web webpage records, calendar documents, spreadsheets, files, snap shots, and different documents on a device. Examining this information can also additionally monitor information that discover an adulterous affair, fraud, malfeasance, downloading or traveling unlawful or worrying fabric (inclusive of pornography), or different sports that might decide the out- come of a lawsuit.

Because the information received thru pc forensics consists of files, spreadsheets, and different documents that comprise statistics out of doors of the pc professional's scope of expertise, extra professionals could be used to provide an explanation for what has been discovered. In such conditions, the research and resulting crook or civil litigations will frequently use different professionals which might be desirable to the proof.

Medical and Psychological Experts

Like pc forensic professionals, clinical and mental professional witnesses may be utilized in each civil and crook litigation. Medical and mental professionals respectively offer perception and help in bodily and intellectual problems that can be worried in a courtroom docket case. They can be utilized by both facet in a courtroom docket case to carry out assessments, examine present diagnoses, or testify approximately technical information associated with proof.

Medical professionals are medical doctors or fitness experts which might be devoted to specialised fields of medicine. They can be used to carry out DNA or toxicology assessments, testify to the volume of accidents suffered through a sufferer or plaintiff, or offer statistics on diseases, disabilities, practices, and/or strategies. Some of the alternative regions wherein they offer specialised help consist of:

- Dentistry, that can consist of forensic dentistry and chew marks
- Drugs, which can also additionally contain attesting approximately prescription medicine or unlawful tablets taken through a man or woman. This form of professional can testify approximately extraordinary kinds of tablets and their outcomes, or carry out and examine drug assessments on an accused individual or people worried in a case.
- Malpractice, wherein mistakes made through medical doctors or clinical experts are evaluated, reported, and offered in courtroom docket.

Psychological professionals are medical doctors and clinical experts who concentrate on regions of intellectual fitness, mental, and psychiatric fields. They can be used to assess and testify to the competency of an accused individual or man or woman worried within side the case, inclusive of while it wishes to be decided whether or not someone is suit to face trial, or to set up the intellectual country of someone while against

the law took region. In hearings concerning kids, they will additionally be used to set up whether or not a figure is unfit, or must be allowed to have unsupervised entry to kids. Some of the regions wherein they offer specialised help consist of:

- Diagnosis and remedy of intellectual illnesses
- Medications and psychotropic tablets
- Standards of care
- Emotional misery and outcomes of against the law or occasion

Since clinical and mental experts can be utilized sooner or later of an exploration, they will be needed to affirm with respect to insights they outfitted ahead of time or confirmation got through them. For example, if a scientific or conduct analyst had been utilized to expand a profile of a chronic executioner and victims identified with the case, the insights in the past outfitted to police may appear as evidence in a tribulation. The expert would then need to affirm, to give a clarification to the systems that had been utilized, and give a clarification to data that will not be unquestionably perceived to the court agenda.

Construction and Architecture Experts

Criminal and common prosecution likewise can contain issues that adapt to genuine property and the way wherein a developing or shape changed into constructed or designed. To offer insight and contributions in those examples, creation and design proficient observers can be utilized. A portion of the elective locales wherein they offer particular assistance comprise of:

- Building and hearthplace codes
- Project the executives
- Defects underway or format
- Accidents and assurance

Development and design experts additionally can offer measurements on how occurrences concerning homes occurred. For example, if a developing changed into besieged, experts will be utilized to give a clarification to how the bomb changed into situated in a spot that may convey down the building. In criminal and common cases, experts additionally can offer discernment regarding how various sorts of damage had been because of terrible creation, botches in how the building changed into planned, or various issues that prompted money related misfortune, injury, or death.

Testimony and Evidence

Declaration and confirmation fall connected at the hip with one another in a court agenda case. Proof every now and again wishes a couple of account to put it into the setting of the case, and is predicated on witness

declaration to do that. When an individual providing specialized data of a case offers declaration, it can fall into one in all classifications:

- Technical declaration
- Expert declaration

Specialized stories are articulations given underneath pledge that blessing data of a specialized sort. In offering the measurements, the observer should be actually right while deciphering confounded and clinical issues to simple expressions and thoughts. In various expressions, comparably to validating around the case, she or he should moreover prepare the jury and additionally choose so they perceive the pertinence of those specialized data. Since it's far basic that the ones inside side the court agenda perceive what's being referenced at the remain, there are some of variables you may transfer in your declaration to make it extra conceivable to laymen, comprehensive of:

- Refrain from the utilization of language.
- Explain the which means and importance of expressions and abbreviations. For example, "EnCase is legal programming program that changed into used to collect data from the pc. It's an exhibited item which the FBI has utilized for parcels years."
- Provide a thesaurus of specialized expressions and thoughts to crime suggest. This will likewise be used by the court agenda journalist while interpreting your declaration.
- Provide charts and photographs so one can allow the jury as well as choose to higher perceive what's being talked around.

It is oftentimes gainful while bearing on specialized measurements to talk in a slow, gentle manner of speaking. Despite the fact that you should convey slow adequate that the court agenda columnist can viably decipher your announcement, and the choose and jury can notice the improvement of your declaration, you shouldn't impart so progressive that it appears you're belittling the ones inside side the room. Rehearsing the beat and wooden of your voice on pals and own circle of family members sooner than authenticating can help with sorting out the fine way of talk me unquestionably.

Since numerous people will not perceive sure innovation being referenced, and could find it intense in regards to your declaration, you should endeavor to utilize analogies while clarifying extreme ideas. For example, "IP addresses are similar as road addresses. The equivalent way your property adapt to will we various people perceive in which you live, IP addresses likewise are exact addresses that become mindful of one pc to others on a local area." By the utilization of a familiar idea, people can extra easily identify with what's being expressed.

Except if you're confirmed as an expert, you should ensemble from introducing any audits roughly the case, as they'll be considered inadmissible. You must country the data, and arrangement inquiries without providing any private or master ends.

Master observers furthermore ordinarily supply specialized declaration, in any case are fit for make greater on their criticism through communicating audits and ends. Master declaration is articulations given underneath vow through a distinguished as an expert in a chose observer's region. In providing data so one can help a jury as well as choose higher perceive the case, the observer can likewise moreover unequivocal a proficient assessment related with their area of specialized or concentrated expertise. The extent of this mastery is mounted while qualifying the observer as an expert, and figures out what the observer is and isn't permitted to express eventually of the preliminary. Any surveys which may be out of entryways of the person's skill are thought about prohibited.

Rules of Evidence

The suggestions that direct whether somebody might be recognized as an expert observer, and the suitability of verification, are managed through the legitimate rules of the ward of the court agenda wherein the confirmation could be added. Thus, investigators must wind up familiar with the applicable lawful guidelines. These guidelines are finished resolution and are normally systematized directly into a record named Rules of Evidence.

In the USA, Congress kept the Federal Rules of Evidence (FRE) as a firm of necessities that choose how verification is offered and considered permissible in court agenda. Since nation and government lawful rules are uncommon, numerous states have furthermore followed their own special units of guidelines, various which can be same to the ones inside side the Federal Rules. The FRE conveys a decent estimated scope of guidelines, nonetheless the ones adapting to surveys and expert declaration are characterized underneath Article VII.

The guidelines underneath this Article envelop:

- Rule 701, Opinion Testimony through Lay Witnesses
- Rule 702, Testimony through Experts
- Rule 703, Basis of Opinion Testimony through Experts
- Rule 704, Opinion on Ultimate Issue
- Rule 705, Disclosure of Facts or Data Underlying Expert Opinion
- Rule 706, Court Appointed Experts

Rule 701, Opinion Testimony by Lay Witnesses

Rule 701 addresses evidentiary observers who aren't in court agenda to offer proficient declaration. Along these lines, the extent of declaration is

obliged to exercises that unfolded, and to what somebody saw, heard, or did. Any surveys and inductions that the observer makes are compelled to the ensuing models:

- They should be normally basically dependent on their conviction.
- They are valuable to achieving a perfect aptitude of the declaration or resolve of a reality in a difficult situation.
- They aren't fundamentally founded absolutely on clinical, specialized or concentrated skill. Albeit this standard permits the observer to have an assessment at the exercises she or he mind nessed, it does limitation the assessment to a thin extension. For example, if a mugger held a firearm in your mind and expressed, "Give me the entirety of your cash. You don't have to pass on," a reasonable conviction of this event may be that he changed into going to kill you in the event that you didn't supply him your money. Such audits are bereft of any particular skill and manage explaining the event, and what you accepted changed into happening.

Rule 702, Testimony by Experts

Rule 702 addresses declaration through proficient observers who might have surveys basically dependent on clinical, specialized, or concentrated mastery. As we referenced ahead of time, for this standard to follow, the observer should be ensured as an expert sooner than she or he affirms in court agenda. Rule 702 states the ensuing: "If clinical, specialized, or diverse specific aptitude will help the trier of reality to perceive the evidence or to choose a reality in a tough situation, an observer affirmed as an expert through mastery, expertise, experience, tutoring, or preparing, can likewise furthermore affirm thereto inside side the state of an assessment or in some other case, if (1) the declaration is basically founded absolutely upon enough data or data, (2) the declaration is the produced using trustworthy ideas and procedures, and (three) the observer has carried out the ideas and methods dependably to the data of the case."

In looking at this standard, you may see that the component of providing proficient declaration is to help in aptitude, sorting out, and in regards to evidence and data offered inside side the case. The measurements the expert offers should be essentially founded absolutely on data or data and should utilize reliable ideas and strategies. In various expressions, any methods utilized might be repeated.

Logical methods that now not, at this point mainstream also can not be utilized for proficient declaration. For example, suppose an expert principally based absolutely his decisions that the respondent changed into mindful on physiognomy, that is a pseudoscience wherein criminal direct might be chosen fundamentally dependent on a litigant's facial appearance, head shape, and changed materially capacities. Since this is certainly not a reliable or mainstream science, the audits, ends, and most likely the litigant's finished declaration may be prohibited.

Rule 703, Basis of Opinion Testimony by Experts

Rule 703 is some other chief principle for proficient observers and the surveys they will unequivocal in testi-fying. This rule expresses: "The data or data inside side the one of a kind case whereupon an expert bases an assessment or deduction can be the ones seen through or made respected to the expert at or sooner than the paying attention to. On the off chance that of a sort reason capably depended upon through experts inside side the interesting region in shaping surveys or deductions upon the issue, the data or data need now presently don't be allowable in verification so with respect to the assessment or surmising to be conceded. Realities or data which may be in some other case prohibited will now presently don't be uncovered to the jury through the defender of the assessment or induction with the exception of the Court discovers that their probative cost in supporting the jury to evaluate the expert's assessment widely offsets their biased effect."

The establishment of this standard is that experts have get section to confirmation or insights past to an affliction. In such occasions, the expert can likewise also shape an assessment on those data, in any event, assuming they're currently not, at this point utilized or are forbidden in court agenda. For example, a psychological expert is likely cognizant that a respondent being investigated for responsibility for porn had before feelings for baby attack. Regardless of whether the jury isn't permitted to focus roughly those previous feelings, the therapist might need to utilize this measurements to shape a learned assessment that the litigant is a pedophile. The proficient couldn't bring up the prior feelings in court agenda, notwithstanding may need to country an assessment that changed into molded through this insights.

Rule 703 is questionable to a couple, as confirmation that couldn't be used in court agenda is being used in a sideways way. The verification the expert utilized doesn't totally offer an indirect access to documenting evidence, despite the fact that there might be a couple of legitimacy to this contention. On the off chance that the jury has issue contrasting the expert's surveys, the choose might need to offer them with insights and evidence that the expert utilized, in any event, assuming it changed into in some other case unacceptable. Indeed, even alevn however the expert's assessment is thought about basic to a hardship, and may even offset the biased effect of sure verification, this isn't to make reference to that restricting features are feeble to an expert's conclusions. The witness can regardless be cross-tried to extend the legitimacy of their audits, and the contradicting aspect can name their own special expert observers to offer freedom ends and surveys at the data of the case. Nonetheless, an issue with this strategy is that after experts are known as to project or offer clashing surveys to a previous expert, the stop final product is that the jury can wind up compelled or even unengaged. Since the surveys communicated can in the end be disposed of, it's far alluded to as garbage declaration.

Rule 704, Opinion on Ultimate Issue

Rule 704 offers with the capacity of felony recommend to item to reviews made through knowledgeable, and what an expert can testify to insecure conditions. In maximum instances, a legal professional cannot item to an opinion made through knowledgeable, due to the actual fact its validity must be determined through the info of the case. in numerous phrases, cross-exam and proof within side the case must assist evolve a variety concerning whether or not the professional is accurate. However, an objection could even be made if the professional testifies approximately the intellectual country of a defendant during a very crook case, and whether or not the defendant had this intellectual situation whilst committing the crime or while the utilization of it as a protection. The professional isn't accredited to make this sort of end, because the knowledge of the case must determine this trouble, now not the reviews of a witness.

Rule 705, Disclosure of Facts or Data Underlying Expert Opinion

Rule 705, Disclosure of Facts/Data Underlying Expert Opinion Rule 705 addresses problems raised in Rule 703 concerning information and knowledge that had been used to shape an expert opinion being disclosed to the jury. during this rule, the professional can also additionally offer an opinion without liberating statistics or proof that helped to shape that opinion. He or she is going to be capin an edge to reveal those information if the decide instructs her or him to achieve this, or might be required to reveal sure information at some point of cross-exam. This rule states that "the professional can also additionally testify in phrases of opinion or inference and supply motives consequently with out first attesting to the underlying information or information, except the Court involves within the other case. The professional can even additionally in any occasion be required to reveal the underlying information or information on cross-exam."

Rule 706, Court Appointed Experts

Rule 706, Court Appointed Experts Rule 706 offers recommendations on how professionals must be appointed through the courtroom docket. The rule offers statistics coping with:

- How they're appointed
- The economic repayment they acquire
- Disclosure, which sincerely states that the courtroom docket can even additionally tell the jury that the courtroom docket appointed an witness
- That felony recommends (i.e., the prosecution and protection) may additionally name their very own professional witnesses

Authentication of Evidence

The regulations of country courts can also additionally range from those of the federal courts, and thus the regulations for proof in crook trials may additionally range from those for civil trials. Generally, proof should be authenticated, which on this context typically manner that some witness should testify to its authenticity. within the case of virtual proof, this might be a witness who has private expertise of the proof (e.g., someone who shared the pc with the accused and located the record or document in query at the pc). it should even be the primary responder who noticed the proof on display while responding to the incident, or knowledgeable who tested the pc and proof after it become seized. In phrases of while a reproduction of the info became made the utilization of forensic software program, attesting approximately how the software program authenticates a information photograph is typically all that's important. one of the utmost vital elements of constructing ready to introduce proof in courtroom docket is deciding which witnesses will testify on its life and validity, describe the situations of its discovery, and affirm that it's now not been tampered with. Certain sorts of proof are from time to time held through the foundations of Evidence to be self-authenticating. this manner testimony on authenticity isn't required and typically refers to things like public files below seal, licensed copies of public statistics, authentic courses, and also the likes of . it's likewise feasible for each facets at trial to evolve to stipulate on the authenticity of slightly of proof, wherein case it does now not should be authenticated thru testimony. When each facets conform to the stipulation of a reality (inclusive of the very fact that the proof is authentic), the decide will endorse the jury that they're to presume that the reality is authentic and it isn't always a count that has got to be proved or disproved at trial.

Evidence Processing

Computer forensic requirements had been advanced that follow to the gathering and renovation of virtual proof, which differs in nature from maximum different kinds of proof and as a result calls for extraordinary techniques of managing. Following strategies which might be right, popular, and, in a few instances, prescribed through regulation in coping with proof is critical to the a hit prosecution of a cybercrime case. The right managing of those strategies comes into play at extraordinary factors in a tribulation:

- If proof isn't always amassed and treated in keeping with the right requirements, the decide can also additionally deem the proof inadmissible while it's far offered (typically primarily based totally at the opposing legal professional's movement to suppress) and the jury participants will in no way get a threat to assess it or don't forget it in making their selection.
- If the proof is admitted, the opposing legal professional will assault its credibility at some point of wondering of the witnesses who testify concerning it. Such an assault can create doubt in jury participants' minds

so one can purpose them to brush aside the proof in making their selection—and possibly even taint the credibility of the complete case.

The complete research could be of little price if the proof that indicates the defendant's guilt isn't always allowed into the trial or if the jury offers it no weight. Thus, right managing of proof is one of the maximum vital problems going through all crook investigators and, due to the intangible nature of virtual proof, cybercrime investigators in unique. Because that is such an vital subject matter—now no longer best for investigators, however additionally for prosecutors, judges, and justice device experts worried in cybercrime instances—many agencies and courses are dedicated totally to problems regarding virtual proof:

- The International Organization of Computer Evidence (IOCE) changed into mounted in 1995 to offer a discussion board for regulation enforcement businesses round the sector to alternate statistics approximately pc forensic problems; its U.S. issue is the Scientific Working Group on Digital Evidence (SWGDE).
- The International Association of Computer Investigative Specialists (IACIS; www.cops.org) is a nonprofit corporation this is devoted to teaching regulation enforcement experts within side the vicinity of pc forensics.
- The International Journal of Digital Evidence (www.ijde.org) is a web guide dedicated to discussions of the principle and exercise of managing virtual proof.
- Computer Forensics Magazine is posted through DIBS, a maker of pc forensic system. Computer Forensics Online (www.shk-dplc.com/cfo) is a Webzine this is run through legal professionals and technical experts that specialize in pc regulation.

Various similar resources that target pc criminology are to be had, and extra wide-principally based absolutely offices comprehensive of the American Academy of Forensic Sciences (www.aafs.org) adapt to pc wrongdoings and virtual verification close by various criminological points. A gander at any of those resources will screen that virtual verification overseeing is a major topic that may easily fill various books (and as of now has). It is far past the extent of this reference section to cowl every thing of get-together and keeping up with virtual confirmation.

Admissibility of Evidence

There are some of necessities for confirmation to be allowable in court docket. The verification should be skilled (i.e., trustworthy and believable), it should be appropriate (it tends to show a truth of the case), and it should be texture (it proves a difficulty this is in question inside side the case). Furthermore, to be acceptable in U.S. courts, evidence should be gotten legally. That is, it should be gotten agreeing with the lawful rules administering look for and seizure, comprehensive of legitimate rules communicated inside side the U.S. what's more, country constitutions. In

the event that evidence is gotten through an unlawful look for, despite the fact that it demonstrates the blame of the litigant, the verification is mulled over to be "polluted."

This is alluded to as the "summit of the poisonous tree" convention, or the exclusionary rule. Case guideline in a couple of purviews units one of a kind guidelines for the tolerability of clinical evidence. Under the Federal Rules of Evidence, Rule 402, all relevant verification is allowable other than as in some other case outfitted underneath the U.S. Constitution, through Act of Congress, or underneath the Federal Rules of Evidence themselves (e.g., verification got disregarding a presume's protected rights).

Rule 401 characterizes pertinent confirmation as "any evidence having a tendency to make the existence of any reality this is of impact to the self control of the movement extra presumably or considerably less most likely than it'd be without the proof." This is alluded to as the significance investigate. Another boundless every now and then carried out to clinical evidence is the general fame investigate, moreover alluded to as the Frye inescapable, which holds that a deliberate methodology should be commonly famous inside side the region sooner than the results of the methodology might be conceded as verification.

Digital Evidence

Albeit the guidelines of evidence concerning virtual data aren't basic, it's far constantly generally secure to surpass the negligible necessities for suitability. At the point when specialists avoid potential risk to ensure the uprightness of verification, above and past what the court agenda may find alluring, presently not, at this point best will the chance of getting the confirmation rejected through the choose be forestalled, be that as it may also the effect at the jury could be extra good. Associations comprehensive of the IACIS offer necessities administering criminological test techniques for their members. Appearing in court agenda which you clung to such inordinate necessities in taking part in the exploration will improve your case.

Most pc legal offices and experts concur on a couple of basic prerequisites concerning the overseeing of virtual verification, which might be summed up as follows:

- The one of a kind verification should be saved in a nation as close as achievable to the country it changed into in while found.
- If in any regard plausible, a real copy (photo) of the special should be made for use for test all together now no longer to hurt the uprightness of the exceptional.
- Copies of data made for test should be made on media which may be forensically clean this is, there should be no previous data at the plate or distinctive media; it should be totally "clean" and checked for independence from infections and deformities.

- All evidence should be very much labeled and reported and the chain of guardianship protected, and each progression of the legal test should be archived in component.

Testifying As an Expert Witness

Affirming as an expert observer might be a scary and upsetting appreciate, especially if it's your first time. You can be strange with the court agenda, its configuration, what's expected of you, and what will occur in court agenda. In spite of the fact that you can procure a couple of training from the lawful expert who will name you as an observer, often you get next to zero practice and experience like you're genuinely tossed inside side the place of extreme peril.

Albeit the court agenda can appear to be master and respectful, the minutes among occasions and breaks in court agenda might be earnestly tumultuous. Administrative work wishes to be handled, uncovers need to be coordinated, witnesses need to be ready and state-of-the-art, and individuals stressed in an affliction end up involved in a whirlwind of leisure activity at the rear of the scenes. Albeit this tumult can get out into the preliminary, what greatest people see while coming into a court agenda is an arranged and calm climate. Every individual stressed in an affliction have their own personal locale inside side the room and their own special obligations to do, comprehensive of the resulting:

- Judge This is a court agenda true that is both delegated or chosen to direct the court agenda, and make decisions on issues in preliminaries and hearings.
- Court journalist This is a court agenda official that translates the declaration and contentions made inside side the preliminary, which turns into a genuine document of the claims.
- Court representative This is a court agenda official that plays regulatory commitments, comprehensive of swearing in witnesses, overseeing uncovers, and acting various commitments for the court agenda.
- Bailiff This is a court agenda official that is responsible for maintaining control and decency inside side the court agenda. In a couple of locales and nations, the bailiff can likewise furthermore as an option be court agenda security, and be designated as a novel constable of the police. The bailiff has authority of the jury and could accompany them inside and outside of the court agenda, and can also do various commitments, comprehensive of bringing in witnesses prepared out of entryways the court agenda.
- Prosecutor This is the lawful expert addressing the nation (or the Crown in Canada and the United Kingdom) in hooligan court agenda occasions. In doing as such, the examiner addresses the people and is responsible for taking lawful offense movement contrary to the litigant and setting him, her, or them being investigated.

- **Defense lawful expert** This is the lawful expert addressing the litigant in a hooligan court agenda case.
- **Plaintiff** This is the individual suing a respondent in common prosecution. In common case, each the offended party and the litigant may also have their own personal crime suggest.
- **Defendant** This is the individual accused of illegal (in evildoer court agenda) or the individual being sued (in common court agenda).
- **Jury** This is a bunch of occupants which have been settled on to focus evidence and render a decision.
- **Witnesses** These are individuals bearing witness to exercises that occurred or confirmation offered as uncovers inside side the preliminary.
- **Spectators** These are members of the overall population or potentially media looking the trial. They can likewise moreover incorporate mates and own circle of family members of the respondent, or intrigued occasions who've come to take a gander at the claims. Of those jobs, filling in as an observer might be one of the most extreme horrible to satisfy. Without the declaration and confirmation an observer offers, it'd be unrealistic to harvest a conviction.

Despite the fact that authenticating might be awkward in any event, when you have long periods of appreciate as an evidentiary or expert observer, seeing around the way calms bunches of the pressure. In the areas that notice, we'll talk components of the court agenda, preliminary claims, the methods that investigators and assurance legitimate experts can likewise also utilize, and what you may accept while attesting. The less amazements and the extra coordinated you're, the less difficulties you'll coincidentally find at the stand.

Layout of a Courtroom

Courts are generally determined in a chosen way, with seating arrangements and installations coordinated for exceptional capacities. Dissimilarities can be self-evident while assessing courts which may be utilized for uncommon capacities or legal designs, comprehensive of while assessing own circle of family members court agenda to a military court agenda military, or the ones of different nations. In any case, regardless of whether those varieties are noticeable, likenesses in capacity can ordinarily be distinguished.

As demonstrated in Figure A.1, a court agenda configuration can incorporate severa man or lady added substances, comprehensive of the resulting:

- **Judge's seat** This is a table area where the choose is situated to manage the preliminary

- Witness stand This is an encased seating area wherein the observer offers declaration.
- Court journalist's table This is in which the sworn claims of the preliminary are deciphered.
- Court agent's table This is in which court agenda measurements are kept up with.
- Jury holder This is seating for members of the jury.
- Prosecution's work area This is in which the examiner is situated. In a common case, this will be the offended party's work area.
- Defendant's work area This is in which the litigant and their lawful offense board (i.e., security lawful expert) is situated.
- Podium This is in which the investigator and assurance legitimate experts will stand while formally tending to the court agenda and assessing/cross-reviewing observers.
- Well of the court agenda This is the essential area of the court agenda wherein claims of the preliminary take locale.
- Bar This is a railing separating the exhibition from the appropriately of the court agenda.
- Gallery This is a spot where members of the overall population, media, and various onlookers are situated.

A court agenda serves in light of the fact that the arranging area of a hardship, and has a dramatic layout. When looking at Figure A.1, you may see that it's far expected to house an objective market, as most extreme preliminaries are available to public observers. Albeit public preliminaries offer obligation concerning how they're completed, the format of a court agenda is moreover enlivened as the centuries progressed vintage exercise of it being a state of public entertainment. The organization of a court agenda is intended to offer most perceivability to the ones looking the preliminary (regardless of whether they be choose, jury, or onlookers), and to acknowledgment their advantage at the developments and entertainers stressed inside side the court agenda way.

To help harvest this, the added substances of a court agenda are layered to different heights. The conclude's seat is found better compared to various seating locales inside side the room. It allows her or him to lead over the court agenda from a vantage factor that disregards the entire thing, nonetheless it furthermore passes on that the choose is a definitive and executing discover that has control over the room. The testimony box will likewise be raised notwithstanding is decline than that of the choose's seat, driving each body offering declaration to appearance up on the choose, in any case keep on being at eye stage with the lawyers who remain at a platform inside side the appropriately of the court agenda while investigating and cross-reviewing observers. Less seen are the court

agenda authorities who sit down on the foot of the choose's seat. Albeit the court agenda columnist ordinarily remains not noted sooner or later of the preliminary while translating the claims, the court agenda representative is gener-closest companion noticed best while swearing in witnesses or acting distinctive court agenda capabilities. To the aspect of the choose, a jury holder offers the ensuing fine doable seats. In a jury preliminary, the attendants could be fit for see and focus the entire thing inside side the preliminary since it performs out toward the front of them, actually like the observers who sit down inside side the exhibition to the backs of the lawyers and the blamed.

Technology in the Courtroom

Despite the fact that subculture has directed the design, age has moreover motivated the court agenda. More current courts are every now and again developed with age in considerations, while more seasoned ones can be retrofitted to house PC frameworks and show virtual verification extra easily. Since there aren't any prerequisites for the inventory of age, what you can see can run fundamentally among courts.

Indeed, even in more seasoned town halls, a definite amount of age could be blessing. Amplifiers are utilized inside side the observer holder, choose's seat, and platform to allow voices to be heard sooner or later of the court agenda, and lawyers will much of the time use PC frameworks to keep their notes and various measurements acquainted with court agenda. Albeit more moderen courts are intended to have an enough scope of electrical retailers, this ordinarily isn't the situation in more seasoned town halls. All things considered, those and some different contraptions acquainted with court agenda can likewise also require additional lines as well as power bars to be taped or hung all through the floor. This might be a touch sudden to look while walking around the testimony box, and venturing over a mat or conduit tape overlaying electric strings. In more moderen or retrofitted courts, there might be an additional reconciliation among age and the equity gadget. A portion of the unrivaled age you can situate in those courts can likewise furthermore comprise of the ensuing:

- Document computerized digicam This is an instrument on which documents or a little to medium-length thing might be situated all together that an overhead advanced digicam can hold onto its photograph. The advanced digicam can likewise moreover mission the photo to a presentation (actually like an overhead projector may) or communicate it to video show units arranged on the whole inside side the room.
- Display video show units These are utilized to show previews, media introductions, or diverse yield from a pc or a record computerized digicam. These might be level board shows which may be set at the choose's seat, at the observer compartment, at the court agenda official's desk(s) (i.e., court agenda agent, court agenda correspondent), on crime suggest's tables, and among sets of hearers inside side the jury holder.

- Annotation video show units These are video show units put on the platform and witness compartment that grant in plain view drawings to be made, comprehensive of charts or various measurements that enhance what's shown on various video show units inside side the court agenda.
- Real-time record This grants translated declaration to be coordinated to the choose's seat and suggest tables.
- Translation and listening devices These grant any declaration in some other language to be spoken directly into a mouthpiece, deciphered through some other individual, after which broadcast through infrared or diverse innovation to listening contraptions (i.e., headsets, and so on) which may be worn through the choose, attendants, lawful offense suggest, court agenda authorities, and others immediately connected with the preliminary.
- Videoconferencing This involves cameras steady inside side the court agenda which may be focused at the choose, witness, and lawful offense suggest on the platform. Different cameras will likewise be establishment in various rooms of the town hall, comprehensive of the choose's chamber or a room utilized for declaration through individuals who've been pardoned from verifying inside side the court agenda. Utilizing the previews caught through those cameras, video conferencing would then be able to be utilized for pretrial meetings, distant observer declaration, or various claims. For example, a baby who changed into physically mishandled is most likely pardoned from going through their victimizer inside side the court agenda, and be fit for affirm from a distant spot.
- Computer-equipped suggest tables These are tables used by the indictment and assurance legitimate professionals. These can be discretely furnished with electric retailers and ports that grant associations with show video show units or various abilities to be had through the court agenda.
- Printers These license measurements showed on video show units to be distributed, notwithstanding data from any or exact PC frameworks inside side the court agenda.

Since the degree of age to be had in a court agenda can likewise moreover run, you can need to talk over with the arraignment concerning whether sure framework could be close by to your declaration. For example, on the off chance that your declaration is predicated on showing the previews or various archives found on a troublesome circle, it'd be valuable to perceive whether they might be shown on video show units as of now inside side the court agenda, if a pc projector and show are to be had, or in the event that you might need to convey your own personal framework. By being coordinated and aptitude what's to be had to brought to the table your declaration, you may avoid conditions that make bearing witness to tumultuous and upsetting.

Order of Trial Proceedings

The preliminary way in actuality begins off evolved while a suspect is captured or a warrant is given for a presume's capture. After the capture, the respondent is taken sooner than a Justice of the Peace (a choose or, in a couple of cases, the city hall leader of a town or town) inside a definite period—regularly inside 48 hours—and charged. This arraignment is a relaxed way wherein the Justice of the Peace mentions to the respondent what costs had been recorded contrary to her or him, Mirandizes the litigant, and units or denies bail. An underlying paying attention to ordinarily takes locale inside certain days. In this paying attention to, the arraignment should blessing adequate evidence to convince the conclude that the litigant should visit preliminary.

In a couple of occurrences, the litigant is going sooner than an amazing jury instead of a decide. This is a secret continuing wherein the terrific jury goes to a choice whether nearby down a prosecution. Then, an appropriate arraignment can be held, at which the litigant can enter a supplication for the costs contrary to her or him.

Prior to the genuine preliminary, there is regularly a pretrial show or paying attention to at which movements might be documented (e.g., asking for an exaltate of setting). At last, the case is going to preliminary. In the event that the respondent argues now not, at this point capable to the costs, a jury is picked through the voir critical way, sooner or later of which each feature gets to reprimand limit attendants and strike, or avoid, a definite range. The choose trains the jury at the pertinent guideline, after which the lawful experts each supply a hole announcement. Since the heap of proof is at the indictment, the arraigning legitimate proficient gets to head first with a hole presentation. After the insurance lawful expert's setting up presentation, the indictment considers witnesses. With each witness, the arraignment poses inquiries; this way is known as immediate examination. Then the security legitimate proficient is approved to impugn the observer roughly the subjects that had been presented up eventually of direct test. A short time later, the indictment can divert, and afterward the security can recross. This way happens with each observer till each lawful experts are finished pondering that observer.

An examiner or IT master validating as to private skill of the evidence inside side the case (an evidentiary observer) could be authenticating as an arraignment witness and accordingly could be on the double tried through the investigator and get tried through the assurance legitimate proficient. Master observers can likewise moreover affirm for both aspect, nonetheless should be guaranteed as experts past to verifying all together that any surveys they've can be ensured inside side the declaration.

At the point when the indictment has offered every one of its observers and confirmation, the security legitimate proficient commonly makes a development to ignore the case as a result of loss of verification. On the off chance that this development is without a doubt, the preliminary is finished and the respondent is going free. On the off chance that now no

more, the assurance gives its case, calling observers to testify. These witnesses are get tried through the examiner, etc, inside side the equivalent way on the grounds that the indictment witnesses. After the assurance has offered its case, the arraignment is approved to name answer observers, and the insurance can counter the ones witnesses.

At last, while the entirety of the replies are done, the legitimate experts offer their leftover expressions (which aspect is going first depends upon at the court agenda) and the choose offers additional orders to the members of the jury, who're then, at that point despatched out to accomplish a decision.

Subpoenas

A Subpoena is a crime record this is given through the court agenda to illuminate you which you are needed to stand by court agenda to offer verification as a witness. The court agenda can likewise furthermore summon you for the benefit of the indictment, the insurance, or each. In looking on the summon demonstrated in Figure A.2, that is a genuine summon with the relevant data disposed of, you may see that it conveys a lot of insights concerning an affliction, comprehensive of the resulting:

- The call and adapt to of the individual being gathered to court agenda
- The date and time you're needed to stand by court agenda
- The call of the litigant
- What the respondent is accused of
- The adapt to in which the preliminary will take area
- The call and reach out to measurements of the official in cost of the case
- The call of the legitimate proficient summoning you
- Instructions to convey any books, records, composing, or diverse uncovers related with the present circumstance with you The summon is hand-brought to you through a request official or distinctive court agenda official, who will utilize measurements at the summon and distinctive touch insights that you can have once in the past given to the agent or legitimate proficient. Whenever you have got been presented with the request to appear to be in court agenda as an observer, you're needed to stand by. On the off chance that you neglect to pause, evildoer costs can be squeezed contrary to you, and on the off chance that you are indicted you can confront detainment as well as a fine.

Depositions

A Deposition is the way of pondering observers past to a hardship, and it's far utilized inside side the pretrial scopes of each respectful and criminal cases. In a statement, the observer is underneath vow and is

expected to illuminate the truth as a level however inside side the preliminary. Legitimate suggest can study and cross-study the observer, and can even utilize this as a likelihood to discover measurements that can be utilized inside side the later preliminary. Since the affidavit doesn't need a public conversation board, it can now at this point don't generally be held inside side the court agenda, notwithstanding as an option in a gathering room or whatever other setting that has been settled upon.

All through the affidavit, a court agenda correspondent or a transcriber documents the inquiries and articulations made, all together that they might be protected for fate reference. Albeit the statement doesn't refresh authenticating eventually of the preliminary, besides there are huge circumstances for why the observer can't pause (comprehensive of death sooner than the preliminary starts off evolved), the insights amassed inside side the testimony can later be used in preliminary. Lawyers can likewise furthermore utilize proclamations made in an affidavit to uncover inconsistencies in later declaration, subsequently disparaging the observer through showing mistakes among garbled explanations committed to underneath vow.

Affirming in a testimony is ordinarily substantially less formal than the actual preliminary, despite the fact that the equivalent behavior of showing respect for the court agenda and individuals stressed inside side the way applies. Along these lines, demands for a harm might be made each time required. In spite of the fact that it can be considerably less formal, you should not the slightest bit expect something is off the record. Any criticism made sooner or later of the affidavit could be recorded, so you should ensemble from articulating something you don't require saved for any kind of family down the line till you're farfar from the court agenda journalist and the spot in which the statement is held.

When an affidavit has been deciphered, an observer is given the likelihood to check its substance for any mistakes and to make redresses. It is indispensable which you look at the record altogether, because of the reality after you analyze and signal it, it's anything but a legitimate file. When inspecting the record, you should look for blunders in dates, occurrences, amounts, or specialized data which can appear to be later eventually of the preliminary as proof. The extra right it's far the substantially less danger a misstep could be utilized to negate dependable articulations made later in court agenda.

Swearing vs. Affirming

When filling in as an observer, you're extremely expected to advise the reality. To guarantee that you may accomplish this, one in all short proper systems is completed in that you guarantee to be genuine. They are:

- Swearing in
- Affirming

For various intentions, most extreme observers inside side the Western World are confirmed. This involves both holding your legitimate hand at the Bible or taking a Bible for your appropriate hand and holding up your left hand. In the wake of doing as such, you're then, at that point mentioned whether you vow to advise the truth "so help you God." In a couple of courts, the point out of God isn't utilized, despite the fact that most extreme keep up with to accomplish this. In pledging to educate the truth, you're presently an observer and might keep up with the task of providing declaration.

In case you're a skeptic or have non common beliefs that restrict you from pledging to God, there might be also the decision of putting forward. When you affirm, you will be mentioned to hoist your hand while committing to a vow to promise to advise the truth. In doing as such, no Bible or point out of God is utilized. Whenever that is completed, you're confirmed, and you have completed a declaration of genuineness that incorporates the equivalent load as being confirmed.

Asserting or promising to advise the truth happens immediately after you've been referred to as an observer and brought the stand. Whenever you've entered the observer holder, the choose or court agenda agent will find out if you might truly want to be confirmed or affirmed. Which you select is totally just about as much as you, and has no effect or predisposition inside side the exercises that notice, while you're bearing witness to. Whether or not or not you've been confirmed or attested, on the off chance that you lie you might be accused of prevarication.

Being insisted or sworn in can emerge in both common or hoodlum claims, notwithstanding testimonies and affirmations (which we'll talk subsequent). The object they're used in such a great deal of districts of guideline is simple: It is fundamental for the observer to advise the truth. On the off chance that the truth wasn't offered to the court agenda, a right determination of exercises can not be made, and a right decision can not be made.

Affidavits

An oath is an appropriate presentation of information. When you're an observer in a convict preliminary or common question you will be needed to offer a sworn articulation that diagrams the data as you understand them. This offers a put down model of your formal declaration. This composed account states what you saw, heard, or in some other case perceive to be the truth. In expressions of an expert observer, this will be insights this is inside your area of expertise. It is endorsed through you to approve that the entire thing you have got composed is true, and through some other person who has you are making an oath. The vow is which you both swear or affirm that the entire thing said inside side the record is authentic. The vow is taken through an individual legitimate through the court agenda, comprehensive of a legal official public or a court agenda official, which formalizes the record as being real and lawful offense.

Lawful Etiquette and Ethics

Similarly as with any real gathering, there are certain codes of conduct that should be followed. As per lawful offense manners and morals, you're expected to conduct your self with a chose phase of polished methodology while going to court agenda. Manners is the guidelines of socially beneficial direct and graciousness, while morals are moral ideas or values. Together, they layout how somebody acts inside side the court agenda.

Courts should be grave, mirroring the outrageous idea of the conversation board they offer. Directing your self such that proceeds with this environment demonstrates appreciate now not, at this point best to the court agenda itself, in any case moreover to people who should join in and include their destinies decided in preliminaries. Similarly as you will act in a limit and obliging way at a dedication supplier, service, or distinctive proper event, you should show the equivalent phase of appreciate inside side the court agenda. A portion of the ways to deal with uncover this appreciate comprise of:

- Dress minimalistically in big business clothing (comprehensive of a fit, dress, or diverse moderate attire you may put on to a venture get together or grave occasion).
- Arrive early and be to be needed to affirm while known as.
- When speakme to the choose, check with her or him as "your honor."
- Do now at this point don't murmur or impart inside side the court agenda aside from it's far genuinely significant. In the event that measurements should be traded, it's far higher to byskip a know to the lawful expert or diverse individual you're deliberating with.
- Bring best the notes you may use at the stand. Do now presently don't convey magazines or distinctive considering texture to byskip the time.

The crime behavior and good lead you show in a court agenda applies now not, at this point best to the ones going to as members of the jury and lawful offense suggest, be that as it may furthermore (and especially) to witnesses. The way you act inside side the court agenda and at the testimony box could be situated through others inside side the court agenda, and could affect the way they comprehend your believability as an observer underneath direct and interrogations.

Direct Examination

Direct test alludes back to the way of an observer being pondered through the lawful expert who known as her or him to the stand. Since the lawful expert who known as you to the stand needs you to offer appropriate declaration, any inquiries which may be mentioned are for the intention of inspiring data roughly the case. In various expressions, the legitimate proficient poses those inquiries that will help you offer verification. The primary guideline for giving direct declaration (or any sworn declaration)

is to constantly advise the reality. Witnesses should now presently don't be reluctant to make reference to "I don't perceive" or "I don't remember" while that is the reality. Telling the fact of the matter is basic to providing data to the case, and neglecting to illuminate the fact of the matter is an outrageous check. Lying beneath pledge is an evildoer offense known as prevarication, and it can achieve detainment and fines being forced on you.

Notwithstanding this most extreme crucial and central detail of being an observer, there are some of fine practices for authenticating in court agenda. Recall that the jury will inspect the believability of each observe and decide if to concur with the declaration essentially dependent on that appraisal.

Here are a couple of ways to deal with enhance your validity as an observer:

- Be on schedule or scarcely right on time for court agenda. Although we referenced this and the accompanying variable inside side the past section, going to court agenda early allows you an opportunity to assemble and investigate the configuration of the court agenda, the course you'll walk around of your seat inside side the court agenda to the testimony box, etc. Showing up past due has a horrendous effect at the jury and diminishes out of your validity.
- Dress expertly. Appearance does check, and your validity could be more beneficial through traditionalist endeavor clothing.
- Don't seem like stressed. Juries accept people to act stressed while they're relying. You may not be fit for control the manner in which you experience, notwithstanding with practice you may control any seen signs of apprehension, comprehensive of dull motions.
- Keep a fabulous stance. Juries will contemplate somebody's edge language while drawing closer, leaving, or sitting inside side the observer compartment. Standing and sitting up immediately convey certainty, while slumping can appear as aleven however you're awkward and are trying to camouflage something. In spite of the fact that you should be agreeable at the stand, don't disregard about what your mother exhorted you roughly sitting up quickly.
- Remain quiet and don't get angry. The contradicting lawful expert may endeavor to cause you to blow your top; doing as such will hurt your believability with the jury. Witnesses must not the slightest bit contend or be wry in response to a legitimate proficient's inquiries. Essentially, you should melody from showing antagonism nearer to the respondent, as this may cause it to have all the earmarks of being you have got a private timetable contrary to the person. Keeping quiet and supportive of fessional will work on the case.
- When significant, arrangement with "sure" or "no". Although this is going inseparably with our resulting factor, while noting a question to

the agreed or poor, you should ceaselessly utilize the expression "sure" or "no." On the stand, people regularly make the blunder of gesturing or shaking their head to answer, snorting arrangements, or the utilization of expressions comprehensive of uh-huh, that's right, no, or equivalent phrases. Whenever this happens, the lawful expert pondering you should precise you and let you know to answer with sure or no, that can get dreary and disturb one and all rapidly.

- Don't volunteer more measurements Answer the inquiries you're mentioned, notwithstanding don't offer additional insights or veer off the topic. Try not to offer talk confirmation (what various people expressed to you), as it's normally unacceptable.
- Avoid making absolutes for your assertions Making an outright statement comprehensive of "I constantly ..." or "I not the slightest bit ..." can make an unfriendly situation in later cross-test, which can be utilized to show you wrong. All things considered, practically zero is total. In any event, articulating "the sunlight based consistently sparkles inside side the sky" is wrong while you remember shrouds and evening time.
- Don't talk the case with each body be that as it may the legitimate proficient When going to court agenda as an observer, you can invest little energy inside side the genuine court docket. You'll ordinarily be restricted from coming into the court agenda till being known as, and suspensions and breaks will allow you to withdraw court agenda for a period. During those minutes, you'll be revealed to other people who can likewise moreover affirm; victims and respondents for a situation; and presumably even the media. Since you probably will not perceive who limit of those people are, you should not the slightest bit talk the case with each body. Doing as such can corrupt the declaration of others or offer tricky insights to the erroneous people.
- Consider the question mindfully sooner than you arrangement Be positive you perceive the inquiry, and on the off chance that you don't, request that the legitimate proficient duplicate it. Try not to start replying till you're positive that the legitimate proficient is finished asking the question.
- Speak certainly and hopefully An amazing observer doesn't yell, nonetheless talks noisily adequate to be heard through the choose, jury, and lawful professionals. Testimony as an evidentiary observer should be obliged to "just the data, ma'am, basically the data." Don't give assessment or hypothesis; in an autonomous, objective way, genuinely illuminate what you most likely did or found.
- If the choose or lawful expert beginnings off evolved to talk, forestall speaking When you're authenticating, legitimate experts or the choose can likewise moreover add to achieve a higher aptitude of a chose factor, or keep you from uncovering measurements this is inadmissible. When the two of them talks, immediately forestall your declaration and concentrate to what exactly they're articulating.

- Avoid retaining arrangements Although it's imperative which you assessment the notes and totally perceive particulars of your declaration ahead of time, preparing answers for anticipated inquiries could cause your declaration to appear to be prearranged and questionable.
- Remain free and convey to the data Remember that as an observer, you're offering data of the case. Never misrepresent, not the slightest bit surmise, and not the slightest bit oversee answers for a lawful expert's inquiry to favor one feature or the other option. Basically advise the truth, regardless of whose feature the arrangement can likewise also advantage.

Cross-Examination

Cross-test is the way of providing the restricting aspect in an adversity the likelihood to reprimand an observer. In any preliminary, the indictment has the legitimate to denounce observers known as through the insurance, and security has the appropriate to reprimand observers known as through the arraignment. It is the movement of the cross-assessing lawful expert to dishonor the restricting aspect's observer. Lawyers can likewise also utilize mental methodologies to attempt to ruin witnesses. When authenticating, be careful now no longer to fall into their snares. Be coordinated for and outfitted to avoid such cross-test strategies as:

- Rapid-hearthplace inquiries with out a chance to answer among questions
- Leading questions ("Isn't it bona fide that what you saw changed into ...?")
- Repeating your expressions with a bend that changes their which implies
- Pretending to be wonderful, then, at that point turning contrary to you at the same time
- Feigning bewilderment, shock, or shock at what you've expressed

Prolonged quietness intended to reason torment in trusts you'll say extra The greatest indispensable part with an end goal to remember while exposed to those methods is this: Don't think about the lawful expert's techniques literally; she or he is basically doing a movement. Our suggestion to the observer is to just do your action; keep up with your cool and country the data.

You can utilize some of clues to adapt to a lawful expert's strategies eventually of cross-test. Attorneys will oftentimes attempt to profit a rhythm to their inquiries, starting through posing inquiries with some time among them, after which shortening the time among inquiries till they're being shot in a word succession. This limits the time you need to consider an arrangement, and it will expand the chance of being stuck in a snare. Numerous occurrences, a question could be mentioned one way, after

which mentioned an uncommon way later. In the event that you convert your answer, the lawful expert will utilize this to ruin your declaration. A simple way to stop those quick hearthplace questions is to pressure a delay sooner than replying. By unobtrusively tapping your foot 3 occurrences sooner than giving an arrangement, you supply your self one moment to assume, and furthermore you control the rhythm of the inquiries and arrangements being given. Since you're sitting in an encased observer holder, it's not possible for anyone to see you discretely tapping your foot and stopping the legitimate proficient's endeavor at quick hearthplace pondering.

Consistently concentrate to the inquiries being mentioned, and be equipped to answer. A legitimate proficient can likewise furthermore ask a question, anticipate an arrangement, after which rehash what you've expressed in any case turn the expressions. Doing as such can exaltate the which method for your assertion and might turn what you've expressed to the lawful expert's like. In the event that the lawful expert rehashes it as an inquiry (comprehensive of through beginning with "Along these lines, you're articulating that ...") and furthermore you're currently done paying interest, you can in actuality consider something you not the slightest bit expressed. Never be reluctant to make reference to, "That is presently no longer what I expressed" in those conditions, and emphasize your previous presentation.

Another not unusualplace strategy is to start pondering you with variables of settlement. In doing as such, the legitimate proficient taking part in the cross-test appears to be wonderful and brings the observer's ensure down. The witness will normally be additional agreeable, and the lawful expert can then both destroy going before proclamations through asking notice up inquiries, or pose fundamental inquiries which can reason the observer to offer expressions so one can be great to the restricting aspect's capacity. Regularly, when your secure is down, the lawful expert will flip from being lovely to at the same time assaulting what you've expressed or transforming into confrontational. This can befuddle you and withdraw you feeling a touch double-crossed the essential time it occurs, and it allows the lawful expert to take the lead hand in pondering you. Other mental ploys can contain articulating almost no or nothing in any regard. Whenever you've finished replying, the legitimate proficient can likewise also delay asking the resulting question, settling on as a choice to stop for an extended period. Since the all-inclusive quiet might be awkward, the observer can likewise furthermore encounter that she or he should say extra. If nothing is added, the legitimate proficient will subvert your input through articulating, "Goodness, I'm grieved, would you say you are done?" A considerable lot of the strategies legitimate experts use are done sooner or later of the preliminary way, comprehensive of while an observer is being affirmed as a professional. When troublesome an observer, the lawful expert will request an arrangement from requests to test data of the observer's capabilities and look at their phase of ability. In trendy, the troublesome festival is given a sensibly detached rule inside side the inquiries mentioned roughly somebody's qualifications, and judges and legitimate experts calling you can allow a line of pondering to

keep up with till it appears to be the observer is in effect unreasonably assaulted. How crime suggest undermines the observer's power will go, as lawyers have phenomenal sorts of cross-assessing observers. One method this is utilized to different reaches is to check your qualifications, after which subvert them through rehashing data in a mean manner of speaking. For example, if a pc expert moved on from network school, the legitimate proficient may rehash the call of the school in a snide tone, after which ask, In this fashion, you not the slightest bit visited a college?" equally, inside the event that you {simply|that you just} simply had a CompTIA confirmation, the lawful knowledgeable might rehash "CompTIA?" as on the off likelihood that you simply} just had been creating it up. it's a simple strategy that issues nearly no mastery around a haul.

Top of Form

They can likewise furthermore phony to be an ardent advocate of equity, or an individual who truly cares and accepts of their benefactor's honesty. Albeit this could be credible of a couple of court agenda authorities, actually lawyers will watch clients regardless of whether they're liable or innocuous. In spite of this, they'll utilize a strategy of professing to be ethically offended, confused, or paralyzed through an announcement. Since lawyers likewise are ordinarily horrendous entertainers, this might be extra upsetting than startling while it takes place. The endeavor is made to play into the arms of the jury, and show up reasonable through showing up terrible.

Refusing to Answer

While filling in as an expert observer, you is presumably mentioned an inquiry that you do now presently don't have to answer. A lawful expert can likewise moreover ask an inquiry this is humiliating to you, or which you situate irrelevant to the case. In such conditions, you may find out if you're needed to answer the question. On the off chance that the choose agrees that the inquiry isn't material to the situation or imperative to answer, the person can have the option to help you currently no longer to answer on the off chance that you would prefer not to. On the off chance that the choose educates you to answer the question, in any case, you haven't any genuine inclination in any case to go along, or danger being referenced with hatred of court agenda.

Another situation wherein you can decline to answer is at the same time may reason you to concede to illegal. Under the fifth Amendment of the U.S. Constitution, and underneath the wellbeing of the Charter of Rights and Freedoms in Canada, you do now presently don't have any desire to affirm in the event that your declaration will implicate you. This is because of the reality through replying in a way that isn't implicating, you're essentially constrained to commit prevarication.

Utilizing Notes and Visual Aids

What in the event that you're needed to affirm as an observer, nonetheless your memory isn't so phenomenal? What in the event that you're terrified

of failing to remember essential data, especially measurements that is hard to remember, comprehensive of numbers? Is it crime for you as an observer to take notes with you to apply as a kind of perspective while validating?

Police authorities and various observers use notes as a memory asset sooner or later of court agenda declaration the entirety of the time. There are endowments and disadvantages in doing as such. A few hearers is likely propelled through the truth which you're concentrating from notes, because of the reality they could concur with the composed expression extra than a predicated on individual memory all alone. On the elective hand, others may assume you're being trained or welcomed on in the event that you check with notes; they concur with that if what you're articulating is the truth, you will remember it with out notes.

An essential consideration in seeing if or not to apply notes is the truth that if a mind ness does as such, the notes could be gone into confirmation and brought into the care of the court agenda during the preliminary. In the event that you do choose to apply notes, thusly, guarantee that the wallet or paper on which they're composed doesn't create different notes that check with subjects now not, at this point related with the case, because of the reality the restricting legitimate proficient can question you around something inside side the notes.

Visual guides are some other not surprising spot detail, especially in examples that contain verification comprehensive of virtual previews, or require guides of a place. When identifying with apparent guides, comprehensive of pictures or graphs, be just about as engaging as possible. Maybe than hoisting your hand and articulating, "Here we see," you should endeavor to acknowledgment the eye on the thing you're talking roughly, comprehensive of through articulating "In the lessening legitimate hand corner." Not best does this make it less hard for the ones looking your declaration to perceive what you're talking around, be that as it may it also makes it less hard to perceive inside side the record of the declaration.

Testifying As an Expert Witness

- A court agenda is in which a hardship takes locale, and it incorporates a choose's seat, testimony box, court agenda columnist's table, court agenda representative's table, jury holder, platform, and tables for the indictment and assurance. A bar (that is a railing) is utilized to part the exhibition in which observers sit down from the appropriately of the court agenda.
- Technology in courts can run, so you should get mindful of what framework is to be had and regardless of whether you might need to offer any arrangement of your own personal to show uncovers.
- A summon is a crime record this is given through the court agenda to advise you which you are needed to stand by court agenda on a rigid date and time to offer evidence as an observer.

- Being sworn in calls for which you area your hand on a Bible and vow to God which you'll advise the truth for your declaration, while advancing earnestly involves a guarantee which you'll illuminate the truth.
- Depositions are a way of pondering observers past to an adversity, and are utilized inside side the pretrial scopes of each polite and law breaker occasions.
- Courtroom decorum should consistently be followed, comprehensive of treating one and all inside side the court agenda with appreciate and identifying with the choose as "your honor."
- Direct test alludes back to the way of an observer being pondered through the lawful expert who known as her or him to the stand.
- Cross-test is the subsequent one line of pondering an observer faces, wherein the contradicting feature in a hardship or paying attention to has the likelihood to welcome inquiries.
- Once an observer is cross-tried, the lawful expert who known as the observer has the likelihood to divert, and ask furthermore questions. The contradicting lawful expert can then recross, and moreover pose additional inquiries.
- Witnesses aren't needed to answer an inquiry underneath promise if doing as such will implicate them. In the event that this doesn't follow, and the observer in any case doesn't have to answer, she or he should ask the choose if answer the question, after which stand through the choose's choice.
- Notes which may be utilized as reference texture while bearing witness to beneath promise are gone into confirmation.

10.4 SUMMARY

Mobile Forensics Summary

In this liquidation we discovered the resulting:

- Mobile Forensics is a branch of Digital Forensics. It is set the buy and assessment of cell contraptions to improve virtual verification for measurable examination.
- Android is an open stockpile working gadget fundamentally dependent on Linux Kernel progressed through Google for cell contraptions.
- Rooting Android opens its center module to a shopper, which permits get passage to the covered areas of the instrument.
- ADB is an order line gadget that permits us to join an Android instrument to a pc have gadget through a USB link. It is an absolutely adaptable gadget since it allows a shopper to do various obligations

comprehensive of introducing, investigating, and disposing of applications, and so forth

- Joint investigate movement association or JTAG is a convoluted data extraction procedure used in cell criminology. JTAG offers an interface through which a pc can talk immediately with the chipboard. It involves associating the verification cell device's Test Access Port (TAP) to a JTAG emulator to get passage to uncooked data.
- Chip-Off involves disposing of the memory chip of the cell device and plant it onto a chose equipment for data securing and perusing its substance.
- Micro-look at test involves the utilization of an extreme controlled electron magnifying lens to analyze yield on the entryway stage. The apparatus memory chip is shaved in exceptionally thin layers, and after that the data is inspect gradually from the stockpile the utilization of an electron magnifying lens or diverse device.
- iOS is a cell working gadget made and progressed through Apple Inc. that as of now controls among the business undertaking's cell contraptions, comprehensive of iPhone, iPad, and iPod Touch. • There are 3 unprecedented modes for the boot strategies for iOS contraptions: Normal boot way, Recovery mode, and DFU mode
- iOS jailbreaking is valuable for the thought process of disposing of programming program guidelines forced through Apple on iOS using an arrangement of portion patches. Jailbreaking grants root get passage to iOS.
- All Apple cell devices utilize the HFSX record gadget.
- Logically, iPhone has dividers. One is for putting away the iOS exact archives, liable for stacking the functioning gadget comprehensive of part depictions and arrangement reports. The diverse parcel is utilized for the carport of buyer exact settings and bundles comprehensive of films, music, photographs, contacts, and extra.

Investigated reports Summary

The fragment on explored surveys covers:

Why a researched archive is required.

Report characterizations and specs.

What is assessment and it's anything but a criminological report.

How to expressly state a measurable insightful archive in what should involve.

The capacities of a stupendous archive.

The thought process of an insightful report is to talk the results of the test. It permits the introduction of verification as declaration and helps withinside the statement of expert assessment.

Mobile Forensics, Reports of Investigation, Become a Professional Witness

Understanding the Expert Witness Summary

- Witnesses are people who've firsthand skill of illegal or episode, or who give verification sooner or later of an affliction, court, or paying attention to.
- An evidentiary observer can best affirm as to data (what she or he saw or heard) and can not supply surveys or reach determinations.
- A proficient observer can likewise also don't have any immediate association withinside the case, notwithstanding has exceptional specialized mastery or ability that qualifies her or him to offer master surveys on specialized subjects.
- To qualify as an expert observer, the observer could have their accreditations surveyed through the court agenda, and went into the record in the wake of being confirmed. On the off chance that the contradicting feature needs to project, the observer is cross-tried. The choose assesses the insights got through this way, and may then capture or reject the observer as an expert in a chose region.
- A request great purchase is a settlement wherein the respondent argues dependable to a lesser wrongdoing to have additional outrageous costs dropped.
- A educational plan vitae is a record that traces somebody's preparation, appreciate, and various certifications. It is an indepth outline of the capabilities that make you an expert in a chose region.
- Criminal case proficient observers are utilized to help withinside the arraignment and assurance of individuals stressed in illegal.
- Civil case proficient observers are utilized to help in common court agenda cases in which one man or lady and additionally undertaking suits to cure a debate and recover what they experience is owed them.
- Computer legal experts collect and study limit evidence sooner or later of an exploration, comprehensive of data that has been erased, encoded, or broken.
- Medical and mental experts separately offer discernment and help in real and scholarly issues that can be concerned in a court agenda case. They can be used by both aspect in a court agenda case to do evaluations, analyze present analyses, or affirm around specialized data related with confirmation.
- Construction and design experts can offer insight and help in issues concerning genuine property, building and hearthplace codes, botches underway and format, and various issues concerning homes.

- Technical declaration is explanations given beneath pledge that blessing data of a specialized sort
- Whether somebody might be recognized as an expert observer, and the suitability of confirmation, are each governed through the lawful rules of the court agenda's ward (i.e., nation or federal). These guidelines are finished rule and are commonly arranged directly into a record named Rules of Evidence.
- Under Rules of Evidence, confirmation offered in court agenda should be validated, which implies that an observer should vouch for its realness.
- If verification isn't constantly amassed and treated with regards to the right prerequisites, the choose can likewise moreover consider the confirmation unacceptable while it's far advertised. This can be basically founded absolutely on a development to stifle from the restricting lawful expert all together that members of the jury will not the slightest bit get a danger to survey it or remember it in making their determination.

10.5 REFERENCE FOR IN ADDITION STUDYING

1. Practical Cyber Forensics_An Incident primarily based totally Approach to Forensic Investigation,Niranjan Reddy, Apress Publisher,2019.
2. The authentic CHFI Exam 312-forty nine observe Guide, Dave Kleiman, SYNGRESS Publisher, 2007.
3. Digital Forensics and Incident Response, Gerard Johansen, Packt Publishing,2020.
4. EC-Council CHFIv10 Study Guide, EC-Council Publisher, 2018.
- 5.https://www.researchgate.internet/guide/258726589_iPhone_forensics_a_practical_overview_with_certain_commercial_software/
- 6.https://www.researchgate.internet/guide/281100878_An_Open_Source_Toolkit_for_iOS_Filesystem_Forensics/
- 7.https://www.researchgate.internet/guide/258726387_iPhone_forensics_based_on_Macintosh_open_source_and_freeware_tools/
- 8.https://www.researchgate.internet/guide/261454188_A_Novel_Method_of_iDevice_iPhone_iPad_iPod_Forensics_without_Jailbreaking/
9. <https://developer.android.com/schooling/articles/protection-tips/>
- 10.<http://www.binaryintel.com/offerings/jtag-chip-off-forensics/jtag-forensics/http://www.binaryintel.com/offerings/jtag-chip-off-forensics/jtag-forensics/>

11. Boni, William, and Gerald L. Kovacich. *Netspionage: The Global Threat to Information* (Butterworth-Heinemann: 2000).
12. CSI, the Computer Security Institute; <http://www.gocsi.com/www.gocsi.com/>.
13. Mokhiber, Russell, and Robert Weissman. "Corporate Spooks." March 6, 2001; www.commondreams.org/views01/0306-03.htm (accessed August 2, 2007).

10.6 FREQUENTLY ASKED QUESTIONS

The accompanying Frequently Asked Questions, answered through the writers of this book, are intended to every degree your ability of the Exam Objectives offered on this insolvency, and to assist you with real ways of life execution of those ideas.

Q: I'm an observer in a hooligan case, and highlight established that a mate of mine has been referred to as a hearer to the equivalent case. What must I do?

A: Tell your buddy to tell the court agenda that she or he knows about one of the observers. During the jury decision way, legal hearers are mentioned if there's any purpose(s) that should save you them from being an attendant. This might need to comprise of understanding the respondent, being concerned withinside the exploration, getting observers, or various issues that may affect the eventual outcomes of the preliminary. By having a seeking to one of the observers, somebody will be dispatched from jury obligation.

Q: I'm a piece of an episode response gathering, and I really have end up stressed in an inci-mark so one can more then likely visit court docket. Who would i be able to convey to roughly this?

A: Although you can impart conventionally around the case to each body, you should endeavor to avoid having any discussions roughly it with each body who isn't connected to the situation. In various expressions, despite the fact that you may impart to the legitimate proficient in cost of the case, you shouldn't convey to amigos, far and wide others, or collaborators around the points of interest of the case. By telling an individual who isn't concerned, there might be a danger this insights will be surpassed straightforwardly to other people, comprehensive of members of the media. Moreover, you can accidentally convey to a mindful individual of or is related with the respondent, or can be a limit member of the jury.

Q: How would I perceive while and in which I'm claimed to affirm for a situation?

A: When you're brought to be an observer, you'll be presented with a summon through an official of the court docket. The summon has measurements at the spot of the preliminary, and while you're to stand by court agenda to affirm. Except if the lawful expert who has known as you

shows in some other case, you might need to stand by the town hall every day that the preliminary keeps up with in the event that you're re-known regarding the stand.

Q: My non mainstream beliefs restrict me from the activity of setting my hand at the Bible and committing to God that I'll illuminate the reality. When being known as to affirm, how should I respond?

A: When you're known regarding the stand, you have got the decision of swearing or advancing. When sworn in, you may safeguard your hand on a Bible and vow to God which you'll advise the truth. Certifying doesn't need this. When being attested, you earnestly guarantee that any declaration you supply could be reliable.

Q: Why is it essential that every one the product program used by guideline implementation authorities be ensured and enrolled? Law requirement spending plans are oftentimes close; why now presently don't utilize freeware as parcels as plausible?

A: Some freeware and shareware hardware which may be to be had at the Internet are appropriate gear, and the rate is in all actuality legitimate. Be that as it may, there are a couple of dangers in the utilization of those applications for legal capacities. To begin with, you not the slightest bit perceive unequivocally the thing you're getting while you down load a free programming (and furthermore you in actuality can't ask to your money lower back on the off chance that it doesn't compositions well). Downloads might be kindled with infections or Trojans that could hurt the constructions on that you use them. Utilizing unlicensed programming program (unlawful duplicates) is even worse. The contradicting lawful professional(s) could have a region day if they discover that the police utilized pilfered or "acquired" programming program withinside the research. This direct can crush the validity of the people who did the criminological test or in any event, achieve dropping the case. Moreover, with very much purchased and enrolled programming program, you'll be fit for get specialized help from the vender if significant. Producers of pc scientific programming program as often as possible give decreases to guideline authorization organizations, making it less hard to have sufficient cash the right gear for the action. All things considered, authorities and organizations probably wouldn't propose setting aside money through looking for their duty weapons from a second hand store; that is because of the reality those are basic gear of the substitute and should be pretty much as trustworthy as attainable. For the cybercrime agent or expert, the equivalent is true of the criminological programming program this is utilized to procure and keep evidence that could make or harm a law breaker case.

Q: On my announcement, I composed an off-base date and didn't perceive my misstep till after the affirmation changed into despatched to the examiner. Presently I've been summoned to affirm roughly the information. What must I do?

A: Notify the specialist and examiner immediately around the mistake sooner than any statements and sooner than the preliminary beginnings off evolved. By being genuine and expressing the mistake early, you may avoid any inconsequential inquiries eventually of the preliminary around irregularities withinside the insights you've advertised.

Q: Why is documentation so essential? Doesn't simply the verification impart?

A: In numerous pc-related evildoer examples, the verification communicates in a language that limit of the members of the jury (and regularly the choose, investigator, and guideline implementation authorities) don't perceive. At one time, juries had been likely to just acknowledge the declaration of expert observers with out inquiry, nonetheless as the overall population has end up extra actually best in class and expert declaration has been known as into question in exorbitant profile occurrences comprehensive of the O. J. Simpson case, juries have end up extra distrustful of experts' faultlessness and are considerably more liable to just acknowledge the restricting legitimate proficient's requesting circumstances which lift questions around confirmation handling procedures and scientific strategies. This is the design record the developments of guideline implementation authorities and specialists each progression of the way. Documentation is similarly fundamental to invigorate the memories of people who should affirm withinside the case. Frequently, preliminaries are delayed for quite a long time or possibly years, and by the point an official or specialist is expected to stand up, she or he has treated various occurrences.

