UNIT I

1

INTRODUCTION

Unit Structure

1.1 WHAT IS COMPUTER FORENSICS?

- Computer forensics is the process of methodically examining computer media (hard disks, diskettes, tapes, etc.) for evidence. In other words, computer forensics is the collection, preservation, analysis, and presentation of computer-related evidence.

- Computer forensics also referred to as computer forensic analysis, electronic discovery, electronic evidence discovery, digital discovery, data recovery, data discovery, computer analysis, and computer examination.

- Computer evidence can be useful in criminal cases, civil disputes, and human resources/ employment proceedings.

1.2 USE OF COMPUTER FORENSICS IN LAW ENFORCEMENT

Computer forensics assists in Law Enforcement. This can include:

- Recovering deleted files such as documents, graphics, and photos.
- Searching unallocated space on the hard drive, places where an abundance of data often resides.
- Tracing artifacts, those tidbits of data left behind by the operating system. Our experts know how to find these artifacts and, more importantly, they know how to evaluate the value of the information they find.
- Processing hidden files — files that are not visible or accessible to the user — that contain past usage information. Often, this process requires reconstructing and analyzing the date codes for each file and determining when each file was created, last modified, last accessed and when deleted.
- Running a string-search for e-mail, when no e-mail client is obvious.

1.3 COMPUTER FORENSICS ASSISTANCE TO HUMAN RESOURCES/EMPLOYMENT PROCEEDINGS

Computers can contain evidence in many types of human resources proceedings, including sexual harassment suits, allegations of discrimination, and wrongful termination claims. Evidence can be found in electronic mail systems, on network servers, and on individual employee's computers.

Employer Safeguard Program:

Employers must safeguard critical business information. An unfortunate concern today is the possibility that data could be damaged, destroyed, or misappropriated by a discontented individual. Before an individual is informed of their termination, a computer forensic specialist should come on-site and create an exact duplicate of the data on the individual's computer. In this way, should the employee choose to do anything to that data before leaving, the employer is protected. Damaged or deleted data can be re-placed, and evidence can be recovered to show what occurred. This method can also be used to bolster an employer's case by showing the removal of proprietary information or to protect the employer from false charges made by the employee. You should be equipped to find and interpret the clues that have been left behind. This includes situations where files have been deleted, disks have been reformatted, or other steps have been taken to conceal or destroy the evidence. For example, did you know?

- What Web sites have been visited?

- What files have been downloaded?
- When files were last accessed?
- Of attempts to conceal or destroy evidence?
- Of attempts to fabricate evidence?
- That the electronic copy of a document can contain text that was removed from the final printed version?
- That some fax machines can contain exact duplicates of the last several hundred pages received?
- That faxes sent or received via computer may remain on the computer indefinitely?
- That email is rapidly becoming the communications medium of choice for businesses?
- That people tend to write things in email that they would never consider writing in a memorandum or letter?
- That email has been used successfully in criminal cases as well as in civil litigation?
- That email is often backed up on tapes that are generally kept for months or years?
- That many people keep their financial records, including investments, on computers?

1.4 COMPUTER FORENSICS SERVICES

Computer forensics professionals should be able to successfully perform complex evidence recovery procedures with the skill and expertise that lends credibility to your case.

For example, they should be able to perform the following services:

1. Data Seizure:

- Following federal guidelines, computer forensics experts should act as the representative, using their knowledge of data storage technologies to track down evidence.
- The experts should also be able to assist officials during the equipment seizure process.

2. Data Duplication/Preservation:

- When one party must seize data from another, two concerns must be addressed:

- the data must not be altered in any way
- the seizure must not put an undue burden on the responding party

- The computer forensics experts should acknowledge both of these concerns by making an exact duplicate of the needed data.
- When experts work on the duplicate data, the integrity of the original is maintained.

3. Data Recovery:

- Using proprietary tools, your computer forensics experts should be able to safely recover and analyze otherwise inaccessible evidence.
- The ability to recover lost evidence is made possible by the expert's advanced understanding of storage technologies.

4. Document Searches:

- Computer forensics experts should also be able to search over 200,000 electronic documents in seconds rather than hours.
- The speed and efficiency of these searches make the discovery process less complicated and less intrusive to all parties involved.

5. Media Conversion:

- Computer forensics experts should extract the relevant data from old and un-readable devices, convert it into readable formats, and place it onto new storage media for analysis.

6. Expert Witness Services:

- Computer forensics experts should be able to explain complex technical processes in an easy-to- understand fashion.
- This should help judges and juries comprehend how computer evidence is found, what it consists of, and how it is relevant to a specific situation.

7. Computer Evidence Service Options:

Computer forensics experts should offer various levels of service, each designed to suit your individual investigative needs. For example, they should be able to offer the following services:

- **Standard service:** Computer forensics experts should be able to work on your case during nor-mal business hours until your critical electronic evidence is found.
- **On-site service:** Computer forensics experts should be able to travel to your location to per-form complete computer evidence services. While on-site, the experts should quickly be able to produce exact

duplicates of the data storage media in question.

- **Emergency service:** Your computer forensics experts should be able to give your case the highest priority in their laboratories. They should be able to work on it without interruption until your evidence objectives are met.

- **Priority service:** Dedicated computer forensics experts should be able to work on your case during normal business hours (8:00 A.M. to 5:00 P.M., Monday through Friday) until the evidence is found. Priority service typically cuts your turnaround time in half.

- **Weekend service:** Computer forensics experts should be able to work from 8:00 A.M. to 5:00 P.M., Saturday and Sunday, to locate the needed electronic evidence and will continue 14 Computer Forensics, Second Edition working on your case until your evidence objectives are met.

8. Other Miscellaneous Services:

Computer forensics experts should also be able to provide extended services. These services include:

- Analysis of computers and data in criminal investigations
- On-site seizure of computer data in criminal investigations
- Analysis of computers and data in civil litigation.
- On-site seizure of computer data in civil litigation
- Analysis of company computers to determine employee activity
- Assistance in preparing electronic discovery requests
- Reporting in a comprehensive and readily understandable manner
- Court-recognized computer expert witness testimony
- Computer forensics on both PC and Mac platforms
- Fast turnaround time.

1.5 BENEFITS OF PROFESSIONAL FORENSIC METHODOLOGY

A knowledgeable computer forensics professional should ensure that a subject computer system is carefully handled to ensure that:

1. No possible evidence is damaged, destroyed, or otherwise compromised by the procedures used to investigate the computer.
2. No possible computer virus is introduced to a subject computer during the analysis process.

3. Extracted and possibly relevant evidence is properly handled and protected from later mechanical or electromagnetic damage.
4. A continuing chain of custody is established and maintained.
5. Business operations are affected for a limited amount of time, if at all.
6. Any client-attorney information that is inadvertently acquired during a forensic exploration is ethically and legally respected and not divulged.

1.6 STEPS TAKEN BY COMPUTER FORENSICS SPECIALISTS

The computer forensics specialist should take several careful steps to identify and attempt to retrieve possible evidence that may exist on a subject's computer system. For example, the following steps should be taken:

1. **Protect** the subject computer system during the forensic examination from any possible alteration, damage, data corruption, or virus introduction.
2. **Discover** all files on the subject system. This includes existing normal files, deleted yet remaining files, hidden files, password-protected files, and encrypted files.
3. **Recover** all of discovered deleted files.
4. **Reveal** the contents of hidden files as well as temporary or swap files used by both the application programs and the operating system.
5. **Access** the contents of protected or encrypted files.
6. **Analyze** all possibly relevant data found in special areas of a disk. This includes but is not limited to what is called unallocated space on a disk, as well as slack space in a file (the remnant area at the end of a file in the last assigned disk cluster, that is unused by current file data, but once again, may be a possible site for previously created and relevant evidence).
7. **Print** out an overall analysis of the subject computer system, as well as a listing of all possibly relevant files and discovered file data.
8. **Provide** an opinion of the system layout; the file structures discovered; any discovered data and authorship information; any attempts to hide, delete, protect, and encrypt information; and anything else that has been discovered and appears to be relevant to the overall computer system examination.
9. **Provide** expert consultation and/or testimony, as required.

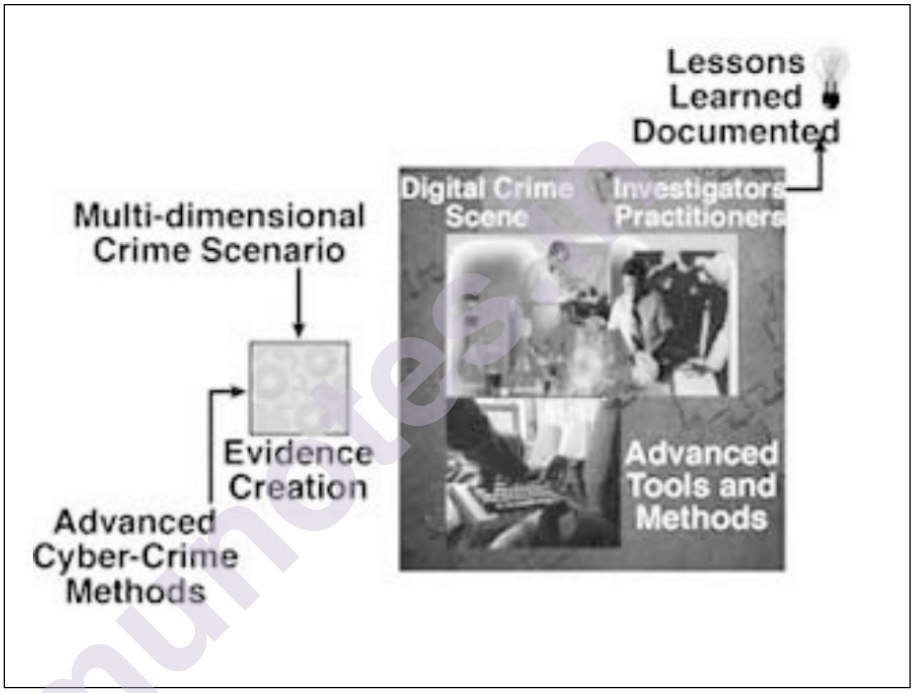
1.7 TYPES OF MILITARY COMPUTER FORENSIC TECHNOLOGY

- Key objectives of cyber forensics include rapid discovery of evidence, estimation of potential impact of the malicious activity on the victim, and assessment of the intent and identity of the perpetrator.
- Real-time tracking of potentially malicious activity is especially difficult when the pertinent information has been intentionally hidden, destroyed, or modified in order to elude discovery.
- National Law Enforcement and Corrections Technology Center (NLECTC) works with criminal justice professionals to identify urgent and emerging technology needs.
- NLECTC centers demonstrate new technologies, test commercially available technologies and publish results — linking research and practice.
- National Institute of Justice (NIJ) sponsors research and development or identifies best practices to address those needs.
- The information directorate entered into a partnership with the NIJ via the auspices of the NLECTC, to test the new ideas and prototype tools. The Computer Forensics Experiment 2000 (CFX-2000) resulted from this partnership.

Computer Forensic Experiment-2000 (Cfx-2000):

- CFX-2000 is an integrated forensic analysis framework.
- The central hypothesis of CFX-2000 is that it is possible to accurately determine the motives, intent, targets, sophistication, identity, and location of cyber criminals and cyber terrorists by deploying an integrated forensic analysis framework.
- The cyber forensic tools involved in CFX-2000 consisted of commercial off-the-shelf software and directorate-sponsored R&D prototypes. CFX includes SI-FI integration environment.
- The Synthesizing Information from Forensic Investigations (SI-FI) integration environment supports the collection, examination, and analysis processes employed during a cyber-forensic investigation.
- The SI-FI prototype uses digital evidence bags (DEBs), which are secure and tamperproof containers used to store digital evidence.
- Investigators can seal evidence in the DEBs and use the SI-FI implementation to collaborate on complex investigations.
- Authorized users can securely reopen the DEBs for examination, while automatic audit of all actions ensures the continued integrity of their contents.

- The teams used other forensic tools and prototypes to collect and analyze specific features of the digital evidence, perform case management and time lining of digital events, automate event link analysis, and perform steganography detection.
- The results of CFX-2000 verified that the hypothesis was largely correct and that it is possible to ascertain the intent and identity of cyber criminals.
- As electronic technology continues its explosive growth, researchers need to continue vigorous R&D of cyber forensic technology in preparation for the onslaught of cyber reconnaissance probes and attacks.



1.8 TYPES OF LAW ENFORCEMENT COMPUTER FORENSIC TECHNOLOGY

Computer forensics tools and techniques have become important resources for use in internal investigations, civil lawsuits, and computer security risk management. Law enforcement and military agencies have been involved in processing computer evidence for years.

Computer Evidence Processing Procedures:

Processing procedures and methodologies should conform to federal computer evidence processing standards.

1. Preservation of Evidence:

- Computer evidence is fragile and susceptible to alteration or erasure by any number of occurrences.

- Computer evidence can be useful in criminal cases, civil disputes, and human resources/ employment proceedings.
- Black box computer forensics software tools are good for some basic investigation tasks, but they do not offer a full computer forensics solution.
- SafeBack software overcomes some of the evidence weaknesses inherent in black box computer forensics approaches.
- SafeBack technology has become a worldwide standard in making mirror image backups since 1990.

Trojan Horse Programs:

- The computer forensic expert should be able to demonstrate his or her ability to avoid destructive programs and traps that can be planted by computer users bent on destroying data and evidence.
- Such programs can also be used to covertly capture sensitive information, passwords, and network logons.

Computer Forensics Documentation:

- Without proper documentation, it is difficult to present findings.
- If the security or audit findings become the object of a lawsuit or a criminal investigation, then documentation becomes even more important.

File Slack:

- Slack space in a file is the remnant area at the end of a file in the last assigned disk cluster, that is unused by current file data, but once again, may be a possible site for previously created and relevant evidence.
- Techniques and automated tools that are used by the experts to capture and evaluate file slack.

Data-Hiding Techniques:

- Trade secret information and other sensitive data can easily be secreted using any number of techniques. It is possible to hide diskettes within diskettes and to hide entire computer hard disk drive partitions. Computer forensic experts should understand such issues and tools that help in the identification of such anomalies.

E-Commerce Investigations:

- Net Threat Analyzer can be used to identify past Internet browsing and email activity done through specific computers. The software analyzes a computer's disk drives and other storage areas that are generally unknown to or beyond the reach of most general computer

users. Net Threat Analyzer avail-able free of charge to computer crime specialists, school officials, and police.

Dual-Purpose Programs:

- Programs can be designed to perform multiple processes and tasks at the same time. Computer forensics experts must have hands-on experience with these programs.

Text Search Techniques:

- Tools that can be used to find targeted strings of text in files, file slack, unallocated file space, and Windows swap files.

Fuzzy Logic Tools Used To Identify Unknown Text:

- Computer evidence searches require that the computer specialist know what is being searched for. Many times not all is known about what may be stored on a given computer system.
- In such cases, fuzzy logic tools can provide valuable leads as to how the subject computer was used.

2. Disk Structure:

- Computer forensic experts must understand how computer hard disks and floppy diskettes are structured and how computer evidence can reside at various levels within the structure of the disk.
- They should also demonstrate their knowledge of how to modify the structure and hide data in obscure places on floppy diskettes and hard disk drives.

3. Data Encryption:

- Computer forensic experts should become familiar with the use of software to crack security associated with the different file structures.

4. Matching a Diskette to a Computer:

- Specialized techniques and tools that make it possible to conclusively tie a diskette to a computer that was used to create or edit files stored on it. Computer forensic experts should become familiar how to use special software tools to complete this process.

5. Data Compression:

- Computer forensic experts should become familiar with how compression works and how compression programs can be used to hide and disguise sensitive data and also learn how password-protected compressed files can be broken.

6. Erased Files:

- Computer forensic experts should become familiar with how previously erased files can be recovered by using DOS programs and by manually using data-recovery technique & familiar with cluster chaining.

7. Internet Abuse Identification and Detection:

- Computer forensic experts should become familiar with how to use specialized software to identify how a targeted computer has been used on the Internet.
- This process will focus on computer forensics issues tied to data that the computer user probably doesn't realize exists (file slack, unallocated file space, and Windows swap files).

8. The Boot Process and Memory Resident Programs:

- Computer forensic experts should become familiar with how the operating system can be modified to change data and destroy data at the whim of the person who configured the system.
- Such a technique could be used to covertly capture keyboard activity from corporate executives, for example. For this reason, it is important that the experts understand these potential risks and how to identify them.

1.9 TYPES OF BUSINESS COMPUTER FORENSIC TECHNOLOGY

The following are different types of business computer forensics technology: -

Remote Monitoring of Target Computers:

- Data Interception by Remote Transmission (DIRT) is a powerful remote-control monitoring tool that allows stealth monitoring of all activity on one or more target computers simultaneously from a remote command center.
- No physical access is necessary. Application also allows agents to remotely seize and secure digital evidence prior to physically entering suspect premises.

CREATING TRACKABLE ELECTRONIC DOCUMENTS:

- Binary Audit Identification Transfer (BAIT) is a powerful intrusion detection tool that allows users to create trackable electronic documents.
- BAIT identifies (including their location) unauthorized intruders who access, download, and view these tagged documents.

- BAIT also allows security personnel to trace the chain of custody and chain of command of all who possess the stolen electronic documents.

THEFT RECOVERY SOFTWARE FOR LAPTOPS AND PCS:

What it really costs to replace a stolen computer:

- The price of the replacement hardware & software.
- The cost of recreating data, lost production time or instruction time, reporting and investigating the theft, filing police reports and insurance claims, increased insurance, processing and ordering replacements, cutting a check, and the like.
- The loss of customer goodwill.
- If a thief is ever caught, the cost of time involved in prosecution.

Pc Phonehome:

- PC PhoneHome is a software application that will track and locate a lost or stolen PC or laptop any-where in the world. It is easy to install. It is also completely transparent to the user.
- If your PC PhoneHome-protected computer is lost or stolen, all you need to do is make a report to the local police and call CD's 24-hour command center. CD's recovery specialists will assist local law enforcement in the recovery of your property.

FORENSIC SERVICES AVAILABLE:

Services include but are not limited to:

- Lost password and file recovery
- Location and retrieval of deleted and hidden files
- File and email decryption
- Email supervision and authentication
- Threatening email traced to source
- Identification of Internet activity
- Computer usage policy and supervision
- Remote PC and network monitoring
- Tracking and location of stolen electronic files
- Honeypot sting operations
- Location and identity of unauthorized software users
- Theft recovery software for laptops and PCs

- Investigative and security software creation
- Protection from hackers and viruses.

COMPUTER FORENSIC EVIDENCE & CAPTURE

1.10 DATA RECOVERY DEFINED

- Data recovery is the process in which highly trained engineers evaluate and extract data from damaged media and return it in an intact format.
- Many people, even computer experts, fail to recognize data recovery as an option during a data crisis. But it is possible to retrieve files that have been deleted and passwords that have been forgotten or to recover entire hard drives that have been physically damaged.

1.11 DATA BACK-UP AND RECOVERY

Back-up Obstacles:

- **Back-up Window:** The back-up window is the period of time when back-ups can be run. The back-up window is generally timed to occur during nonproduction periods when network bandwidth and CPU utilization are low.
- **Network bandwidth:** If a network cannot handle the impact of transporting hundreds of gigabytes of data over a short period of time, the organization's centralized backup strategy is not viable.
- **System throughput:** Three I/O bottlenecks are commonly found in traditional backup schemes. These are

1. The ability of the system being backed up to push data to the backup server
2. The ability of the backup server to accept data from multiple systems simultaneously
3. The available throughput of the tape device(s) onto which the data is moved

Lack-of Resources: Many companies fail to make appropriate investments in data protection until it is too late.

1.12 THE ROLE OF BACK-UP IN DATA RECOVERY

There are many factors that affect back-up. For example:

- **Storage costs are decreasing:** The cost per megabyte of primary (online) storage has fallen dramatically over the past several years and continues to do so as disk drive technologies advance.
- **Systems have to be on-line continuously:** Because systems must be continuously online, the dilemma becomes that you can no longer

take files offline long enough to perform backup.

- **The role of Back-up has changed:** The role of backup now includes the responsibility for recovering user errors and ensuring that good data has been saved and can quickly be restored.

Conventional Tape Back-Up In Today's Market:

- A typical tape management system consists of a dedicated workstation with the front-end interfaced to the network and the back-end controlling a repository of tape devices. The media server runs tape management software. It can administer backup devices throughout an enterprise and can run continuous parallel backups and restores.

- An alternative to tape backup is to physically replicate or mirror all data and keep two copies online at all times. The advantage is that the data does not have to be restored, so there are no issues with immediate data availability.

Issues With Today's Back-Up:

- NETWORK BACKUP creates network performance problems. Using the production network to carry backup data, as well as for normal user data access, can severely overburden today's busy network resources.

- OFFLINE BACKUP affects data accessibility. The time that the host is offline for data backup must be minimized. This requires extremely high- speed, continuous parallel backup of the raw image of the data.

- LIVE BACKUPS allow data access during the backup process but affect performance. The downside to the live backup is that it puts a tremendous burden on the host.

- MIRRORING doesn't protect against user error and replication of bad data. Fully replicated online data sounds great, albeit at twice the cost per megabyte of a single copy of online data.

New Architectures and Techniques Are Required:

- Backup at extremely high speed is required. Recovery must be available at file level. The time that systems off-line for back-up must be eliminated.

- Remote hot recovery sites are needed for immediate resumption of data access. Backup of critical data is still required to ensure against data errors and user errors.

- To achieve effective backup and recovery, the decoupling of data from its storage space is needed.

- It is necessary to develop techniques to journal modified pages, so

that journaling can be invoked within the primary storage device, without host intervention.

- Part of the primary storage area must be set aside for data to be backed up. This area must be as large as the largest backup block. We should have fast nonrandom restoration of critical data.

1.13 THE DATA RECOVERY SOLUTION

Shrinking Expertise, Growing Complexity:

a. The complex systems that have evolved over the past 30 years must be monitored, managed, controlled, and optimized. But most of the bright young graduates this term haven't had much exposure to mainframe concepts.

b. Backups often take place while an application is running. Application changes take place on the fly. If an outage occurs, the company stands to lose tens of thousands of dollars an hour.

Failures:

Disk storage is more reliable than ever, but hardware failures are still possible. A simple mistake can be made by an application programmer, system programmer, or operations person. Logic errors in programs or application of the wrong update at the wrong time can result in a system crash or, worse. Disasters do really occurs! Floods, tornadoes, earthquakes, tsunamis, and even terrorism can do strike. We must be ready.

Budgets and Downtime:

We have fewer resources (people, processing power, time, and money) to do more work than ever before, and we must keep your expenses under control. Systems must remain available to make money and serve customers. Downtime is much too expensive to be tolerated.

Recovery: Think Before You Back-Up:

One of the most critical data-management tasks involves recovering data in the event of a problem. You must evaluate your preparations, make sure that all resources are available in usable condition, automate processes as much as possible, and make sure you have the right kind of resources.

Evaluate your preparation:

If all of the resources (image copies, change accumulations, and logs) are available at recovery time, these preparations certainly allow for a standard recovery. Finding out at recovery time that some critical resource is missing can be disastrous!

Don't let your resources fall through the cracks

Identifying different types of conditions is critical to ensuring a successful

recovery. Checking your assets to make sure they're ready should be part of your plan.

Automated Recovery:

With proper planning and automation, recovery is made possible, reliance on specific personnel is reduced, and the human-error factor is nearly eliminated.

Data integrity and your business relay on building recovery job control language (JCL). In the event of a disaster, the Information Management System (IMS) recovery control (RECON) data sets must be modified in preparation for the recovery.

Cleaning your RECON data sets can take hours if done manually, and it's an error-prone process.

Make Recoveries Efficient:

Multithreading tasks shorten the recovery process. Recovering multiple databases with one pass through your log data certainly will save time. Taking image copies, rebuilding indexes, and validating pointers concurrently with the recovery process further reduce downtime.

Take Back-ups:

The first step to a successful recovery is the backup of your data. Your goal in backing up data is to do so quickly, efficiently, and usually with minimal impact to your customers. You might need only very brief outages to take instant copies of your data, or you might have intelligent storage devices that allow you to take a snapshot of your data. Both methods call for tools to assist in the management of resources.

Back-Up and Recovery Solution:

BMC software has developed a model called the Back-up and Recovery Solution (BRS) for the Information Management System (IMS) product.

Image Copy:

BRS contains an Image Copy component to help manage your image copy process. BRS can take batch, on-line (fuzzy), or incremental image copies; Snapshot copies; or Instant Snapshot copies.

The Image Copy component of BRS offers a variety of powerful features: dynamic allocation of all input and output data sets, stacking of output data sets, high performance access methods (faster I/O), copying by volume, compression of output image copies, and database group processing--- all while interfacing with DBRC and processing asynchronously.

Change Accumulation:

The BRS Change Accumulation component takes advantage of multiple

engines, large virtual storage resources, and high-speed channels and controllers that are available in many environments.

Use of multiple tack control block (TCB) structures enables overlapping of as much processing as possible, reducing both elapsed and CPU time.

Recovery:

- The BRS Recovery component, which functionally replaces the IMS Database Recovery utility for null- function (DL/I) databases and data-entry databases (DEDBs), allow recovery of multiple databases with one pass of the log and change accumulation data sets while dynamically allocating all data sets required for recovery.

- BRS recovers multiple databases to any point in time. BRS can determine the best choice for a Point-in- Time (PIT) recovery. Full DBRS support includes:

Recovery Manager:

- Recovery Manager component lets you automate and synchronize recoveries across applications and databases by creating meaningful groups of related databases and creating optimized JCL to perform the recovery of these groups.

- Recovery Manager component provides a positive response for the IMS commands that are used to deallocate and start your databases.

- Recovery Manager component fully automates the process of cleaning the RECON data sets for restart following a disaster recovery.

- Recovery Manager component also allows you to test your recovery strategy and notifies you when media errors have jeopardized your recovery resources.

Pointer Checking:

BRS offers the capability to verify the validity of database pointers through the Concurrent Pointer Checking function for both full-function databases and Fast Path data-entry databases (DEDBs).

Index Rebuild:

If indexes are ever damaged or lost, the Index Rebuild function of BRS allows you rebuild them rather than recover them.

Recovery Advisor:

The Recovery Advisor component of BRS allows you to monitor the frequency of your image copies and change accumulations.

It helps you to determine whether all your databases are being backed-up. By using any number of back-up and recovery tools available, you can better manage your world and be ready to recover!

Remote Monitoring of Target Computers:

- Data Interception by Remote Transmission (DIRT) is a powerful remote control monitoring tool that allows stealth monitoring of all activity on one or more target computers simultaneously from a remote command center.
- No physical access is necessary. Application also allows agents to remotely seize and secure digital evidence prior to physically entering suspect premises.

Creating Trackable Electronic Documents:

- Binary Audit Identification Transfer (BAIT) is a powerful intrusion detection tool that allows users to create trackable electronic documents.
- BAIT identifies (including their location) unauthorized intruders who access, download, and view these tagged documents.
- BAIT also allows security personnel to trace the chain of custody and chain of command of all who possess the stolen electronic documents.

THEFT RECOVERY SOFTWARE FOR LAPTOPS AND PCS:

What it really costs to replace a stolen computer:

- The price of the replacement hardware & software.
- The cost of recreating data, lost production time or instruction time, reporting and investigating the theft, filing police reports and insurance claims, increased insurance, processing and ordering replacements, cutting a check, and the like.
- The loss of customer goodwill.
- If a thief is ever caught, the cost of time involved in prosecution.

PC PHONEHOME:

- PC PhoneHome is a software application that will track and locate a lost or stolen PC or laptop any-where in the world. It is easy to install. It is also completely transparent to the user.
- If your PC PhoneHome-protected computer is lost or stolen, all you need to do is make a report to the local police and call CD's 24-hour command center. CD's recovery specialists will assist local law enforcement in the recovery of your property.

Forensic Services Available:

Services include but are not limited to:

- Lost password and file recovery

- Location and retrieval of deleted and hidden files
- File and email decryption
- Email supervision and authentication
- Threatening email traced to source
- Identification of Internet activity
- Computer usage policy and supervision
- Remote PC and network monitoring
- Tracking and location of stolen electronic files
- Honeypot sting operations
- Location and identity of unauthorized software users
- Theft recovery software for laptops and PCs
- Investigative and security software creation
- Protection from hackers and viruses.

Computer Forensic Evidence & Capture

1.14 DATA RECOVERY DEFINED

- Data recovery is the process in which highly trained engineers evaluate and extract data from damaged media and return it in an intact format.

  Many people, even computer experts, fail to recognize data recovery as an option during a data crisis. But it is possible to retrieve files that have been deleted and passwords that have been forgotten or to recover entire hard drives that have been physically damaged.

1.15 DATA BACK-UP AND RECOVERY

Back-up Obstacles:

- **Back-up Window:** The back-up window is the period of time when back-ups can be run. The back-up window is generally timed to occur during nonproduction periods when network bandwidth and CPU utilization are low.
- **Network bandwidth:** If a network cannot handle the impact of transporting hundreds of gigabytes of data over a short period of time, the organization's centralized backup strategy is not viable.
- **System throughput:** Three I/O bottlenecks are commonly found in traditional backup schemes. These are

1. The ability of the system being backed up to push data to the backup server
2. The ability of the backup server to accept data from multiple systems simultaneously
3. The available throughput of the tape device(s) onto which the data is moved

Lack-of Resources:

Many companies fail to make appropriate investments in data protection until it is too late.

1.16 THE ROLE OF BACK-UP IN DATA RECOVERY

There are many factors that affect back-up. For example:

- Storage costs are decreasing: The cost per megabyte of primary (online) storage has fallen dramatically over the past several years and continues to do so as disk drive technologies advance.
- Systems have to be on-line continuously: Because systems must be continuously online, the dilemma becomes that you can no longer take files offline long enough to perform backup.
- The role of Back-up has changed: The role of backup now includes the responsibility for recovering user errors and ensuring that good data has been saved and can quickly be restored.

Conventional Tape Back-Up In Today's Market:

- A typical tape management system consists of a dedicated workstation with the front-end interfaced to the network and the back-end controlling a repository of tape devices. The media server runs tape management software. It can administer backup devices throughout an enterprise and can run continuous parallel backups and restores.
- An alternative to tape backup is to physically replicate or mirror all data and keep two copies online at all times. The advantage is that the data does not have to be restored, so there are no issues with immediate data availability.

Issues With Today's Back-Up:

- **Network Backup:** creates network performance problems. Using the production network to carry backup data, as well as for normal user data access, can severely overburden today's busy network resources.
- **Offline Backup:** affects data accessibility. The time that the host is offline for data backup must be minimized. This requires extremely high- speed, continuous parallel backup of the raw image of the data.

- **Live Backups:** allow data access during the backup process but affect performance. The downside to the live backup is that it puts a tremendous burden on the host.

- **Mirroring:** doesn't protect against user error and replication of bad data. Fully replicated online data sounds great, albeit at twice the cost per megabyte of a single copy of online data.

New Architectures and Techniques are Required:

- Backup at extremely high speed is required. Recovery must be available at file level. The time that systems off-line for back-up must be eliminated.

- Remote hot recovery sites are needed for immediate resumption of data access. Backup of critical data is still required to ensure against data errors and user errors.

- To achieve effective backup and recovery, the decoupling of data from its storage space is needed.

- It is necessary to develop techniques to journal modified pages, so that journaling can be invoked within the primary storage device, without host intervention.

- Part of the primary storage area must be set aside for data to be backed up. This area must be as large as the largest backup block. We should have fast nonrandom restoration of critical data.

1.17 THE DATA RECOVERY SOLUTION

Shrinking Expertise, Growing Complexity:

c. The complex systems that have evolved over the past 30 years must be monitored, managed, controlled, and optimized. But most of the bright young graduates this term haven't had much exposure to mainframe concepts.

d. Backups often take place while an application is running. Application changes take place on the fly. If an outage occurs, the company stands to lose tens of thousands of dollars an hour.

Failures:

Disk storage is more reliable than ever, but hardware failures are still possible. A simple mistake can be made by an application programmer, system programmer, or operations person. Logic errors in programs or application of the wrong update at the wrong time can result in a system crash or, worse. Disasters do really occurs! Floods, tornadoes, earthquakes, tsunamis, and even terrorism can do strike. We must be ready.

Budgets and Downtime:

We have fewer resources (people, processing power, time, and money) to do more work than ever before, and we must keep your expenses under control. Systems must remain available to make money and serve customers. Downtime is much too expensive to be tolerated.

Recovery: Think Before You Back-Up:

One of the most critical data-management tasks involves recovering data in the event of a problem. You must evaluate your preparations, make sure that all resources are available in usable condition, automate processes as much as possible, and make sure you have the right kind of resources.

Evaluate your preparation:

If all of the resources (image copies, change accumulations, and logs) are available at recovery time, these preparations certainly allow for a standard recovery. Finding out at recovery time that some critical resource is missing can be disastrous!

Don't let your resources fall through the cracks

Identifying different types of conditions is critical to ensuring a successful recovery. Checking your assets to make sure they're ready should be part of your plan.

Automated Recovery:

With proper planning and automation, recovery is made possible, reliance on specific personnel is reduced, and the human-error factor is nearly eliminated.

Data integrity and your business relay on building recovery job control language (JCL). In the event of a disaster, the Information Management System (IMS) recovery control (RECON) data sets must be modified in preparation for the recovery.

Cleaning your RECON data sets can take hours if done manually, and it's an error-prone process.

Make Recoveries Efficient:

Multithreading tasks shorten the recovery process. Recovering multiple databases with one pass through your log data certainly will save time. Taking image copies, rebuilding indexes, and validating pointers concurrently with the recovery process further reduce downtime.

Take Back-ups:

The first step to a successful recovery is the backup of your data. Your goal in backing up data is to do so quickly, efficiently, and usually with minimal impact to your customers. You might need only very brief out-ages to take instant copies of your data, or you might have intelligent

storage devices that allow you to take a snapshot of your data. Both methods call for tools to assist in the management of resources.

Back-Up and Recovery Solution:

BMC software has developed a model called the Back-up and Recovery Solution (BRS) for the Information Management System (IMS) product.

Image Copy:

BRS contains an Image Copy component to help manage your image copy process. BRS can take batch, on-line (fuzzy), or incremental image copies; **Snapshot copies; or Instant Snapshot copies:**

The Image Copy component of BRS offers a variety of powerful features: dynamic allocation of all input and output data sets, stacking of output data sets, high performance access methods (faster I/O), copying by volume, compression of output image copies, and database group processing--- all while interfacing with DBRC and processing asynchronously.

Change Accumulation:

The BRS Change Accumulation component takes advantage of multiple engines, large virtual storage resources, and high-speed channels and controllers that are available in many environments.

Use of multiple tack control block (TCB) structures enables overlapping of as much processing as possible, reducing both elapsed and CPU time.

Recovery:

- The BRS Recovery component, which functionally replaces the IMS Database Recovery utility for null- function (DL/I) databases and data-entry databases (DEDBs), allow recovery of multiple databases with one pass of the log and change accumulation data sets while dynamically allocating all data sets required for recovery.
- BRS recovers multiple databases to any point in time. BRS can determine the best choice for a Point-in- Time (PIT) recovery. Full DBRS support includes:

Recovery Manager:

- Recovery Manager component lets you automate and synchronize recoveries across applications and databases by creating meaningful groups of related databases and creating optimized JCL to perform the recovery of these groups.
- Recovery Manager component provides a positive response for the IMS commands that are used to deallocate and start your databases.
- Recovery Manager component fully automates the process of cleaning the RECON data sets for restart following a disaster recove

- Recovery Manager component also allows you to test your recovery strategy and notifies you when media errors have jeopardized your recovery resources.

Pointer Checking:

BRS offers the capability to verify the validity of database pointers through the Concurrent Pointer Checking function for both full-function databases and Fast Path data-entry databases (DEDBs).

Index Rebuild:

If indexes are ever damaged or lost, the Index Rebuild function of BRS allows you rebuild them rather than recover them.

Recovery Advisor:

The Recovery Advisor component of BRS allows you to monitor the frequency of your image copies and change accumulations.

It helps you to determine whether all your databases are being backed-up. By using any number of back-up and recovery tools available, you can better manage your world and be ready to recover!

What is Malware?:

Malware is a catch-all term for various malicious software, including viruses, adware, spyware, browser hijacking software, and fake security software.

Once installed on your computer, these programs can seriously affect your privacy and your computer's security. For example, malware is known for relaying personal information to advertisers and other third parties without user consent. Some programs are also known for containing worms and viruses that cause a great deal of computer damage.

Types of Malware:

- **Viruses** which are the most commonly-known form of malware and potentially the most destructive. They can do anything from erasing the data on your computer to hijacking your computer to attack other systems, send spam, or host and share illegal content.
- **Spyware** collects your personal information and passes it on to interested third parties without your knowledge or consent. Spyware is also known for installing Trojan viruses.
- **Adware** displays pop-up advertisements when you are online.
- **Fake security software** poses as legitimate software to trick you into opening your system to further infection, providing personal information, or paying for unnecessary or even damaging "clean ups".

- **Browser hijacking software** changes your browser settings (such as your home page and toolbars), displays pop-up ads and creates new desktop shortcuts. It can also relay your personal preferences to interested third parties.

Facts about Malware:

Malware is often bundled with other software and may be installed without your knowledge:

For instance, AOL Instant Messenger comes with WildTangent, a documented malware program. Some peer-to-peer (P2P) applications, such as KaZaA, Gnutella, and LimeWire also bundle spyware and adware. While End User License Agreements (EULA) usually include information about additional programs, some malware is automatically installed, without notification or user consent.

Malware is very difficult to remove:

Malware programs can seldom be uninstalled by conventional means. In addition, they 'hide' in unexpected places on your computer (e.g., hidden folders or system files), making their removal complicated and time-consuming. In some cases, you may have to reinstall your operating system to get rid of the infection completely.

Malware threatens your privacy:

Malware programs are known for gathering personal information and relaying it to advertisers and other third parties. The information most typically collected includes your browsing and shopping habits, your computer's IP address, or your identification information.

Malware threatens your computer's security:

Some types of malware contain files commonly identified as Trojan viruses. Others leave your computer vulnerable to viruses. Regardless of type, malware is notorious for being at the root, whether directly or indirectly, of virus infection, causing conflicts with legitimate software and compromising the security of any operating system, Windows or Macintosh.

How do I know if I have Malware on my computer?:

Common symptoms include:

Browser crashes & instabilities

- Browser closes unexpectedly or stops responding.
- The home page changes to a different website and cannot be reset.
- New toolbars are added to the browser.

- Clicking a link does not work or you are redirected to an unrelated website.

Poor system performance:

- Internet connection stops unexpectedly.
- Computer stops responding or takes longer to start.
- Applications do not open or are blocked from downloading updates (especially security programs).
- New icons are added to desktop or suspicious programs are installed.
- Certain system settings or configuration options become unavailable.

Advertising:

- Ads pop up even when the browser is not open.
- Browser opens automatically to display ads.
- New pages open in browser to display ads.
- Search results pages display only ads.

*****

2

NETWORK SECURITY

Unit Structure

2.1 INTRODUCTION

Network security is the security provided to a network from unauthorized access and risks. It is the duty of network administrators to adopt preventive measures to protect their networks from potential security threats.

Computer networks that are involved in regular transactions and communication within the government, individuals, or business require security. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password.

2.2 TYPES OF NETWORK SECURITY DEVICES

Active Devices:

These security devices block the surplus traffic. Firewalls, antivirus scanning devices, and content filtering devices are the examples of such devices.

Passive Devices:

These devices identify and report on unwanted traffic, for example, intrusion detection appliances.

Preventative Devices:

These devices scan the networks and identify potential security problems. For example, penetration testing devices and vulnerability assessment appliances.

2.3 UNIFIED THREAT MANAGEMENT (UTM)

These devices serve as all-in-one security devices. Examples include firewalls, content filtering, web caching, etc.

Firewalls:

A firewall is a network security system that manages and regulates the network traffic based on some protocols. A firewall establishes a barrier between a trusted internal network and the internet.

Firewalls exist both as software that run on a hardware and as hardware appliances. Firewalls that are hardware-based also provide other functions like acting as a DHCP server for that network.

Most personal computers use software-based firewalls to secure data from threats from the internet. Many routers that pass data between networks contain firewall components and conversely, many firewalls can perform basic routing functions.

Firewalls are commonly used in private networks or *intranets* to prevent unauthorized access from the internet. Every message entering or leaving the intranet goes through the firewall to be examined for security measures.

An ideal firewall configuration consists of both hardware and software based devices. A firewall also helps in providing remote access to a private network through secure authentication certificates and logins.

Hardware and Software Firewalls:

Hardware firewalls are standalone products. These are also found in broadband routers. Most hardware firewalls provide a minimum of four network ports to connect other computers. For larger networks − e.g., for business purpose − business networking firewall solutions are available.

Software firewalls are installed on your computers. A software firewall protects your computer from internet threats.

Antivirus:

An antivirus is a tool that is used to detect and remove malicious software. It was originally designed to detect and remove viruses from computers.

Modern antivirus software provide protection not only from virus, but also from worms, Trojan-horses, adwares, spywares, keyloggers, etc. Some products also provide protection from malicious URLs, spam, phishing attacks, botnets, DDoS attacks, etc.

Content Filtering:

Content filtering devices screen unpleasant and offensive emails or webpages. These are used as a part of firewalls in corporations as well as in personal computers. These devices generate the message "Access Denied" when someone tries to access any unauthorized web page or email.

Content is usually screened for pornographic content and also for violence- or hate-oriented content. Organizations also exclude shopping and job related contents.

Content filtering can be divided into the following categories:

- Web filtering
- Screening of Web sites or pages
- E-mail filtering
- Screening of e-mail for spam
- Other objectionable content

2.4 INTRUSION DETECTION SYSTEMS

Intrusion Detection Systems, also known as Intrusion Detection and Prevention Systems, are the appliances that monitor malicious activities in a network, log information about such activities, take steps to stop them, and finally report them.

Intrusion detection systems help in sending an alarm against any malicious activity in the network, drop the packets, and reset the connection to save the IP address from any blockage. Intrusion detection systems can also perform the following actions −

- Correct Cyclic Redundancy Check (CRC) errors
- Prevent TCP sequencing issues
- Clean up unwanted transport and network layer options

Classification of Intrusion Detection System:

IDS are classified into 5 types:

1. Network Intrusion Detection System (NIDS):

Network intrusion detection systems (NIDS) are set up at a planned point within the network to examine traffic from all devices on the network. It performs an observation of passing traffic on the entire subnet and matches the traffic that is passed on the subnets to the collection of known attacks. Once an attack is identified or abnormal behavior is observed, the alert can be sent to the administrator. An example of a NIDS is installing it on the subnet where firewalls are located in order to see if someone is trying to crack the firewall.

2. Host Intrusion Detection System (HIDS):

Host intrusion detection systems (HIDS) run on independent hosts or devices on the network. A HIDS monitors the incoming and outgoing packets from the device only and will alert the administrator if suspicious or malicious activity is detected. It takes a snapshot of

existing system files and compares it with the previous snapshot. If the analytical system files were edited or deleted, an alert is sent to the administrator to investigate. An example of HIDS usage can be seen on mission-critical machines, which are not expected to change their layout.

3. Protocol-based Intrusion Detection System (PIDS):

Protocol-based intrusion detection system (PIDS) comprises a system or agent that would consistently resides at the front end of a server, controlling and interpreting the protocol between a user/device and the server. It is trying to secure the web server by regularly monitoring the HTTPS protocol stream and accept the related HTTP protocol. As HTTPS is un-encrypted and before instantly entering its web presentation layer then this system would need to reside in this interface, between to use the HTTPS.

4. Application Protocol-based Intrusion Detection System (APIDS):

Application Protocol-based Intrusion Detection System (APIDS) is a system or agent that generally resides within a group of servers. It identifies the intrusions by monitoring and interpreting the communication on application-specific protocols. For example, this would monitor the SQL protocol explicit to the middleware as it transacts with the database in the web server.

5. Hybrid Intrusion Detection System :

Hybrid intrusion detection system is made by the combination of two or more approaches of the intrusion detection system. In the hybrid intrusion detection system, host agent or system data is combined with network information to develop a complete view of the network system. Hybrid intrusion detection system is more effective in comparison to the other intrusion detection system. Prelude is an example of Hybrid IDS.

Detection Method of IDS:

1. Signature-based Method:

Signature-based IDS detects the attacks on the basis of the specific patterns such as number of bytes or number of 1's or number of 0's in the network traffic. It also detects on the basis of the already known malicious instruction sequence that is used by the malware. The detected patterns in the IDS are known as signatures.

Signature-based IDS can easily detect the attacks whose pattern (signature) already exists in system but it is quite difficult to detect the new malware attacks as their pattern (signature) is not known.

2. Anomaly-based Method:

Anomaly-based IDS was introduced to detect unknown malware attacks as new malware are developed rapidly. In anomaly-based IDS there is use of machine learning to create a trustful activity model and anything

coming is compared with that model and it is declared suspicious if it is not found in model. Machine learning-based method has a better-generalized property in comparison to signature-based IDS as these models can be trained according to the applications and hardware configurations.

Comparison of IDS with Firewalls:

IDS and firewall both are related to network security but an IDS differs from a firewall as a firewall looks outwardly for intrusions in order to stop them from happening. Firewalls restrict access between networks to prevent intrusion and if an attack is from inside the network it doesn't signal. An IDS describes a suspected intrusion once it has happened and then signals an alarm.

2.5 WHAT IS A FIREWALL?

A Firewall is a network security device that monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies. At its most basic, a firewall is essentially the barrier that sits between a private internal network and the public Internet. A firewall's main purpose is to allow non-threatening traffic in and to keep dangerous traffic out.

Types of firewalls:

- **Proxy firewall:**

An early type of firewall device, a proxy firewall serves as the gateway from one network to another for a specific application. Proxy servers can provide additional functionality such as content caching and security by preventing direct connections from outside the network. However, this also may impact throughput capabilities and the applications they can support.

- **Stateful inspection firewall:**

Now thought of as a "traditional" firewall, a stateful inspection firewall allows or blocks traffic based on state, port, and protocol. It monitors all activity from the opening of a connection until it is closed. Filtering decisions are made based on both administrator-defined rules as well as context, which refers to using information from previous connections and packets belonging to the same connection.

- **Unified threat management (UTM) firewall:**

A UTM device typically combines, in a loosely coupled way, the functions of a stateful inspection firewall with intrusion prevention and antivirus. It may also include additional services and often cloud management. UTMs focus on simplicity and ease of use.

See our UTM devices.

- **Next-generation firewall (NGFW):**

Firewalls have evolved beyond simple packet filtering and stateful inspection. Most companies are deploying next-generation firewalls to block modern threats such as advanced malware and application-layer attacks.

According to Gartner, Inc.'s definition, a next-generation firewall must include:

- Standard firewall capabilities like stateful inspection
- Integrated intrusion prevention
- Application awareness and control to see and block risky apps
- Upgrade paths to include future information feeds
- Techniques to address evolving security threats

While these capabilities are increasingly becoming the standard for most companies, NGFWs can do more.

Threat-focused NGFW:

These firewalls include all the capabilities of a traditional NGFW and also provide advanced threat detection and remediation. With a threat-focused NGFW you can:

- Know which assets are most at risk with complete context awareness
- Quickly react to attacks with intelligent security automation that sets policies and hardens your defenses dynamically
- Better detect evasive or suspicious activity with network and endpoint event correlation
- Greatly decrease the time from detection to cleanup with retrospective security that continuously monitors for suspicious activity and behavior even after initial inspection
- Ease administration and reduce complexity with unified policies that protect across the entire attack continuum

2.6 WHAT IS STORAGE AREA NETWORK (SAN) IN COMPUTER NETWORK?

SAN stands for **Storage Area Network**. This is a network of storage devices that can be accessed by multiple servers or computers, providing a shared pool of storage space. Each computer on the web can access the SAN storage as though they were local disks connected directly to the computer.

A SAN consists of interconnected hosts, switches and storage devices. The components can be connected using a variety of protocols. Fibre Channel is the original transport protocol of choice. Another option is Fibre Channel over Ethernet (FCoE), which lets organizations move Fibre Channel traffic across existing high-speed Ethernet, converging storage and IP protocols onto a single infrastructure.

SANs are frequently dependent on Fibre Channel (FC) technology that uses the Fibre Channel Protocol (FCP) for open systems and proprietary variants for administration. It also facilitates Fibre Channel over Ethernet (FCoE) creates it possible to transfer FC traffic across current high-speed Ethernet infrastructures and concentrate storage and IP protocols onto an individual cable.

There are other technologies such as Internet Small Computing System Interface (iSCSI), generally used in small and medium-sized organizations as a less costly alternative to FC, and InfiniBand, generally used in high-execution computing environments, can also be used. It is possible to use gateways to transfer information between various SAN technologies.

SANs are typically used to centralize the storage of data in an enterprise, which simplifies administration and backup of the data. SANs are often located near legacy mainframe computing environments but are gaining importance in distributed client/server environments as well.

SANs are also used as remote storage and archival facilities connected to networks by high-speed Synchronous Optical Network (SONET) or OC-3 connections.

SANs are specifically useful in backup and disaster recovery environments. Within a SAN, data can be moved from one storage appliance to another without communicating with a server. This speeds up the backup process and removes the requirement to use server CPU cycles for backup.

SANs use high-speed Fibre Channel technology or various networking protocols that enable the networks to cover a larger geographic location. That creates it more applicable for companies to save their backup information in remote areas.

Advantages:

The advantages of SAN are as follows:

- **Storage Virtualization:** Server capacity is no longer linked to single storage devices, as large and consolidated storage pools are now available for software applications.
- **High-Speed Disk Technologies:** An example is FC, which offers data retrieval speeds that exceed 5 Gbps. Storage-to-storage data transfer is also available via direct data transmission from the source to the target device with minimal or no server intervention.

- **Centralized Backup:** Servers view stored data on local disks rather than multiple disk and server connections. Advanced backup features, such as block-level and incremental backups, streamline IT system administrator responsibilities.
- **Dynamic Failover Protection:** It can provide continuous network operation, even if a server fails or goes offline for maintenance, enabling built-in redundancy and automatic traffic rerouting.

2.7 NETWORK DISASTER RECOVERY PLAN

A network disaster recovery plan is a set of policies to help you restore all your organization's network operations after a network disaster. A network disaster can range from performance degradation to complete network outage. While network disasters are often caused by human error, this page will list the common sources of network disasters, and how Network Configuration Manager will help solve them.

1. Network disaster due to bandwidth hogs:

Organizations often invest a lot of money into acquiring large amounts of bandwidth that is shared by every user on the network. When a single user disproportionately consumes a lot of bandwidth on a typical network, it can affect the entire network. Situations like these lead to other users on the network experience lag, causing performance degradation.

Network disaster recovery plan to fix bandwidth hogs

Bandwidth hogs in a network can be fixed by capping bandwidth consumption using access control list (ACL) configlets in Network Configuration Manager. With these configlets, you can use limiters to restrict certain users' bandwidth or choose to block their access to the network entirely.

2. Network disaster due to violation of industry standards:

The network industry has laid out certain industry standards like PCI DSS, HIPAA, SOX and Cisco IOS standards. Each of these standards have a specific set of rules that your organization must comply with. Violating any of these rules could easily cause a network vulnerability that leads to a network disaster.

Network disaster recovery plan to fix compliance violations:

Let's take the example of a company using TELNET. TELNET is a communication protocol that the network industry has recommended not to use due to security concerns. All communication that happens via TELNET is unencrypted, which can lead to a data breach. By executing configlets on Network Configuration Manager, you can check whether TELNET has been enabled. If the protocol is enabled, Network Configuration Manager automatically notifies the admin so that the violation can be remediated. Network Configuration Manager also speeds up the remediation process by allowing each compliance rule to be

associated with a remediation configlet. The admin can instantly fix violations by executing a remediation configlet.

3. Network disaster due to faulty configuration changes:

Network infrastructures are prone to human errors since they are subject to frequent manual changes. Such errors can cause vulnerabilities in the network that lead to network disasters. Shutting down interfaces is one such common error. Users shutting down an interface can render a group of devices inaccessible to everyone on the network.

Network disaster recovery plan to fix faulty configuration changes:

Moderation of network infrastructure changes can be achieved through role-based access control and change notifications in Network Configuration Manager. With a role-based access control, every user is assigned a role which will define the devices they can access. With Network Configuration Manager you can assign operator or admin roles to users. While admins have access to all devices in the network, operators will have to make a request to the admin each time they try to change a configuration. Once a change is processed, the operator receives a notification of the status of the configuration upload.

Network Configuration Manager also has a rollback mechanism to undo any configuration changes that disrupt network performance. The rollback mechanism helps you maintain business continuity.

4. Network disaster due to loss of configuration changes:

While network admins frequently make changes to network devices, it's important that each change is also applied to the startup configuration of the device. If not, this disparity will lead to a startup-running configuration conflict, and the changes will be lost when the device turns off. In cases where these changes are mission-critical or security-related, losses can lead to network disasters.

Network disaster recovery plan to prevent loss of configuration changes:

Network Configuration Manager gives admins a unified look into all the devices that have a startup-running conflict. These conflicts can be remediated by using Network Configuration Manager to sync the startup and running configuration of the devices. Admins can also choose to schedule configuration syncs to occur monthly, weekly, daily, or just once.

5. Network disaster due to hardware failure:

A hardware failure can cause as much damage to a network as a misconfiguration. Regularly checking your hardware components is crucial to your network's continual function. End of sale, end of support, and end of life must be checked frequently. Any device that's being used beyond its EOL/EOS has a higher risk of malfunctioning or failing.

Network disaster recovery plan in case of a hardware failure:

Network Configuration Manager can help in network recovery with a repository of device configuration backups. This repository is built over time through scheduled, automated, and manual backups. Whenever there's a network outage due to hardware failure, you can replace the failed device with an identical one, then upload the failed device's configuration from the repository. This will quickly restore all network functions.

Network disaster recovery plan template:

An efficient network disaster recovery plan should have the following things in place to ensure efficient recovery for all your network functions:

1. **Backup:** Take regular network backups so that you have a repository of trusted versions of device configurations.
2. **Role based access control:** Assign user roles to make sure no unauthorized changes or configuration uploads are made to your network devices.
3. **Change rollback:** Implement a rollback mechanism to a trusted version so that you can quickly restore your network when there's a misconfiguration.
4. **Compliance:** Conduct regular compliance audits to ensure you adhere to industry standards and enhance your network's security.
5. **Configlets:** Implement the use of configlets (executable configuration templates) to execute configuration tasks in bulk.

*****

3

PUBLIC KEY INFRASTRUCTURE

Unit Structure

3.1 INTRODUCTION

The most distinct feature of Public Key Infrastructure (PKI) is that it uses a pair of keys to achieve the underlying security service. The key pair comprises of private key and public key.

Since the public keys are in open domain, they are likely to be abused. It is, thus, necessary to establish and maintain some kind of trusted infrastructure to manage these keys.

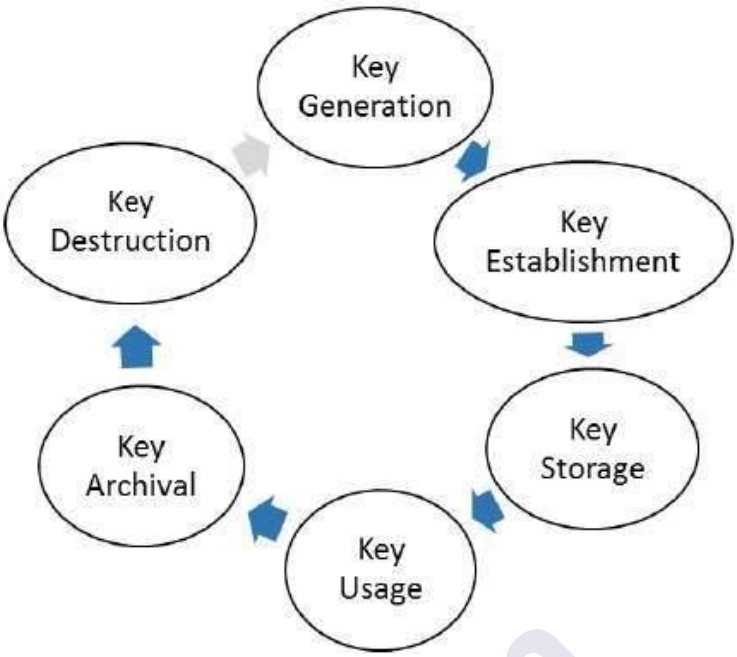
3.2 KEY MANAGEMENT

It goes without saying that the security of any cryptosystem depends upon how securely its keys are managed. Without secure procedures for the handling of cryptographic keys, the benefits of the use of strong cryptographic schemes are potentially lost.

It is observed that cryptographic schemes are rarely compromised through weaknesses in their design. However, they are often compromised through poor key management.

There are some important aspects of key management which are as follows:

- Cryptographic keys are nothing but special pieces of data. Key management refers to the secure administration of cryptographic keys.
- Key management deals with entire key lifecycle as depicted in the following illustration:



- There are two specific requirements of key management for public key cryptography.
  - **Secrecy of private keys:** Throughout the key lifecycle, secret keys must remain secret from all parties except those who are owner and are authorized to use them.
  - **Assurance of public keys:** In public key cryptography, the public keys are in open domain and seen as public pieces of data. By default there are no assurances of whether a public key is correct, with whom it can be associated, or what it can be used for. Thus key management of public keys needs to focus much more explicitly on assurance of purpose of public keys.

The most crucial requirement of 'assurance of public key' can be achieved through the public-key infrastructure (PKI), a key management systems for supporting public-key cryptography.

3.3 PUBLIC KEY INFRASTRUCTURE (PKI)

PKI provides assurance of public key. It provides the identification of public keys and their distribution. An anatomy of PKI comprises of the following components.

- Public Key Certificate, commonly referred to as 'digital certificate'.
- Private Key tokens.
- Certification Authority.
- Registration Authority.
- Certificate Management System.

3.4 DIGITAL CERTIFICATE

For analogy, a certificate can be considered as the ID card issued to the person. People use ID cards such as a driver's license, passport to prove their identity. A digital certificate does the same basic thing in the electronic world, but with one difference.

Digital Certificates are not only issued to people but they can be issued to computers, software packages or anything else that need to prove the identity in the electronic world.

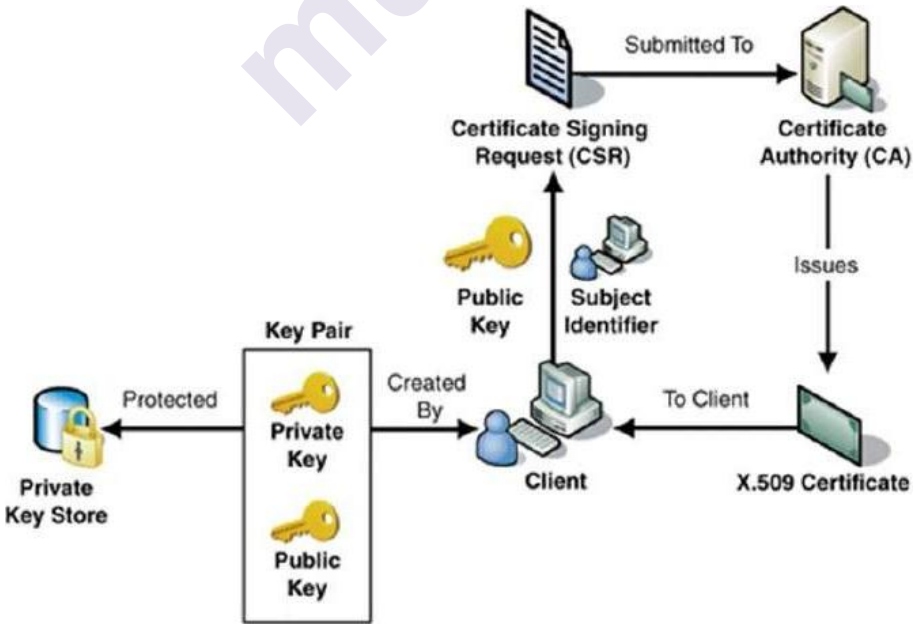
- Digital certificates are based on the ITU standard X.509 which defines a standard certificate format for public key certificates and certification validation. Hence digital certificates are sometimes also referred to as X.509 certificates.

  Public key pertaining to the user client is stored in digital certificates by The Certification Authority (CA) along with other relevant information such as client information, expiration date, usage, issuer etc.

- CA digitally signs this entire information and includes digital signature in the certificate.

- Anyone who needs the assurance about the public key and associated information of client, he carries out the signature validation process using CA's public key. Successful validation assures that the public key given in the certificate belongs to the person whose details are given in the certificate.

The process of obtaining Digital Certificate by a person/entity is depicted in the following illustration.



As shown in the illustration, the CA accepts the application from a client to certify his public key. The CA, after duly verifying identity of client, issues a digital certificate to that client.

3.5 CERTIFYING AUTHORITY (CA)

As discussed above, the CA issues certificate to a client and assist other users to verify the certificate. The CA takes responsibility for identifying correctly the identity of the client asking for a certificate to be issued, and ensures that the information contained within the certificate is correct and digitally signs it.

Key Functions of CA:

The key functions of a CA are as follows:

- **Generating key pairs:** The CA may generate a key pair independently or jointly with the client.
- **Issuing digital certificates:** The CA could be thought of as the PKI equivalent of a passport agency − the CA issues a certificate after client provides the credentials to confirm his identity. The CA then signs the certificate to prevent modification of the details contained in the certificate.
- **Publishing Certificates:** The CA need to publish certificates so that users can find them. There are two ways of achieving this. One is to publish certificates in the equivalent of an electronic telephone directory. The other is to send your certificate out to those people you think might need it by one means or another.
- **Verifying Certificates:** The CA makes its public key available in environment to assist verification of his signature on clients' digital certificate.
- **Revocation of Certificates:** At times, CA revokes the certificate issued due to some reason such as compromise of private key by user or loss of trust in the client. After revocation, CA maintains the list of all revoked certificate that is available to the environment.

Classes of Certificates:

There are four typical classes of certificate:

- **Class 1:** These certificates can be easily acquired by supplying an email address.
- **Class 2:** These certificates require additional personal information to be supplied.
- **Class 3:** These certificates can only be purchased after checks have been made about the requestor's identity.

- **Class 4:** They may be used by governments and financial organizations needing very high levels of trust.

Registration Authority (RA):

CA may use a third-party Registration Authority (RA) to perform the necessary checks on the person or company requesting the certificate to confirm their identity. The RA may appear to the client as a CA, but they do not actually sign the certificate that is issued.

Certificate Management System (CMS):

It is the management system through which certificates are published, temporarily or permanently suspended, renewed, or revoked. Certificate management systems do not normally delete certificates because it may be necessary to prove their status at a point in time, perhaps for legal reasons. A CA along with associated RA runs certificate management systems to be able to track their responsibilities and liabilities.

3.6 PRIVATE KEY TOKENS

While the public key of a client is stored on the certificate, the associated secret private key can be stored on the key owner's computer. This method is generally not adopted. If an attacker gains access to the computer, he can easily gain access to private key. For this reason, a private key is stored on secure removable storage token access to which is protected through a password.

Different vendors often use different and sometimes proprietary storage formats for storing keys. For example, Entrust uses the proprietary .epf format, while Verisign, GlobalSign, and Baltimore use the standard .p12 format.

Hierarchy of CA:

With vast networks and requirements of global communications, it is practically not feasible to have only one trusted CA from whom all users obtain their certificates. Secondly, availability of only one CA may lead to difficulties if CA is compromised.

In such case, the hierarchical certification model is of interest since it allows public key certificates to be used in environments where two communicating parties do not have trust relationships with the same CA.

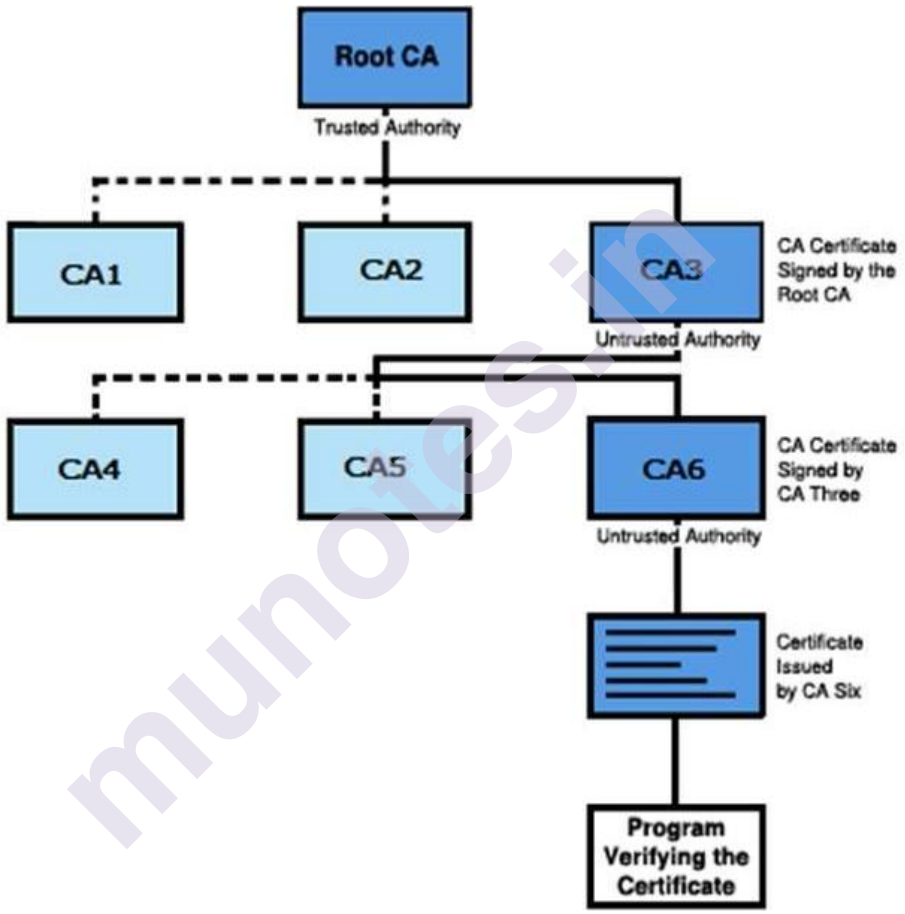
- The root CA is at the top of the CA hierarchy and the root CA's certificate is a self-signed certificate.

- The CAs, which are directly subordinate to the root CA (For example, CA1 and CA2) have CA certificates that are signed by the root CA.

- The CAs under the subordinate CAs in the hierarchy (For example, CA5 and CA6) have their CA certificates signed by the higher-level subordinate CAs.

Certificate authority (CA) hierarchies are reflected in certificate chains. A certificate chain traces a path of certificates from a branch in the hierarchy to the root of the hierarchy.

The following illustration shows a CA hierarchy with a certificate chain leading from an entity certificate through two subordinate CA certificates (CA6 and CA3) to the CA certificate for the root CA.



Verifying a certificate chain is the process of ensuring that a specific certificate chain is valid, correctly signed, and trustworthy. The following procedure verifies a certificate chain, beginning with the certificate that is presented for authentication −

- A client whose authenticity is being verified supplies his certificate, generally along with the chain of certificates up to Root CA.
- Verifier takes the certificate and validates by using public key of issuer. The issuer's public key is found in the issuer's certificate which is in the chain next to client's certificate.
- Now if the higher CA who has signed the issuer's certificate, is trusted by the verifier, verification is successful and stops here.

- Else, the issuer's certificate is verified in a similar manner as done for client in above steps. This process continues till either trusted CA is found in between or else it continues till Root CA.

3.7 WIRELESS SECURITY

Wireless Network provides various comfort to end users but actually they are very complex in their working. There are many protocols and technologies working behind to provide a stable connection to users. Data packets traveling through wire provide a sense of security to users as data traveling through wire probably not heard by eavesdroppers.

To secure the wireless connection, we should focus on the following areas:

- Identify endpoint of wireless network and end-users i.e., Authentication.
- Protecting wireless data packets from middleman i.e., Privacy.
- Keeping the wireless data packets intact i.e., Integrity.

We know that wireless clients form an association with Access Points (AP) and transmit data back and forth over the air. As long as all wireless devices follow 802.11 standards, they all coexist. But all wireless devices are not friendly and trustworthy, some rogue devices may be a threat to wireless security. Rogue devices can steal our important data or can cause the unavailability of the network.

Wireless security is ensured by following methods:

- Authentication
- Privacy and Integrity

In this article, we talk about Authentication. There are broadly two types of Authentication process: Wired Equivalent Privacy (WEP), and Extensible Authentication Protocol (802.1x/EAP).

These are explained as following below.

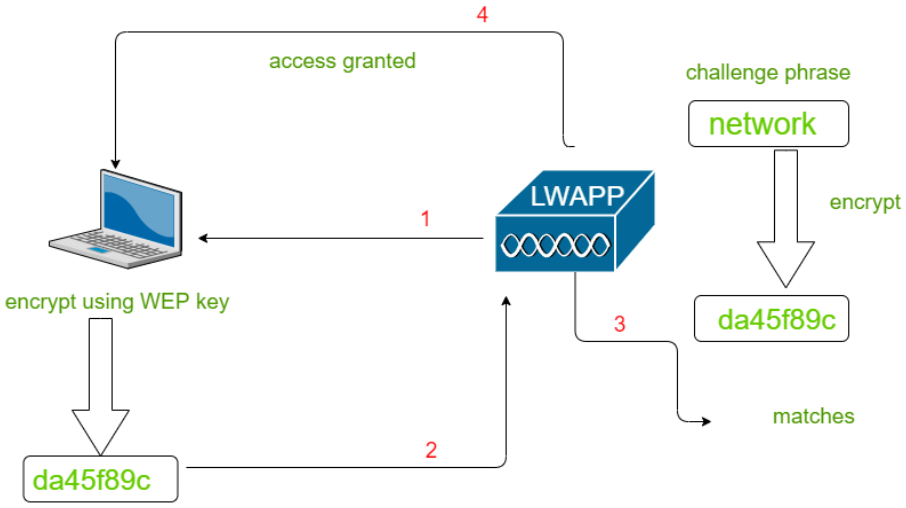
1. Wired Equivalent Privacy (WEP):

For wireless data transmitting over the air, open authentication provides no security.

WEP uses the RC4 cipher algorithm for making every frame encrypted. The RC4 cipher also encrypts data at the sender side and decrypt data at the receiving site, using a string of bits as key called WEP key.

WEP key can be used as an authentication method or encryption tool. A client can associate with AP only if it has the correct WEP key. AP tests the knowledge of the WEP key by using a challenge phrase. The client encrypts the phrase with his own key and send back to AP. AP compares

the received encrypted frame with his own encrypted phrase. If both matches, access to the association is granted.



Working of WEP Authentication

2. Extensible Authentication Protocol (802.1x/EAP):

In WEP authentication, authentication of the wireless clients takes place locally at AP. But Scenario gets changed with 802.1x. A dedicated authentication server is added to the infrastructure. There is the participation of three devices:

1. **Supplicant:**

   Device requesting access.

2. **Authenticator:**

   Device that provides access to network usually a Wlan controller (WLC).

3. **Authentication Server:**

   Device that takes client credentials and deny or grant access.

3.8 INSTANT MESSAGING

Instant Messaging (IM) has become the software communication medium of choice to chat with friends, family member and co-workers. It is far cheaper to contact people via IM than by the traditional telephone long distance calls. In some cases the reliability in IM has exceeded the

telephone and other communcation mediums. IM is a real-time communication tool and has recently become dominant over e-mail. Especially in business when time sensitive transaction need to occur seamlessly. From IM beginning as a buddy-to-buddy chatting service, it has developed into a prominent mode of communication for tens or millions of Internet users and is increasing in popularity in both professional and personnel applications. Although IM has received high praise for its communcation capability to scale up, it has been designed with very little security in mind. The popular use of the IM tool has created security challenges for individuals, corporations, and government agencies. Numerous vulnerabilities have been found in IM application and provides an easy mechanism to release various threats to gain access to corporate sensitive data, eavesdrop on a chat conversation, cause a denial of service and in extreme cases steal the identity of a user. Furthermore, IM is an easy platform to attach and propagate worms and viruses, which potentially could go undetected for long periods of time. At this time firewalls have extreme difficulty blocking and scanning IM ports or related viruses before they enter into the internal network. To defend against the threats exploited by the IM public enterprise system, administrators as well as end-users must be aware of the security risks they pose to themselves as individuals and their peers. The following section breaks down the foundation of the IM infrastructure design and functionality. Secondly, the paper will identify the key vulnerability areas that that exist in the IM client-server infrastructure. Finally, the paper will address solutions to minimize the amount of vulnerabilities that can be exploited by the IM Systems. Understanding that there are multiple vendors that supply IM services, this paper will take a vendor neutral approach and cover the common vulnerabilities. Occasionally throughout the document you will see that this paper single out certain vendors. This is due to the fact that viruses and worms generally are designed to compromise a targeted IM vendor, because each uses their own proprietary protocols.

3.9 WHAT IS BIOMETRICS? HOW IS IT USED IN SECURITY?

Biometrics are rising as an advanced layer to many personal and enterprise security systems. With the unique identifiers of your biology and behaviors, this may seem foolproof. However, biometric identity has made many cautious about its use as standalone authentication.

Modern cybersecurity is focused on reducing the risks for this powerful security solution: traditional passwords have long been a point of weakness for security systems. Biometrics aims to answer this issue by linking proof-of-identity to our bodies and behavior patterns.

In this article, we'll explore the basics of how cybersecurity uses biometrics. To help break things down, we'll answer some common biometrics questions:

- What is the meaning of biometric?

- What is biometric data?
- What is a biometric scanner?
- What are the risks of biometric security?
- How can we make biometrics more secure?

What is Biometrics:?

For a quick biometrics definition: Biometrics are biological measurements — or physical characteristics — that can be used to identify individuals. For example, fingerprint mapping, facial recognition, and retina scans are all forms of biometric technology, but these are just the most recognized options.

Researchers claim the shape of an ear, the way someone sits and walks, unique body odors, the veins in one's hands, and even facial contortions are other unique identifiers. These traits further define biometrics.

Three Types of Biometrics Security:

While they can have other applications, biometrics have been often used in security, and you can mostly label biometrics into three groups:

1. Biological biometrics
2. Morphological biometrics
3. Behavioral biometrics

Biological biometrics use traits at a genetic and molecular level. These may include features like DNA or your blood, which might be assessed through a sample of your body's fluids.

Morphological biometrics involve the structure of your body. More physical traits like your eye, fingerprint, or the shape of your face can be mapped for use with security scanners.

Behavioral biometrics are based on patterns unique to each person. How you walk, speak, or even type on a keyboard can be an indication of your identity if these patterns are tracked.

Biometric Security Works:

Biometric identification has a growing role in our everyday security. Physical characteristics are relatively fixed and individualized — even in the case of twins. Each person's unique biometric identity can be used to replace or at least augment password systems for computers, phones, and restricted access rooms and buildings.

Once biometric data is obtained and mapped, it is then saved to be matched with future attempts at access. Most of the time, this data is encrypted and stored within the device or in a remote server.

Biometrics scanners are hardware used to capture the biometric for verification of identity. These scans match against the saved database to approve or deny access to the system.

In other words, biometric security means your body becomes the “key” to unlock your access.

Biometrics are largely used because of two major benefits:

- **Convenience of use:** Biometrics are always with you and cannot be lost or forgotten.
- **Difficult to steal or impersonate:** Biometrics can’t be stolen like a password or key can.

While these systems are not perfect, they offer tons of promise for the future of cybersecurity.

Examples of Biometric Security:

Here are some common examples of biometric security:

- Voice Recognition
- Fingerprint Scanning
- Facial Recognition
- Iris Recognition
- Heart-Rate Sensors

In practice, biometric security has already seen effective use across many industries.

Advanced biometrics are used to protect sensitive documents and valuables. Citibank already uses voice recognition, and the British bank Halifax is testing devices that monitor heartbeat to verify customers' identities. Ford is even considering putting biometric sensors in cars.

Biometrics are incorporated in e-Passports throughout the world. In the United States, e-passports have a chip that contains a digital photograph of one’s face, fingerprint, or iris, as well as technology that prevents the chip from being read — and the data skimmed — by unauthorized data readers.

As these security systems are rolled out, we are seeing the pros and cons play out in real-time.

3.10 WHAT IS IDENTITY THEFT?

Identity theft occurs when criminals steal a victim's personal information to commit criminal acts. Using this stolen information, a criminal takes over the victim's identity and conducts a range of fraudulent activities in their name.

Cyber criminals commit identity theft by using sophisticated cyber attack tactics, including social engineering, phishing, and malware. Identity theft can also result from rudimentary tactics with criminals stealing mail, digging through dumpsters, and listening in on phone conversations in public places.

The ultimate goal with many cyber attacks is to steal enough information about a victim to assume their identity to commit fraudulent activity. Unfortunately, most people only discover they're victims of identity theft when they apply for a loan, attempt to open a bank account, apply for a job, receive a call from a collection agency, or request a new credit card.

*****

UNIT II

4

DATA RECOVERY

Unit Structure

4.0 OBJECTIVES

This chapter would make you:

- Understand the concept of Data Recovery
- Methods & Techniques of backup and recovery
- Importance of backup & Solutions
- Concept of hidden data & methods to recover the hidden data

4.1 INTRODUCTION

Computer systems may crash, the files may be accidentally deleted or corrupted due to computer viruses. Disks may accidentally be reformatted. The files may be accidentally overwritten. A disgruntled employee may try to destroy your files out of revenge or for self-benefit. All of these can lead to the loss of the user's critical data. At an instance, the data is lost but with use of the latest tools and techniques the data can be recovered

but as the data cannot be found using the limited software tools available to most users. The advanced recovery tools allow us to find your files and restore them for your use. The computer forensic experts helps to recover such irreparably damaged data. In other words, Data recovery in forensic computing leads towards a new meaning that what is thrown away becomes an important component for the others which may be related to some past events.

Data Recovery:

Data recovery is the process in which highly trained engineers evaluate and extract data from damaged media and return it in an intact format. People and computer experts, fail to recognize data recovery as an option during a data crisis, but it is possible to retrieve files that have been deleted and passwords that have been forgotten or to recover entire hard drives that have been physically damaged. As we use computers for important transactions and storage functions, and more important data is stored on them. The information that is stored on computers is subjected to a virus attack, suffers damage from smoke or fire, or the drive has been immersed in water—the data recovery experts are the rescuers in such situations. For example, consider, what would happen to the productivity of your organization in the event of a system-wide data center failure? For most companies, the loss would be catastrophic. Hundreds, perhaps thousands, of employees would be rendered unproductive. Sales transactions would be impossible to complete and customer service would suffer. The cost of replacing this data would be extraordinary—if it could be replaced at all.

4.2 DATA RECOVERY AND BACKUP:

4.2.1 Data Backup:

The following are obstacles to backing up applications:

- **Backup window:** The back-up window is the period of time when back-ups can be run. The back-up window is generally timed to occur during non-production periods when network bandwidth and CPU utilization are low.

- **Network bandwidth:** If a network cannot handle the impact of transporting hundreds of gigabytes of data over a short period of time, the organization's centralized backup strategy is not viable.

- **System throughput:** Three I/O bottlenecks are commonly found in traditional backup schemes. These are:

1. The ability of the system being backed up to push data to the backup server

2. The ability of the backup server to accept data from multiple systems simultaneously

3. The available throughput of the tape device(s) onto which the data is moved

- **Lack of resources:** Many companies fail to make appropriate investments in data protection until it is too late.

4.2.2 The Future of Data Back-up:

A successful data back-up and recovery is composed of four key elements:

A. The Backup Server

B. The Network

C. The Backup Window

D. The Backup Storage Device.

A. The Back-Up Server:

- The backup server is responsible for managing the policies, schedules, media catalogs, and indexes associated with the systems it is configured to back up.

- The systems being backed up are called clients.

- The overall performance of a backup or recovery was directly related to the ability of the backup server to handle the I/O load created by the backup process.

- Tape servers allow administrators to divide the backup tasks across multiple systems while maintaining scheduling and administrative processes on a primary or backup server. This approach often involves attaching multiple tape servers to a shared tape library, which reduces the overall cost of the system.

- The new backup architecture implements a serverless backup solution that allows data to be moved directly from disk to tape, bypassing the backup server altogether. This method of data backup removes the bottleneck of the backup server completely.

- However, the performance of serverless backup is then affected by another potential bottleneck— bandwidth. A backup using a shared tape library A serverless backup system.

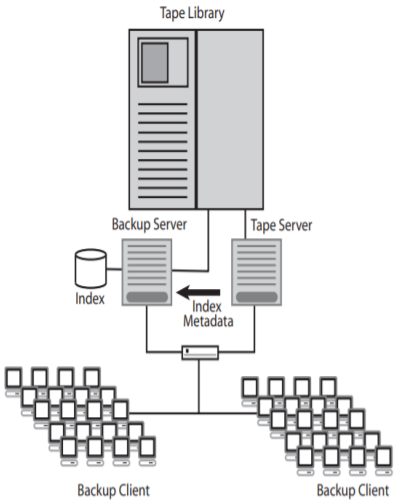


Fig.4.1: A backup using a

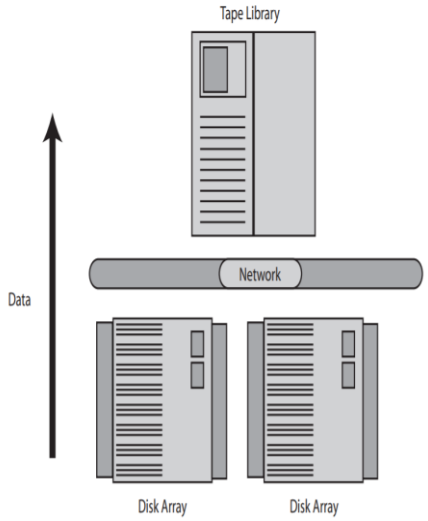


Fig.4.2: A serverless Backup

B. The Network Data Path:

- Centralization of a data-management process such as backup and recovery requires a robust and available network data path.
- The movement and management of hundreds or thousands of megabytes of data can put a strain on even the best-designed networks.
- An enterprise-class backup solution can distribute backup services directly to the data source, while at the same time centralizing the administration of these resources.
- For example, if there is a 600-gigabyte database server that needs to be backed up nightly, a tape backup device can be attached directly to that server.
- This effectively eliminates the need to move the 600-gigabyte database across the network to a centralized backup server. This approach is called a LAN-less backup, and it relies on a remote tape server capability. Figure 4.3 demonstrates how this approach is configured.

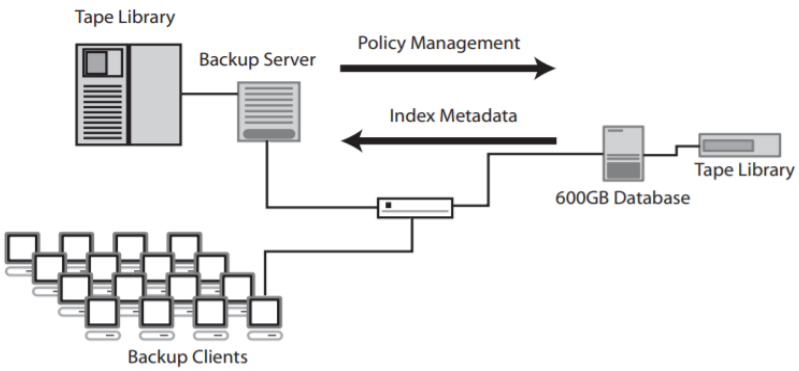


Fig.4.3: A LAN-less back-up using a remote tape server.

- We can install a network path dedicated to the management and movement of data.
- This data path can be SCSI, Ethernet, ATM, fiber distributed data interface (FDDI), or fibre channel.
- Creating a dedicated data path is the beginning of a storage area network (SAN).
- SANs are quickly dominating the backup landscape, and applications such as serverless and LAN-less backup will continue to push this emerging technology forward. Figure 4.4 shows an example of a dedicated SAN topology.

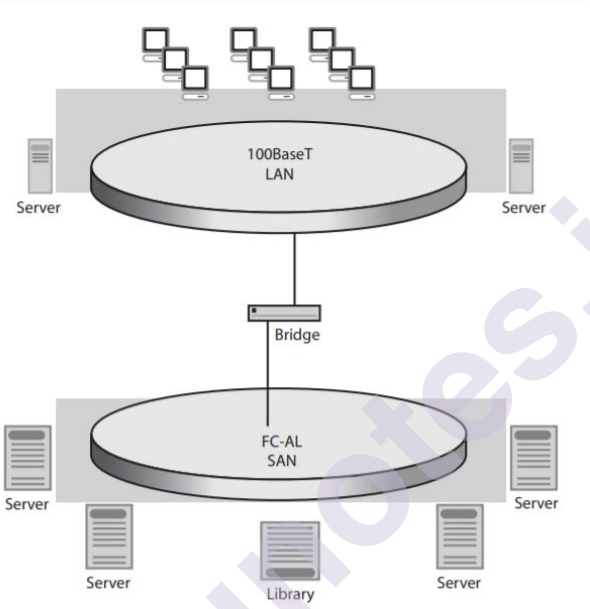


Fig.4.4: A storage area network using

C. The Backup Window:

- A backup window defines how much time is available to back up the network.
- Time plays an important role in choosing how much server, network, and resource support needs to be deployed.
- Most of the companies are managing too much data to complete backup during these ever-shrinking backup windows.
- the backup-software community has once again developed a way to overcome the element of time by using incremental backup, block-level backup, image backups, and data archiving.

Incremental Backup:

Incremental backups only transfer data that has changed since the last backup. On average, no more than 5% of data in a file server changes daily. So, an incremental backup may only require 5% of the time it takes

to back up the entire file system. Even though, a full backup had to be made regularly, or restoration of the data.

Block-Level Incremental Backup:

Block-level incremental backups provide similar benefits as incremental backups, but with even more efficiency. Rather than backing up entire files that have been modified since the last backup, only the blocks that have changed since the last backup are marked for backup. This approach can reduce the amount of incremental data requiring backup nightly by orders of magnitude.

Image Backups:

Image backups are quickly gain favour among storage administrators. This type of backup creates copies, or snapshots, of a file system at a particular point in time. Image backups are much faster than incremental backups and provide the ability to easily perform a bare bones recovery of a server without loading the operating systems, applications. It also provides specific point-in-time backups that can be done every hour rather than once a day.

Data Archiving:

Removing infrequently accessed data from a disk drive can reduce the size of a scheduled backup by up to 80%. Static data that has been archived is easily recalled when needed but does not add to the daily data backup requirements of the enterprise. This method also provides the additional benefit of freeing up existing disk space without adding required additional capacity.

D. The Backup Storage Device:

- The most expensive item in a back-up project is the back-up storage device. Determining the tape format, number of tape drives, and how many slots are required is predicted on many variables.
- For best suitable back-up storage device, the user must consider Back-up windows, growth rates, retention policies, duplicate tape copies, and network and server throughputs.
- Tape libraries are sized using two variables: the number of tape drives, the number of slots.
- Tape libraries today are available with 5 to 50,000 slots and can support anywhere from 1 to 256 tape-drives.

4.2.3 Recommended Back-Up Features:

- **Data Interleaving:** To back up multiple systems concurrently, the backup application must be able to write data from multiple clients to tape in an interleaved manner.

- **Remote Back-up:** Many remote systems are exposed to unrecoverable data loss. A backup application should have a method to back up systems across a WAN or over dial-up connections.
- **Global Monitoring:** A robust backup application should be able to support reporting and administration of any backup system, regardless of location.
- **Performance:** An enterprise backup application should be able to benchmark backup data rates exceeding one terabyte per hour.

4.3 ROLE OF BACK-UP IN DATA RECOVERY

4.3.1 Factors affecting Data Backup:

There are many factors that affect back-up like:

1. **Storage costs are decreasing:** The cost per megabyte of primary (online) storage has fallen dramatically over the past several years and continues to do so as disk drive technologies advance.
2. **Systems have to be on-line continuously:** Because systems must be continuously online, the dilemma becomes that you can no longer take files offline long enough to perform backup. Higher and higher levels of fault tolerance for the primary data repository is a growing requirement. Because systems must be continuously online
3. **The role of Back-up has changed:** The role of backup now includes the responsibility for recovering user errors and ensuring that good data has been saved and can quickly be restored because ready or mirrored data does not guard against data corruption and user error.

4.3.2 Conventional Tape Backup in Today's Market:

- A typical tape management system consists of a dedicated workstation with the front-end interfaced to the network and the back-end controlling a repository of tape devices.
- The media server runs tape management software.
- It can administer backup devices throughout an enterprise and can run continuous parallel backups and restores.
- An alternative to tape backup is to physically replicate or mirror all data and keep two copies online at all times.
- The advantage is that the data does not have to be restored, so there are no issues with immediate data availability.

4.3.3 Issues with Today's Backup:

1. **Network Backup:** It creates network performance problems. Using the production network to carry backup data, as well as for normal

user data access, can severely overburden today's busy network resources.

2. **Offline Backup:** It affects data accessibility. The time that the host is offline for data backup must be minimized. This requires extremely high-speed, continuous parallel backup of the raw image of the data.

3. **Live Backups:** It allow data access during the backup process but affect performance. The downside to the live backup is that it puts a tremendous burden on the host.

4. **Mirroring**: It doesn't protect against user error and replication of bad data. Fully replicated online data sounds great, albeit at twice the cost per megabyte of a single copy of online data.

4.3.4 New Architectures and Techniques Are Required:

- Backup at extremely high speed is required. Recovery must be available at file level. The time that systems off-line for back-up must be eliminated.
- Remote hot recovery sites are needed for immediate resumption of data access. Backup of critical data is still required to ensure against data errors and user errors.
- To achieve effective backup and recovery, the decoupling of data from its storage space is needed.
- It is necessary to develop techniques to journal modified pages, so that journaling can be invoked within the primary storage device, without host intervention.
- Part of the primary storage area must be set aside for data to be backed up. This area must be as large as the largest backup block. We should have fast non-random restoration of critical data.

4.3.5 Data Recovery Solution:

4.3.5.1 Shrinking Expertise, Growing Complexity:

- Increased availability is good, except for one fact: many systems programmers, database administrators (DBAs), and other mainframe experts are maturing.
- The complex systems that have evolved over the past 30 years must be monitored, managed, controlled, and optimized. But most of the bright young graduates this term haven't had much exposure to mainframe concepts.
- Backups often take place while an application is running. Application changes take place on the fly. If an outage occurs, the company stands to lose tens of thousands of dollars an hour.

4.3.5.2 Failures:

- Disk storage is more reliable than ever, but hardware failures are still possible. A simple mistake can be made by an application programmer, system programmer, or operations person.
- Logic errors in programs or application of the wrong update at the wrong time can result in a system crash or, worse. Disasters do really occurs! Floods, tornadoes, earthquakes, tsunamis, and even terrorism can do strike. We must be ready.

4.3.5.3 Budgets and Downtime:

We have fewer resources (people, processing power, time, and money) to do more work than ever before, and we must keep your expenses under control. Systems must remain available to make money and serve customers. Downtime is much too expensive to be tolerated.

4.3.5.4 Recovery: Think Before You Back-Up:

One of the most critical data-management tasks involves recovering data in the event of a problem. You must evaluate your preparations, make sure that all resources are available in usable condition, automate processes as much as possible, and make sure you have the right kind of resources.

- **Evaluate your preparation:** If all of the resources (image copies, change accumulations, and logs) are available at recovery time, these preparations certainly allow for a standard recovery. Finding out at recovery time that some critical resource is missing can be disastrous!
- **Don't let your resources fall through the cracks**: Identifying different types of conditions is critical to ensuring a successful recovery. Checking your assets to make sure they're ready should be part of your plan.
- **Automated Recovery**: With proper planning and automation, recovery is possible, reliance on specific personnel is reduced, and the human-error factor is nearly eliminated. Data integrity and your business relay on building recovery job control language (JCL). In the event of a disaster, the Information Management System (IMS) recovery control (RECON) data sets must be modified in preparation for the recovery. Cleaning your RECON data sets can take hours if done manually, and it's an error-prone process.
- **Make Recoveries Efficient:** Multithreading tasks shorten the recovery process. Recovering multiple databases with one pass through your log data certainly will save time. Taking image copies, rebuilding indexes, and validating pointers concurrently with the recovery process further reduce downtime.
- **Take Back-ups:** The first step to a successful recovery is the backup of your data. The user's goal in backing up data is to do so quickly, efficiently, and usually with minimal impact to your customers.

User's might need only very brief out-ages to take instant copies of your data, or you might have intelligent storage devices that allow you to take a snapshot of your data. Both methods call for tools to assist in the management of resources.

4.4 HIDING AND RECOVERING HIDDEN DATA

It is common knowledge that whatever is deleted from the computer can sometimes be brought back. Recent analysis of security implications of "alternative data streams" on Windows NT has shown that Windows NTFS filesystem allows data hiding in 206 Computer Forensics, Second Edition alternative data streams connected to files.

These data streams are not destroyed by many file wiping utilities that promise irrecoverable removal of information. Wiping the file means "securely" deleting it from disk (unlike the usual removal of file entries from directories), so that file restoration becomes extremely expensive or impossible.

If an executable erase itself, its contents can be retrieved from /proc memory image: command "cp /proc/$PID/exe /tmp/file" creates a copy of a file in /tmp.

If the file is removed by /bin/rm, its content still remains on disk, unless overwritten by other files. Several Linux unerase utilities including e2undel attempt automated recovery of files.

Overall, if recovery is attempted shortly after file removal and the partition is promptly unmounted, chances of complete recovery are high. If the system was heavily used, the probability of successful data undeletion significantly decreases.

However, if we take a look at the problem from the forensics point of view, the chances of recovering something (such as a small part of the illegal image for the prosecution) is still very high. It was reported that sometimes parts of files from several years ago are found by forensic examiners. Thus, files can be hidden in free space. If many copies of the same file are saved and then erased, the chance of getting the contents back becomes higher using the preceding recovery methods.

4.5 SUMMARY

- Data backup and recovery has become the "killer application" of storage area networking.
- The ability to move data directly from disk to tape at 400 MB/second will offer performance levels that are unprecedented by today's standards.
- SAN-based backup offers benefits such as higher availability, increased flexibility, improved reliability, lower cost, manageability, improved performance, and increased scalability.

- IT professionals face a number of challenges in today's marketplace. Whether your business is retail, health care, banking, manufacturing, public utility, government agency, or almost any other endeavour, one thing is common: your users expect more and more from your systems.
- The persistence of data, however, is remarkable. Contrary to the popular belief that it's hard to recover information, it's actually starting to appear that it's very hard to remove something even if you want to.

4.6 QUESTIONS

1. Explain Data recovery in detail.
2. Explain the Data Recovery Solutions in brief.
3. Explain Data Backup Obstacles.
4. Write short note on Backup Window.

*****

5

EVIDENCE COLLECTION

Unit Structure

5.0 OBJECTIVES

This chapter would make you:

- Understand the importance of evidence
- Identify the difficulties and describe what must be done to overcome them.

5.1 INTRODUCTION

Evidence is difficult to collect at the best of times, but when that evidence is electronic, an investigator faces some extra complexities. Electronic evidence has none of the permanence that conventional evidence has, and it is even more difficult to form into a coherent argument. The simple reason for this is that there never is one correct answer that will guide you through all investigations. No two investigations are the same, and the only thing you can ever be sure about when arriving at the scene is that there is nothing you can be sure about.

5.2 NEED TO COLLECT THE EVIDENCE

5.2.1 Why Collect Evidence?:

- Electronic evidence can be quite expensive to collect. The processes are strict and exhaustive, the systems affected may be unavailable for

regular use for a long period of time, and analysis of the data collected must be performed.

- **There are two simple reasons:**
    - **Future prevention:** Without knowing what happened, you have no hope of ever being able to stop someone else from doing it again.
    - **Responsibility: The attacker** is responsible for the damage done, and the only way to bring him to justice is with adequate evidence to prove his actions. **The victim** has a responsibility to the community. Information gathered after a compromise can be examined and used by others to prevent further attacks.

5.2.2 Evidence Collection options:

- Once a compromise has been detected, you have two options:
    - **Pull the system off the network and begin collecting evidence:** In this case you may find that you have insufficient evidence or, worse, that the attacker left a dead man switch that destroys any evidence once the system detects that its offline.
    - **Leave it online and attempt to monitor the intruder:** you may accidentally alert the intruder while monitoring and cause him to wipe his tracks any way necessary, destroying evidence as he goes.
- **For example:** If a user disconnects the system from the network, user may find that it has insufficient evidence or, worse, that the attacker left a dead man switch that destroys any evidence once the system detects that it's offline. What user choose to do should be based on the situation?

5.2.3 Obstacles:

- Electronic crime is difficult to investigate and prosecute.
- Investigators have to build their case purely on any records left after the transactions have been completed.
- Computer transactions are fast, they can be conducted from anywhere (through anywhere, to anywhere), can be encrypted or anonymous, and have no intrinsic identifying features such as handwriting and signatures to identify those responsible.
- Computer transactions are fast, they can be conducted from anywhere, can be encrypted or anonymous, and have no intrinsic identifying features such as handwriting and signatures to identify those responsible.
- Any paper trail of computer records they may leave can be easily modified or destroyed, or may be only temporary.

- Auditing programs may automatically destroy the records left when computer transactions are finished with them.
- Investigating electronic crimes will always be difficult because of the ease of altering the data and the fact that transactions may be done anonymously.
- The best we can do is to follow the rules of evidence collection and be as assiduous as possible.

5.3 TYPES OF EVIDENCES

Before collecting any evidence, it is important to know the different types of evidence categories. Without taking these into consideration, the user may find that the evidence they found spending several weeks and quite a bit of money collecting is useless. Real evidence is any evidence that speaks for itself without relying on anything else.

The following are the types of evidences:

1. **Real Evidence:** Real evidence is any evidence that speaks for itself without relying on anything else. In electronic terms, this can be a log produced by an audit function—provided that the log can be shown to be free from contamination.
2. **Testimonial Evidence:** Testimonial evidence is any evidence supplied by a witness. As long as the witness can be considered reliable, testimonial evidence can be almost as powerful as real evidence.
3. **Hearsay:** Hearsay is any evidence presented by a person who was not a direct witness. Hearsay is generally inadmissible in court and should be avoided.

5.4 RULES OF EVIDENCES

There are five rules of collecting electronic evidence. These relate to five properties that evidence must have to be useful which are:

1. Admissible
2. Authentic
3. Complete
4. Reliable
5. Believable

1. **Admissible:** Admissible is the most basic rule. The evidence must be able to be used in court or otherwise. Failure to comply with this rule is equivalent to not collecting the evidence in the first place, except the cost is higher.

2. **Authentic:** If we can't tie the evidence positively to the incident, we can't use it to prove anything. Users must be able to show that the evidence relates to the incident in a relevant way.

3. **Complete:** It's not enough to collect evidence that just shows one perspective of the incident. One should collect not only evidence that can prove the attacker's actions, but also evidence that could prove their innocence. For instance, if you can show the attacker was logged in at the time of the incident, you also need to show who else was logged in and why you think they didn't do it. This is called exculpatory evidence and is an important part of proving a case.

4. **Reliable:** The evidence you collect must be reliable. The evidence collection and analysis procedures must not cast doubt on the evidence's authenticity and veracity.

5. **Believable:** The evidence a user present should be clearly understandable and believable to a jury. There's no point presenting a binary dump of process memory if the jury has no idea what it all means. Similarly, if we present them with a formatted, human understandable version, we must be able to show the relationship to the original binary, otherwise there's no way for the jury to know whether we've faked it.

Based on the above rules, we can derive some basic do's and don'ts which are:

- **Minimize handling and corruption of original data:** Once you've created a master copy of the original data, don't touch it or the original. Any changes made to the originals will affect the outcomes of any analysis later done to copies.

- **Account for any changes and keep detailed logs of your actions:** Sometimes evidence alteration is unavoidable. In these cases, it is absolutely essential that the nature, extent, and reasons for the changes be documented.

- **Comply with the five rules of evidence:** Following these rules is essential to guaranteeing successful evidence collection.

- **Do not exceed your knowledge:** If you ever find yourself "out of your depth," either go and learn more before continuing (if time is available) or find someone who knows the territory.

- **Follow your local security policy:** If you fail to comply with your company's security policy, you may find yourself with some difficulties.

- **Capture as accurate an image of the system as possible:** Capturing an accurate image of the system is related to minimizing the handling or corruption of original data.

- **Be prepared to testify:** If you're not willing to testify to the evidence you have collected, you might as well stop before you start. No one is going to believe you if they can't replicate your actions and reach the same results.
- **Work fast:** The faster you work, the less likely the data is going to change. Volatile evidence may vanish entirely if you don't collect it in time. If multiple systems are involved, work parallel.
- **Proceed from volatile to persistent evidence:** Always try to collect the most volatile evidence first.
- **Don't shutdown before collecting evidence:** You should never, ever shutdown a system before you collect the evidence. Not only do you lose any volatile evidence, but also the attacker may have trojaned the startup and shutdown scripts, plug-and-play devices may alter the system configuration, and temporary file systems may be wiped out.
- **Don't run any programs on the affected system:** The attacker may have left trojaned programs and libraries on the system; you may inadvertently trigger something that could change or destroy the evidence you're looking for.

5.5 VOLATILE EVIDENCES

Not all the evidence on a system is lasts very long. Some evidence resides in storage that requires a consistent power supply; other evidence may be stored in information that is continuously changing. Collecting evidence, should always try to proceed from the most volatile to the least. Considering the individual circumstances, the user or individual shouldn't waste time extracting information from an unimportant or unaffected machine's main memory when an important or affected machine's secondary memory hasn't been examined. Once the user has collected the raw data from volatile sources the user may be able to shut down the system.

Always try to collect the most volatile evidence first. An example an order of volatility would be:

1. Registers and cache
2. Routing tables
3. Arp cache
4. Process table
5. Kernel statistics and modules
6. Main memory
7. Temporary file systems
8. Secondary memory

9. Router configuration
10. Network topology

5.6 GENERAL PROCEDURE OF EVIDENCE COLLECTION

1. **Identification of Evidence:** You must be able to distinguish between evidence and junk data.
2. **Preservation of Evidence:** The evidence you find must be preserved as close as possible to its original state.
3. **Analysis of Evidence:** Analysis requires in-depth knowledge of what you are looking for and how to get it.
4. **Presentation of Evidence:** The manner of presentation is important, and it must be understandable by a layman to be effective.

5.7 COLLECTION

Once we've developed a plan of attack and identified the evidence that needs to be collected:

- **Logs and Logging:** Users should run some kind of system logging function. It is important to keep these logs secure and to back them up periodically. Messages and logs from programs can be used to show what damage an attacker did.
- **Monitoring:** By monitoring the user can gather statistics, watch out for irregular, and trace where an attacker is coming from and what he is doing. Unusual activity or the sudden appearance of unknown users should be considered definite cause for closer inspection. You should display a disclaimer stating what monitoring is done when users log on.

5.7.1 Methods of Collection:

There are two basic forms of collection: **Freezing the Scene and Honeypotting.**

- **Freezing the Scene:** It involves taking a snapshot of the system in its compromised state. You should then start to collect whatever data is important onto removable non-volatile media in a standard format. All data collected should have a cryptographic message digest created, and those digests should be compared to the originals for verification.
- **Honeypotting:** It is the process of creating a replica system and luring the attacker into it for further monitoring. The placement of misleading information and the attacker's response to it is a good method for determining the attacker's motives.

5.7.2 Collection Steps:

1. **Find the Evidence:** Use a checklist. Not only does it help you to collect evidence, but it also can be used to double-check that everything you are looking for is there.
2. **Find the Relevant Data:** Once you've found the evidence, you must figure out what part of it is relevant to the case.
3. **Create an Order of Volatility:** The order of volatility for your system is a good guide and ensures that you minimize loss of uncorrupted evidence.
4. **Remove external avenues of change:** It is essential that you avoid alterations to the original data.
5. **Collect the Evidence:** Collect the evidence using the appropriate tools for the job.
6. **Document everything:** Collection procedures may be questioned later, so it is important that you document everything you do. Timestamps, digital signatures, and signed statements are all important.

5.8 SUMMARY

- Operating systems are hardened, firewalls are installed, intrusion detection systems are put in place, honeypots are implemented, security policies and procedures are established, security awareness programs are rolled out, and systems are monitored. But when unauthorized access does occur, the last line of defense is legal action against the intruder. Hence, if evidence of an intrusion is not properly handled, it becomes inadmissible in a court of law.
- It is important to remember one of the basic rules of our legal system: if there is no evidence of a crime, there is no crime in the eyes of the law. Therefore, it is of paramount importance that utmost care is taken in the collection and seizure of data evidence.
- Admissible is the most basic rule (the evidence must be able to be used in court or otherwise).
- If you can't tie the evidence positively with the incident, you can't use it to prove anything. It's not enough to collect evidence that just shows one perspective of the incident.
- You collect not only evidence that can prove the attacker's actions, but also evidence that could prove his innocence.
- The evidence collection and analysis procedures must not cast doubt on the evidence's authenticity and veracity.

- The evidence you present should be clearly understandable and believable by a jury.
- Documentation can be rough, but must be adequate in its depiction of the crime scene layout and the location of evidence.
- The search for evidence can involve looking in a variety of places, but the legalities of searching must always be considered.
- The virus protocol is a means of preventing and containing the threat to electronic evidence by computer viruses.

5.9 QUESTIONS

1. Explain the Concept of Evidence Collection.
2. Write a note on Types of Evidence.
3. Explain the Rules of Evidence.
4. Explain the Evidence Collection Steps.

*****

6

COMPUTER IMAGE VERIFICATION AND AUTHENTICATION

Unit Structure

6.0 OBJECTIVES

This chapter would make you:

- Understand the requirements of authentication of evidence
- Concepts of Digital IDs, Authenticode.

6.1 INTRODUCTION

As law enforcement and other computer forensics investigators become more familiar with handling evidential computer material, it is apparent that a number of more or less formalized procedures have evolved to maintain both the continuity and integrity of the material to be investigated. Although these procedures are extremely effective under the current rules of evidence, it is expected that alternative procedures will develop as technology advances. The current procedures, in use by both law enforcement and computer forensics investigators, work something like this:

At least two copies are taken of the evidential computer. One of these is sealed in the presence of the computer owner and then placed in secure storage. This is the master copy and it will only be opened for examination under instruction from the Court in the event of a challenge to the evidence presented after forensic analysis on the second copy.

If the computer itself has been seized and held in secure storage by law enforcement, this will constitute best evidence.

If the computer has not been seized, then the master copy becomes best evidence. In either case, the assumption is that while in secure storage,

there can be no possibility of tampering with the evidence. This does not protect the computer owner from the possibility that secured evidence may be tampered with.

6.2 SPECIAL NEEDS OF EVIDENTIAL AUTHENTICATION

- During an investigation, it is decided that evidence may reside on a computer system.
- It may be possible to seize or impound the computer system, but these risks violating the basic principle of innocent until proven guilty, by depriving an innocent party of the use of his or her system.
- It should be perfectly possible to copy all the information from the computer system in a manner that leaves the original system untouched and yet makes all contents available for forensic analysis.
- The courts may rightly insist that the copied evidence is protected from either accidental or deliberate modification and that the investigating authority should prove that this has been done. Thus, it is not the content that needs protection, but its integrity.
- **This protection takes two forms:**
    - A secure method of determining that the data has not been altered by even a single bit since the copy was taken.
    - A secure method of determining that the copy is genuinely the one taken at the time and on the computer in question.
- These elements are collectively referred as the Digital Image Verification and Authentication Protocol.

6.2.1 Digital IDS and Authentication Technology:

Without an assurance of the software's integrity, and without knowing who published the software, it's difficult for customers to know how much to trust software.

It's difficult to make the choice of downloading the software from the Internet.

For example (when using Microsoft Authenticode coupled with Digital IDs™ from VeriSign®), through the use of digital signatures, software developers are able to include information about themselves and their code with their programs.

When customers download software **signed with Authenticode** and **verified by VeriSign**, they should be assured of content source, indicating that **the software really comes from the publisher who signed it,** and content integrity, indicating that the software has not been altered or corrupted since it was signed.

6.2.2 Authenticode:

- Microsoft Authenticode allows developers to include information about themselves and their code with their programs through the use of digital signatures.
- Through Authenticode, the user is informed:
  1. Of the true identity of the publisher
  2. Of a place to find out more about the control
  3. The authenticity of the preceding information
- Users can choose to trust all subsequent downloads of software from the same publisher and all software published by commercial publishers that has been verified by VeriSign. Public Key Cryptography
- In public key cryptographic systems, every entity has two complementary keys (a public key and private key) that function only when they are held together.
- Public keys are widely distributed to users, whereas private keys are kept safe and only used by their owner.
- Any code digitally signed with the publisher's private key can only be successfully verified using the complementary public key.
- Code that successfully verified using the publisher's public key, could only have been digitally signed using the publisher's private key, and has not been tampered with.

6.2.3 Certificate Authorities:

Certification Authorities such as VeriSign are organizations that issue digital certificates to applicants whose identity, they are willing to vouch for. Each certificate is linked to the certificate of the CA that signed it.

VeriSign has the following responsibilities:

1. Publishing the criteria for granting, revoking, and managing certificates
2. Granting certificates to applications who meet the published criteria
3. Managing certificates
4. Storing VeriSign's root keys in an exceptionally secure manner
5. Verifying evidence submitted by applicants
6. Providing tools for enrolment
7. Accepting the liability associated with these responsibilities
8. Time-stamping digital signatures Digital ID

6.2.4 Digital ID:

- A Digital ID/Certificate is a form of electronic credentials for the Internet.
- A Digital ID is issued by a trusted third party to establish the identity of the ID holder.
- The third party who issues certificates is known as a Certificate Authority (CA).
- Digital ID technology is based on the theory of public key cryptography.
- The purpose of a Digital ID is to reliably link a public/private key pair with its owner.
- When a CA such as VeriSign issues a Digital IDs, it verifies that the owner is not claiming a false identity.
- When a CA issues you a digital certificate, it puts its name behind the statement that you are the rightful owner of your public/private key pair.

6.2.5 How Authenticode Works with Verisign Digital IDs:

- Authenticode relies on industry-standard cryptography techniques such as X.509 v3 or higher certificates and PKCS #7 and #10 signature standards.
- These are well-proven cryptography protocols, which ensure a robust implementation of code-signing technology.
- Developers can use the WinVerifyTrust API, on which Authenticode is based, to verify signed code in their own Win32 applications.
- Authenticode uses digital signature technology to assure users of the origin and integrity of software.
- In digital signatures, the private key generates the signature, and the corresponding public key validates it.
- To save time, the Authenticode protocols use a cryptographic digest, which is a one-way hash of the document.

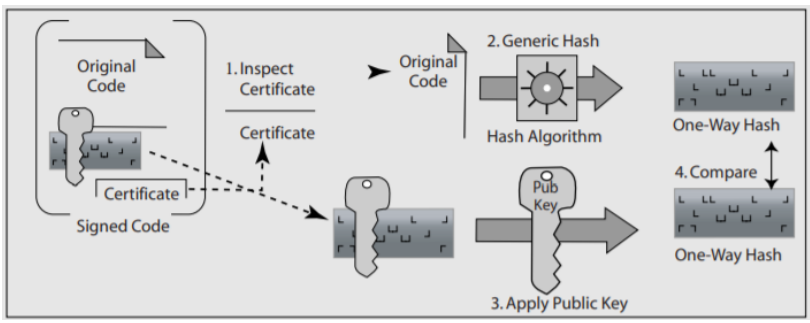


Fig.6.1: Authenticode: VeriSign Digital ID process.

1. Publisher obtains a Software Developer Digital ID from VeriSign
2. Publisher creates code
3. Using the SIGNCODE.EXE utility, the publisher o Creates a hash of the code, using an algorithm such as MD5 or SHA o Encrypts the has using his/her private key o Creates a package containing the code, the encrypted hash, and the publisher's certificate.
4. The end user encounters the package
5. The end user's browser examines the publisher's Digital ID. Using the VeriSign root Public Key, which is already embedded in Authenticode enabled applications, the end user browser verifies the authenticity of Software Developer Digital ID (which is itself signed by the VeriSign root Private Key)
6. Using the publisher's public key contained within the publisher's Digital ID, the end user browser decrypts the signed hash.
7. The end browser runs the code through the same hashing algorithm as the publisher, creating a new hash.
8. The end user browser compares the two hashes. If they are identical, the browser messages that the content has been verified by VeriSign, and the end user has the confidence that the code was signed by the publisher identified in the Digital ID, and the code hasn't been altered since it was signed.

Time Stamping:

Because key pairs are based on mathematical relationships that can theoretically be "cracked" with a great deal of time and effort, it is a well-established security principle that digital certificates should expire.

6.3 SUMMARY

Image verification and authentication security involves a relatively straightforward risk-management equation, in other words, the more security you put in place, the more onerous it is for end users), and until the technology arrives to make impenetrable security invisible to end users, it will remain that way. Most of the **Chief Information Officers** (CIOs) today clearly support increased security, and although they fault their non-IT cohorts for lack of security awareness, they appear to be realistic about the burden it puts on their companies' business units. However, CIOs aren't instituting enough of the high-profile risk-assessment measures that would increase awareness of the problem throughout their corporations.

6.4 QUESTIONS

1. Explain how Authenticode works with Verisign digital ids.
2. Explain the following:
   a. Public Key Cryptography
   b. Certificate Authorities
   c. Digital ID

*****

7

IDENTIFICATION OF DATA

Unit Structure

7.0 OBJECTIVES

This chapter would make you:

- Understand the requirements of identifying the data.
- How keeping an accurate and consistent sense of time is critical for many computer-forensic-related activities such as data identification.
- To being able to investigate incidents that involve multiple computers is much easier when the timestamps on files (identified data) and in logs are in sync.

7.1 INTRODUCTION

The Internet—friend or enemy? As the popularity of the Internet has grown at incredible rates and today it has reached into the hearts of many corporations and households worldwide. The Internet gives computer users access to a wealth of information. It is a wonderful mechanism for the exchange of e-mail communications and file attachments globally. International boundaries no longer exist when it comes to the exchange of information over the Internet. This new technology has proven to be ideal for international commerce and has the potential to be a valuable communications tool for exchange of law enforcement and government information. However, the Internet also provides the crooks with communication capabilities that did not exist previously. Through the use of a modem and with just a few clicks of a mouse, criminals can share information worldwide. It is sad but very true. Cyber crime has become a reality in our modern world. More and more, law enforcement agencies are encountering computers at crime scenes. These computers are used to store the secrets of criminals and are also used in the commission of crimes. Internet-related crimes are clearly on the rise and abuses of corporate and government Internet accounts by employees are becoming commonplace.

7.2 TIMEKEEPING

Although every computer has a clock, none of them appear to be synchronized—unless the computer in question is running the Network Time Protocol (NTP). With NTP, you can synchronize against truly accurate time sources such as the atomic clocks run by the National Institute of Standards and Technology (NIST), the U.S. Naval Observatory, or counterparts in other countries around the world.

Network Time Protocol (NTP): NTP is a protocol built on top of transmission control protocol/Internet protocol (TCP/IP) that ensures accurate local timekeeping with reference to radio, atomic, or other clocks located on the Internet. This protocol is capable of synchronizing distributed clocks within milliseconds over long periods of time.

Time Matters:

- Accurate timekeeping is an advanced science, an avocation practiced by hundreds of scientists around the world, and the paltry clock chip you have in your PC or expensive server winds up being a bit less accurate than your Swatch® watch for several reasons.
- Computer clocks, like most of the electronic clocks, detect the oscillations of a quartz crystal and calculate the passing time based on these oscillations.
- Not all quartz crystals are the same to begin with, but put one inside a nice, hot computer that's cool whenever it's turned off, and the crystal's frequency tends to wander.
- Unix systems base their notion of time on interrupts generated by the hardware clock.
- Delays in processing these interrupts cause Unix system clocks to lose time— slowly. These small changes in timekeeping are what time called as jitter.
- The time protocol provides a server's notion of time in a machine-readable format, and there's also an Internet Control Message Protocol (ICMP) timestamp message.
- The NTP software includes drivers for a large number of devices—radios that listen to time signals such as WWV, global positioning system (GPS) receivers, and even atomic clocks—that serve as references for stratum-one servers.

Clock Filters:

- Accepting another system's statement automatically about the current time can be harmful: suppose the timekeeping system has been taken over by an attacker who needs to turn back the clock so that a replay attack can function.

- NTP guards against this in several ways.
    - NTP assumes that time moves forward, not backward, although small backward changes are acceptable. Also, if a system has been using NTP, the NTP software assumes that changes in a local clock will be small, generally less than a second. This makes controlling a local clock or making large changes literally a time-consuming process—even a one-second change is a big deal.

Autokey:

- Version 4 of NTP has now entered the internet engineering task force (IETF) standards track.
- The important and interesting aspects of version 4 are the **security improvements.**
- A system called the **autokey** uses public key algorithms combined with a list of one-way hashes.
- When a client contacts an NTP server, the client can collect a certificate that contains the server's public key and independently verifies it. Then, using the enclosed public key, the client can check the signature sent by the server containing a list of key ids.
- The key ids are used with session keys to perform a quick digital signature check based on Message Digest 5 (MD5).
- Using public key cryptography for signing timestamps is just too slow. Public key encryption algorithms aren't only slow while comparing to private key algorithms such as RC4, they're inconsistent in that the amount of time used to encrypt may vary by a factor of two—something very unpleasant for those obsessed with keeping accurate time.
- Using the list of key ids reduces the need for public key encryption to once an hour on average.
- Version 4 also supports the Diffie-Hellman key exchange for peers, so that peers can exchange private session keys.
- Multicast updates of clients are also supported and use the client/server autokey for setting up security.

7.3 FORENSIC IDENTIFICATION AND ANALYSIS OF TECHNICAL SURVEILLANCE DEVICES

- It was one sentence among hundreds in a transcription of a dull congressional hearing on the environment, a statement anyone might have missed: Bristol-Myers Squibb Co. was looking to increase its harvest of the Pacific yew, a protected tree.

- The competitive intelligence (CI) officer at arch rival SmithKline Beecham Corp., happened to catch it, thanks to a routine search of competitors' activities on the Web.
- The intelligence officer sprang into action. He knew Bristol-Myers' researchers had been testing a substance in the tree's bark as an experimental agent against breast cancer. But why was Bristol-Myers suddenly seeking to cut down 200 times as many yews? Was it ready to put its planned anticancer drug, Taxol, into production? Back at SmithKline headquarters in Philadelphia, the news was enough to trigger serious nail-biting in the boardroom.
- The intelligence officer's team wasted no time. It immediately began canvassing conferences and scouring online resources for clues.
- It tapped into Web sources on the environment and got staffers to work the phones, gathering names of researchers working for Bristol-Myers.
- It even zeroed in on cities where Bristol-Myers had sponsored experimental trials of the substance.

Information Overload:

- The growing information glut makes it critical for CIOs to start thinking about how they can support their company's CI snoopsters and do it with as much zeal and imagination as they already apply to building hacker-proof security systems.
- Most existing systems and organizations are still ill-equipped to keep pace with the ever-growing amount of information available.
- Many companies are still stumbling to process and respond to competitive information as fast as it pours in.
- The result is that the key to carving out the leading edge of the knowledge gap in one's industry (the difference between what you know and what your rival knows) lies in the ability to build IT systems that can scope out the movements of corporate rivals in real time.
- IT-aided intelligence gathering is so critical that entire industries will be redefined by the companies most skilled at snooping.
- Players unable to surmount their bureaucratic inertia will find their existence threatened.
- The goal is to tie technology and business together in a common pursuit of becoming more competitive and responsive to rivals and customers in the marketplace.
- CI is to a company what radar is to an airplane. Companies are now installing radar in the corporate cockpit, and that's where the CIO comes in.

Building Teams:

- The user needs to build teams with diverse membership. People who understand the concept of organizing information and indexing it could be paired with someone who understands different technology capabilities, such as a relational database showing connections between different terms or items.
- As managers, CIOs have to amass different strengths on a CI project so they don't have an abundance of hammer holders who look only for nails. However, don't get carried away on the technology.
- A study conducted by Fuld & Company [1] found flaws with many of the 170 software packages with potential CI applications. None of them were able to take companies through the process of data identification, discovery, distribution, and analysis. Each did some part of the process, but not the whole thing. The thinking machine has not yet arrived. No company should buy a software package in the hope it will build an intelligence process for the corporation.
- CIOs need to help build that. It won't come off the shelf. In other words, in this business, you need to be aggressive. Take the offensive.
- Always recall the words of ancient Chinese general Sun Tzu (6th– 5th century B.C.): **"Be so subtle that you are invisible, be so mysterious that you are intangible; then you will control your rival's fate."**

7.5 SUMMARY

Computer forensics involves the preservation, identification, extraction, and documentation of computer evidence stored in the form of magnetically encoded information (data). Many times, the computer evidence was created transparently by the computer's operating system and without the knowledge of the computer operator. Such information may actually be hidden from view and, thus, special forensic software tools and techniques are required to preserve, identify, extract, and document the related computer evidence. It is this information that benefits law enforcement and military agencies in intelligence gathering and in the conduct of investigations. Computer forensic software tools and methods can be used to identify passwords, computer network logons, and other information that is transparently and automatically transferred from the computer's memory to floppy diskettes, Iomega Zip Disks, and computer hard disk drives. Trade secret information and other sensitive data can easily be secreted using any number of techniques. It is possible to hide diskettes within diskettes and to hide entire computer hard disk drive partitions. A deterrence-based approach as an element of an overall cyber defence strategy and the need for timely and unequivocal identification of attackers is essential for such an approach to be effective. Unfortunately, the technical basis for such identification has not received much attention from the research and development community. Until

research and development resources are committed to investigation of the relevant issues, the extent of the challenge cannot be fully understood.

7.6 QUESTIONS

1. Explain the following in brief:
    a. Autokey
    b. Building Teams
    c. Timekeeping
    d. Information Overload
2. Explain the concept of Network Time Protocol (NTP)

*****

8

RECONSTRUCTING PAST EVENTS

Unit Structure

8.0 OBJECTIVES

This chapter would make you:

- A user can be a digital detective
- Understand the how the data can be recovered from past events
- Converting the files

8.1 INTRODUCTION

The increase in computer-related crime has led to the development of special tools to recover and analyse computer data. A combination of hardware and software tools has been developed using commercial off-the-shelf utilities integrated with newly developed programs. Procedures have been defined and implemented to protect the original computer data. Processes have been developed to recover hidden, erased and password protected data. All recovery and analysis work is performed on image copies of the original. Because there is a wide variety of computers, peripherals, and software available, including many different forms of archival storage (Zip, Jaz, disk, tape, CDROM, etc.). It is important that a wide variety of equipment be available for recovery and analysis of evidence residing on a computer's hard disk and external storage media. Recovered data must be analyzed, and a coherent file must be reconstructed using advanced search programs specifically developed for this work.

For example, these techniques were recently used to recover data from several computers that indicated a large check forgery ring was in operation throughout California and personal and business identities were being stolen without the knowledge of the victims. Case files going back over five years were cleared with the information obtained.

8.2 HOW TO BECOME A DIGITAL DETECTIVE

Recovering electronic data is only the beginning. Once we recover it, we need to determine how to use it in your case. In other words, how do a user reconstruct past events to ensure that the findings will be admissible as evidence in its respective case? What follows are some recommendations for accomplishing that goal.

8.2.1 If You Need Help, Get Help:

- When a user receives the package of evidence containing a Zip disk and cover letter stating, "Enclosed and produced upon your request, please find …," user may not know what to do with the disk.
- If user don't know, get help. Help may be just down the hall.
- If we(user) have an information services department, consider going there. They might not understand what you mean by a discovery request, but they may be able to help you convert the contents of the disk to a form you can look at.
- If you have a litigation support group, consider contacting them. They may have the tools you need to look at and start working with the data you just received.
- Even if there is no formal entity within your office dedicated to dealing with technological issues, there may be informal resources.

8.2.2 Convert Digital Evidence:

- Before you can reconstruct past events and present the data, you need it on a medium and in a format, you can work with.
- In other words, you need to get the data onto a medium you can use, if it is not already on one.
- Today, data can come on a variety of media, such as holograms, video, data tapes, Zip disks, CD-ROM disks, and even 3.5-inch floppy disks.
- For example, you could use Zip disks. Zip disks are simpler. The cost of Iomega Zip drives (http://www.iomega.com/global/index.jsp) is so low that you can keep one on hand just to copy data from Zip disks you receive (and to copy data to Zip disks when others request data from you on that medium). CDs are even simpler, as CD drives have become commonplace on PCs. Similarly, even 3.5-inch disks generally pose no problem.

8.3 USEABLE FILE FORMATS

- Even if the data is in a format that appears to be one you already use, conversion still may be necessary. The format may be too new.

- The problem is a basic one. In a similar vein, you may have to get the data converted if it comes to you in a format that is too old or runs on a different operating system.
- Although simple files created with one company's software generally can be opened without a problem using a competitor's comparable product, this often does not hold true for more complex files.

8.4 UNUSEABLE FILE FORMATS

- You may get electronic data in a format that you cannot use "out of the box."
- When that happens, you have to convert the files to a format you can use—or find someone to do the conversion for you.
- You may have already encountered these issues with a variety of files including email files, database files from mainframe systems, and ".txt" files containing data dumped from database files.
- For example if you receive a ".txt" file that appears to contain information from a database file, try to find out, among other things, the make and model of the computer the file came from; the name and version of the operating system the computer ran; the name and version of the database program used; the name of the database file; a list of all fields in the database; and descriptions of each field with the descriptions including the type, length, and other characteristics of the field.

8.5 CONVERTING FILES

- If you are going to attempt converting the data yourself, you may be fortunate enough to have received electronic data that you can covert directly into programs such as Access or Excel using the wizards built into those programs.
- It can be the case with ".txt" files. Sometimes the first line in a file you are converting may even contain the names of the fields that need to be created, further simplifying your task. If that information is not in the file, then try to get the field names and descriptions from the producing party.
- Should you fail at that, you may have an exceedingly difficult time carrying out a meaningful conversion.
  - ✓ Get the Right Software, Hardware, and Personnel
  - ✓ Did You Get All the Data?
  - ✓ Did the Evidence Come from the People You Thought It Would?
  - ✓ Look for "Hidden" Data

- ✓ Test the Data
- ✓ Work the Evidence

Get the Right Software, Hardware, and Personnel:

- The user should be associated or linked to get the data into a useable format and getting the right software, hardware, and personnel to work with the format the user choose. Hardware requirements will vary greatly depending on specific circumstances. Personnel requirements present the greatest challenge.
- If the user are going to make sense of the electronic data they have received, converted, and loaded, the user must need know how to use the tools themselves, or, failing that, rely on someone who can use the tools for you.

Did You Get All the Data?:

- To Check whether user has received all the data they should receive. Prepare an inventory of what user received and compare it against what user requested. This may be as simple as preparing and comparing lists of file names.
- It will require that user to develop short descriptions of the data the user received and then match the descriptions with user's discovery requests. It may even mean you will have to closely analyze the data to see whether gaps emerge that indicate some failure to produce all that it ought to have produced.
- Users also can search the electronic data for references to electronic files that should have been given to you but were not. This can be done through a manual review. The manual review can be enhanced if the software you are using to review the data allows you to search for strings of characters.
- If it does, you can search for filename extensions that are typically associated with the types of files you want to find.
- Examples include .doc, .htm, .html, .htx, .rtf, .mcw, .txt, .wps, and .wpd for word processing files; .csv, .dbf, .dif, .txt, .wk1, .wk3, .wk4, .wks, .wq1, .xls, and .xlw for spreadsheet files; and .asc, .csv, .dbe, .dbf, .htm, .html, .mda, .mdb, .mde, .mdw, .tab, .txt, and .xls for database files.
- If the user receives spreadsheet or database files in their native format, the user can scrutinize them for signs of links to files that were used in connection with the files you got but that were not given to you.
- In a spreadsheet file such as an Excel file, this might mean searching the cells for extensions such as the ones previously listed. It also can mean checking the "properties." If you are asked whether you want to re-establish a link when you open the file, that is a clear sign of

potentially missing files; keep track of the file names and check to see whether you received them.

- In a database file such as an Access file, this means closely examining all tables, queries, forms, reports, macros, and modules for references to other files.

Did the Evidence Come from the People You Thought It Would?:

Files often contain indications of who created them, who worked on them, and who last saved them. If you go to File | Properties, you can sometimes find this information.

Look for "Hidden" Data:

- Electronic files often contain "hidden" data (information that does not show up on any printouts of the file) that can potentially prove useful.
- You should go to File | Properties, where you may be able to find out a host of details about the file that the people sending it to you may never have known went with it.
- These can include when the file was created; when it was last modified; who created it; what comments have been added; what title was given to the file; whether intentionally or automatically, which subjects have been assigned to the file; who last saved the file; and how many revisions the file has gone through.

Test the Data:

- Test the electronic data to determine how complete, accurate, and reliable it is. You can test the data against itself.
- Look for inconsistencies.
- Look for errors as well.
- Where feasible, the electronic data can be compared to underlying documents, again to determine the completeness, accuracy, and reliability of the data. This comparison can highlight coding errors made when creating the database such as wrong numbers, dates, and names.
- It also can reveal categories of information that were not added to the electronic data, which if they had been added, would have affected the results of searching the data.
- Just as electronic data can be compared to underlying documents, so also can it be compared to data in other electronic files, the contents of other documents, and information available through the Internet.

Work the Evidence:

- What one can do with data really is limited more by one's imagination than anything else. That said, there are several general recommendations that can be offered: Put the data into tools you can use.

- Spreadsheet programs can allow one to perform calculations, prepare pivot tables that can quickly summarize data across several dimensions, develop charts to graphically present trends in the data, and map out information geographically.

- Database programs can permit one to search or query the databases in complex and subtle ways, perform calculations, and generate a broad range of reports.

- Sharing the data we receive and the knowledge you glean from it to reconstruct past events with your client, experts, and other colleagues, as appropriate, can offer you the opportunity to more effectively handle our case.

8.6 SUMMARY

Once the data has been successfully collected, it must be analyzed to extract the evidence the user wish to present and to rebuild what actually happened. We must make sure that the user or ourselves fully document everything whatever they do; the work will be questioned and the user must be able to show that its results are consistently obtainable from the procedures you performed. Logging utilities are vital for forensics when reconstructing the sequence of events leading up to, during, and after an attack, provided the attacker doesn't delete the log files. Refining the firewall rules, keeping the intrusion detection systems (IDSs) current, and reviewing the log files will be important to stay one step ahead of the bad guys.

8.7 QUESTIONS

1. Explain in your words that Recovering electronic data is only the beginning.

2. Explain the Converting Files & its important aspects in brief.

3. Explain How to become a digital detective?

*****

UNIT III

9

NETWORK FORENSICS AND EVIDENCE ACQUISITION

Unit Structure

9.1 OVERVIEW

After studying this chapter, the learner should be able to:

- Understand some technical knowledge about sources such as routers, web proxies, intrusion detection systems, etc.
- Understand common classes of network devices
- Understand concept of protocols and the OSI model
- Understand Internet Protocol Suite and key features of IPv4, IPv6, TCP, and UDP
- Understand potential criminal activities' sources of evidence in a forensic investigation
- Know different traffic acquisition software
- Check how to conduct active acquisition

9.2 INTRODUCTION

With the tremendous rise in use of technological devices in daily life, the production of the network-based evidence has become an important necessity in most cases for the purpose of establishing accused as guilty or for imposing liability on defendant. The fluctuation or swing in judicial mindset has occurred mostly in recent past and most legal systems across the world have amended their laws to accommodate such change.

Regarding computer forensics, this chapter primarily focuses on fundamental skills necessary to develop and implement security schemes designed to protect organizations' information from attacks. Network investigators must always be ready to learn and adapt. From wires to routers to web proxies to DNS servers, there are innumerable potential sources of network-based evidence. Although most environments are built from the same general types of network devices, there exists a wide variety of equipment, software, and protocols that are constantly changing. This chapter also discusses types of physical media that can be leveraged to passively acquire network-based evidence and explore popular tools and techniques for acquiring network traffic.

9.3 SOURCES OF NETWORK BASED EVIDENCE

9.3.1 On the Wire:

On the wire is a physical cabling that carries data over the network. Network forensic investigators can tap into such cabling to copy and preserve network traffic as it is transmitted across the line. A wiretapping can provide real-time network data. Taps can range from "vampire" taps, which literally puncture the insulation and contact copper wires, to surreptitious fiber taps, which bend the cable and cut the sheathing to reveal the light signals as they traverse the glass. Many commercial vendors also manufacture infrastructure taps, which can plug into common cable connectors and are specifically designed to replicate signals to a passive station without degrading the original signal.

9.3.2 In the Air:

Investigators can gather a lot of information from encrypted wireless networks. Although data packets that traverse a wireless network may be encrypted, commonly management and control frames are not. In the clear, wireless access points advertise their names, presence, and capabilities; stations probe for access points; a MAC addresses of legitimate authenticated stations, unauthenticated stations and suspicious stations that may be attacking the wireless network. Investigators can also conduct volume-based statistical traffic analysis and analyze these patterns. With access to unencrypted or decrypted wireless traffic, of course, investigators can review the full packet captures in detail

9.3.3 Switches:

Packet sniffing is a technique in which attackers surreptitiously insert a software program at remote network switches or host computers. The program monitors information packets as they are sent through networks and sends a copy of the information retrieved to the hacker. By picking up the first 125 keystrokes of a connection, attackers can learn passwords and user identifications, which, in turn, they can use to break into systems. Switches contain a "content addressable memory" (CAM) table, which stores mappings between physical ports and each network card's MAC address. Given a specific device's MAC address, network investigators can examine the switch to determine the corresponding physical port, and potentially trace that to a wall jack and a connected station. Switches also provide a platform from which investigators can capture and preserve network traffic. With many types of switches, network staff can configure one port to "mirror" (copy) traffic from any or all other ports or VLANs, allowing investigators to capture traffic from the mirroring port with a packet sniffer.

9.3.4 Routers:

Nowadays, intelligent defenses against attacks such as denial-of-service attacks could be found, as routers and other devices can be set to verify source addresses and ignore packets if they are bogus or carry a suspicious

pattern. However, beyond the denial-of-service category of vulnerabilities, there are always the standard concerns of open ports, easy passwords, unsecured routers, and unknown "features" that any Internet device may have. Routers have routing tables which map ports on the router to the networks that they connect. This allows a forensic investigator to trace the path that network traffic takes to traverse multiple networks. Depending on the specific device's capabilities, routers may also function as packet filters, denying the transmission of certain types of traffic based on source, destination, or port. Routers may log denied traffic (or sometimes maintain statistics on allowed traffic). One of the primary logs used in computer forensics is syslog, the main system log containing a variety of important messages. This is no secret to hackers, and hence is often one of the first logs to be modified. In addition, routers and firewalls can be configured to add messages to the syslog. Many enterprise-class routers can be configured to send logs and flow record data to a central logging server, which is extremely helpful for investigators, as this makes it very easy to correlate events from multiple sources. Logs stored on the router itself may be volatile and subject to erasure if the device is rebooted or if the available storage is exceeded.

9.3.5 DHCP Servers:

When virtually all private connections to the Internet were made over modems connecting to a dynamic host configuration protocol (DHCP) server where each session was served with a different IP address, it was much less likely that a private machine would be compromised and efforts to compromise machines tended to be focused on commercial, government, and educational systems. Frequently, investigations begin with the IP address of a host that is suspected of being involved in some sort of adverse event—whether it was victim of an attack, origin, or perhaps both. One of the first tasks investigator must undertake is to identify and/or physically locate the device based on its IP address.

When DHCP servers assign (or "lease") IP addresses, they typically create log of the event, which includes the assigned IP address, the MAC address of the device receiving the IP address, and the time the lease was provided or renewed. Other details, such as the requesting system's hostname, may be logged as well. Consequently, DHCP logs can show an investigator exactly which physical network card was assigned the IP address in question during specified time frame.

9.3.6 Name Servers:

DNS servers can be configured to log queries for IP address and hostname resolutions. These queries can be very revealing. For example, if a user on an internal desktop, browses to a web site, the user's desktop will make a DNS query to resolve the host and domain names of the web server prior to retrieving the web page. As a result, the DNS server may contain logs that reveal connection attempts from internal to external systems, including web sites, SSH servers, external email servers, and more. DNS servers can log not only queries, but also the corresponding times.

Therefore, forensic investigators can leverage DNS logs to build timeline of suspect's activities.

9.3.7 Authentication Servers:

Applications and transaction systems ideally request a centralized authentication server to confirm or deny a user's identity. Authentication servers typically log successful and/or failed login attempts and other related events. Investigators can analyze authentication logs to identify brute-force password-guessing attacks, account logins at suspicious hours or unusual locations, or unexpected privileged logins, which may indicate questionable activities.

Unlike analysis of authentication logs on a single hard drive, a central authentication server can provide authentication event information about all devices within an entire authentication domain, including desktops, servers, network devices, and more.

9.3.8 Network Intrusion Detection / Prevention Systems:

Data communication analysis typically includes network intrusion detection, data preservation, and event reconstruction. At a high level, forensic value of a network intrusion detection systems / network intrusion detection systems NIDS/NIPS is designed to provide timely data pertaining to adverse events on the network. This includes attacks in progress, command-and-control traffic involving systems already compromised, or even simple misconfigurations of stations. The value of this data provided by NIDS/NIPS is highly dependent upon the capabilities of the device deployed and its configuration. With many devices, it is possible to recover the entire contents of the network packet or packets that triggered an alert. However, data that is preserved contains little more than source and destination IP addresses, TCP/UDP ports, and time event occurred. During an ongoing investigation, investigators can request that network staff tune NIDS to gather more granular data for specific events of interest or specific sources and destinations.

9.3.9 Firewalls:

Firewalls are a basic means for providing network security, acting like the moat around a medieval castle, by restricting information to enter and leave at carefully controlled points and preventing unacceptable attempts at accessing resources within the firewall. Event logging was of secondary importance for firewall manufacturers. Firewalls were not initially designed to alert security personnel when security violations were taking place, even though they were most definitely designed to implement security policies to prevent violations. Today, modern firewalls have granular logging capabilities and can function as both infrastructure protection devices and useful IDSs as well. All the traffic going through a firewall is part of a connection. A connection consists of the pair of IP addresses that are talking to each other, as well a pair of port numbers that identify the protocol or service. The destination port number of the first packet often indicates the type of service being connected to.

When a firewall blocks a connection, it will save the destination port number to its log file. These logs can help operators manage the network as also serve as evidence for forensic analysts. A common question is how intrusion detection complements firewalls. One way of characterizing the difference is provided by classifying security violations by source—whether they come from outside the organization's network or from within. Firewalls act as a barrier between corporate (internal) networks and the outside world (Internet) and filter incoming traffic according to a security policy. This is a valuable function and would be sufficient protection were it not for these facts:

- Not all access to the Internet occurs through the firewall.
- Not all threat originates outside the firewall.
- Firewalls are subject to attack themselves

9.3.10 Web Proxies:

Web proxies can be a gold mine for forensic investigators, especially when they are configured to retain granular logs for an extended period. Whereas forensic analysis of a single hard drive can produce the web surfing history for users of a single device, an enterprise web proxy can literally store the web surfing logs for an entire organization. There are many commercial and free applications that can interpret web proxy logs and provide visual reports of web surfing patterns according to client IP address or even username (i.e., when correlated with Active Directory logs). This can help forensic analysts gather lists of users who may have succumbed to a phishing email, investigate a roving user's inappropriate web surfing habits, or identify the source of web-based malware. If the web proxy is configured to cache web pages, it is even possible to retrieve the content that an end-user viewed or carve malware out of a cached web page for further analysis. It is advisable to find a Web proxy or gateway website for conducting any type of intelligence collection operation against the attacking host

9.3.11 Application Servers:

There are many kinds of application servers for us to review in depth However, keep in mind that there are many possible sources of network-based evidence. Review local network diagrams and application documentation to identify the sources that will be most useful for your investigation.

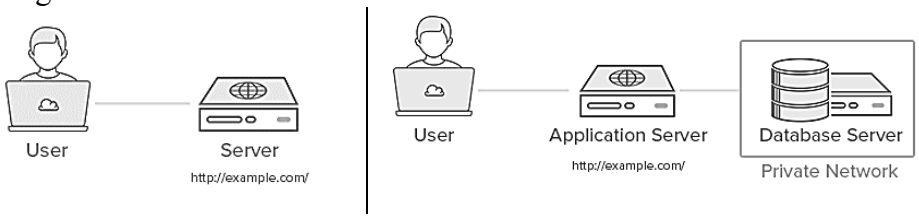


Figure 1.1: Direct connection to server vis-à-vis connection via application server (Creative Commons image

source: https://www.digitalocean.com/community/tutorials/5-common-server-setups-for-your-web-application)

9.3.12 Central Log Servers:

Much like intrusion detection systems, central log servers are designed to help security professionals identify and respond to network security incidents. Even if an individual server is compromised, logs originating from it may remain intact on the central log server.

Furthermore, devices such as routers, which typically have very limited storage space, may retain logs for very short periods of time, but the same logs may be sent in real time to a central log server and preserved for months or years. Some organizations use commercial log analysis products that can provide forensic analysts with complex reports and graphical representations of log data, correlated across a variety of sources.

9.4 PRINCIPLES OF INTERNETWORKING

9.4.1 Protocols:

Protocols can be defined as set of formal rules describing how to transmit data, especially across a network. Protocols take on new meaning when viewed in the context of forensic investigation. Attackers bend and break protocols to smuggle covert data, sneak past firewalls, bypass authentication, and conduct widespread denial-of-service (DoS) attacks.

While network designers and engineers view protocols as rules for facilitating communication between stations, forensic investigators must view them as guidelines that attackers can leverage to get results.

9.4.2 Open Systems Interconnection Model:

The Open Systems Interconnection (OSI) Model was designed by the International Organization for Standardization (ISO) to provide network architects, software engineers, and equipment manufacturers with a modular and flexible framework for development of communications systems.

When data is transmitted across a network, output from one layer is encapsulated with data designed for use by the lower layer processes. Conversely, when data is received by the destination host, input from each layer is demultiplexed for use by the higher layer processes.

Layer 7. Application
Layer 6. Presentation
Layer 5. Session
Layer 4. Transport
Layer 3. Network
Layer 2. Data Link
Layer 1. Physical

Table 1.1 Layers in the OSI model

9.5 INTERNET PROTOCOL SUITE

Background:

The Internet Protocol Suite, also known as the TCP/IP protocol suite, is a collection of protocols that are used to implement important functions on the Internet and in many other packet-switched networks.

The original 1974 "Specification of Internet Transmission Control Program" stated: "Processes are viewed as the active elements of all HOST computers in a network. Even terminals and files or other I/O media are viewed as communicating through the use of processes. Thus, all network communication is viewed as inter-process communication. Since a process may need to distinguish among several communication streams between itself and another process [or processes], we imagine that each process may have a number of PORTs through which it communicates with the ports of other processes. Since port names are selected independently by each operating system, [TCP/IP], or user, they may not be unique. To provide for unique names at each [TCP/IP], we concatenate a NETWORK identifier, and a [TCP/IP] identifier with a port name to create a SOCKET name which will be unique throughout all networks connected together."

Thereafter, work emerged on the Draft Internetwork Protocol Specification, which was eventually published as RFC 791, "Internet Protocol" in September 1981. TCP was revised to excise the network layer functions, and was also published in September 1981 as RFC 793, "Transmission Control Program."

9.5.1 Internet Protocol (IP):

The Internet Protocol (IP) is designed to handle addressing and routing. It includes a method for uniquely identifying source and destination systems on a network (the "IP address") and provides support for routing data through networks. IP operates at Layer 3 of the OSI model (the network layer). It is a connectionless protocol, meaning that it does not explicitly identify individual packets as being part of a related series, and therefore also does not have a method for indicating the initiation or closing of a conversation. There have been several versions of IP. The most widely deployed version is IPv4, which was officially standardized in 1981 and first deployed on January 1, 1983. During the past thirty years, IPv4 has become globally supported. However, work has continued on IP development, fueled primarily by concerns about address space exhaustion. In 1998, the specification for Internet Protocol version 6 (IPv6) was released, and support for it is increasing, slowly but surely. Characteristics of IP include:

- Support for addressing and routing
- Connectionless

- Unreliable
- Includes a header (no footer)
- Header plus payload is called an IP packet

IPv4: IPv4 uses a 32-bit address space to identify the source and destination systems. Typically, human-readable IP addresses are divided into four octets, separated by periods, and written in decimal. Each octet has 28 possible values, ranging from 0 to 255.

IPv6: IPv6 protocol was developed with 128 bits for each of the source and destination addresses. There are approximately 2^{128}, or 340 undecillion possible IP addresses. Human-readable IPv6 addresses are written in hexadecimal and are divided into 08 groups of 16 bits each.

The key changes introduced in IPv6 compared with IPv4 can be summarized as follows:

- Larger address space (128 bits)
- No packet header checksums
- Fixed-length IP packet header
- Designed to interoperate with IPSEC

9.5.2 Transmission Control Protocol (TCP):

TCP is a connection-oriented protocol. It indicates the state of transmissions using flags in the TCP header. TCP uses three steps to establish a reliable bidirectional communication between stations. First, the initiating station sends a segment with the SYN flag set. Next, the responder sends back a segment with the "SYN" and "ACK" flags set. Finally, the initiator responds with a segment that has an "ACK" flag set. This initiation sequence is referred to as the three-way handshake. There is also a corresponding two-step sequence for closing a connection using the "FIN" and "ACK" flags.

Key characteristics of the TCP protocol include:

- Reliable
- Connection-oriented
- Handles sequencing
- Port numbers range from 0 to 65535
- Includes a header (no footer)
- Header plus payload is called a TCP segment

The Transmission Control Protocol (TCP) is designed to handle multiplexing of process communications on the host, as well as reliability

and sequencing. The combination of the TCP header and the encapsulated payload together is referred to as a TCP segment. As with IP, there is no footer. To communicate, a process encapsulates data in a TCP segment header for transmission to another process, possibly on a remote system (in which case the segment would subsequently be encapsulated in an IP packet for transmission across the network and demultiplexed at the receiving end).

9.5.3 User Datagram Protocol (UDP):

The User Datagram Protocol (UDP) is designed to facilitate multiplexing of process communications on the host, without any of the reliability, sequencing, connection setup and teardown, or any of the frills of TCP. This is useful for some applications, such as real-time data streaming (Voice over IP, music, or videos). For these applications, there is no point in attempting to detect if packets arrive out of order or are dropped because the real-time requirements leave no room for retransmission.

It is better to simply drop datagrams when errors occur than to slow down the entire transmission with transport-layer error checking. Like TCP, the UDP header includes 16-byte fields for "source port" and "destination port." The possible values for UDP ports range from 0 to 65,535. Key characteristics of the UDP protocol include:

- Unreliable
- Connectionless
- Port numbers range from 0 to 65535
- Includes a header (no footer)
- Header plus payload is called a UDP datagram

9.6 EVIDENCE ACQUISITION: PHYSICAL INTERCEPTION

Network forensic investigators often refer to "passive" versus "active" evidence acquisition. Passive evidence acquisition is the practice of gathering forensic-quality evidence from networks without emitting data at Layer 2 and above. Traffic acquisition is often classified as passive evidence acquisition.

Active or interactive evidence acquisition is the practice of collecting evidence by interacting with stations on the network. This may include logging onto network devices via the console or through a network interface, or even scanning the network ports to determine current state.

9.6.1 Cables:

Telecommunications equipment can be highly vulnerable, because of the presence of lengthy copper cables between devices. Cables allow for point-to-point connections between stations. The most common materials

for cables are copper and fiber. Each of these can be sniffed, although the equipment and side effects vary based on the physical media. The two most widely used types of copper cabling used in the modern era are coaxial cable and twisted pair. Fiber optic cables consist of thin strands of glass (or sometimes plastic) which are bundled together to transmit signals across a distance. Light is transmitted into the fiber at one end and travels along an optic fiber, reflecting constantly against the walls until it reaches an optical receiver at the other end.

What concerns is vulnerability due to increased use of communications and data communications schemes based on copper cable media. If the copper media were to be replaced with optical fiber to achieve higher bandwidths, the communications infrastructure would become more robust against electromagnetic attack

Intercepting Traffic in Cables:

There are variety of tools available for intercepting traffic in cables, including inline network taps, "vampire" taps, induction coils, and fiber optic taps. General details of the same is mentioned below:

- **Inline Network Taps**: An inline network tap is a Layer 1 device, which can be inserted in-line between two physically connected network devices. The network tap will pass along the packets as also physically replicate copies to a separate port (or multiple ports). Network taps commonly have four ports: two connected inline to facilitate normal traffic, and two sniffing ports, which mirror that traffic (one for each direction). Insertion of an inline network tap typically causes a brief disruption, since the cable must be separated to connect the network tap inline. Network taps are commonly designed to require no power for passively passing packets thereby reducing the risk of a network outage.

- **Vampire Taps:** "Vampire taps" are devices that pierce the shielding of copper wires to provide access to the signal within. Unlike inline network taps, the cable does not need to be severed for a vampire tap to be installed. However, investigators should take caution: As noted by security researcher Erik Hjelmvik, "[i]nserting a vampire tap, even if done correctly, can bring down the link on a TP cable since the characteristics of the required balanced communication will be affected negatively.".

- **Induction Coils**: Induction coils transform the magnetism of weak signals to induce a much stronger signal in an external system. Such a device could potentially capture the throughput of a cable without the detection of the users, administrators, or owners of the wires. However, such devices are not commercially available in a way that the public can acquire to surreptitiously tap Cat5e and Cat6.

- **Fiber Optic Taps:** Inline network taps work similarly for fiber optic cables and copper cables. To place a network tap inline on a fiber optic cable, network technicians splice the optic cable and connect it to each port of a tap. This causes a network disruption. Inline optical

taps may cause noticeable signal degradation. Network engineers often use tools called optical time-domain reflectometers (OTDR) to analyze and troubleshoot fiber optic cable signals. OTDRs can also be used to locate breaks in the cable, including splices inserted for taps. With OTDRs, technicians can create a baseline of the normal signal profile of a fiber optic cable, and potentially detect not only when the profile changes but where on the cable the disruption has likely occurred.

9.6.2 Radio Frequency:

Radio frequency is a popular medium for transmission of packetized data and Internet connectivity. The Institute of Electrical and Electronics Engineers (IEEE) published a series of international standards ("802.11") for wireless local area network (WLAN) communication. These standards specify protocols for WLAN traffic in the 2.4, 3.7, and 5 GHz frequency ranges. The term "Wi-Fi" is used to refer to certain types of RF traffic, which include the IEEE 802.11 standards.

IEEE 802.11 is the most common wireless protocol beyond debate. It is being used in almost every part of our lives, from home security systems to cell phones, on a wide variety of devices and diverse application domains. Naturally, this widespread usage is subject to criminal activity. It is possible to passively capture encrypted Wi-Fi traffic and decrypt it offline later using the encryption keys. Once an investigator has gained full access to unencrypted 802.11x traffic contents, this data can be analyzed in the same manner as any other unencrypted network traffic. Regardless of whether Wi-Fi traffic is encrypted, investigators can gain a great deal of information by capturing and analyzing 802.11 management traffic. This information commonly includes:

- Broadcast SSIDs (and sometimes even non-broadcast ones)
- WAP MAC addresses
- Supported encryption/authentication algorithms
- Associated client MAC addresses
- In many cases, the full Layer 3+ packet contents

There are commercially available 802.11 network adapters that are specifically designed for capturing packets. These adapters include very handy features for forensic investigators, such as the ability to operate completely passively (so the investigator does not have to worry about accidentally transmitting data), connectors for extra antennae, and portable form factors such as USB.

9.6.3 Hubs:

A network hub is a Layer 1 device that physically connects all stations on a local subnet to one circuit. A hub does not store enough state to track what is connected to it, or how. It maintains no knowledge of what devices

are connected to what ports. Investigators must be careful when using hubs as traffic capture devices. The investigator sees all traffic on the segment, but so can everyone else. A compromised system could trivially act as a passive listener and eavesdrop on any data transfers or communications. Any evidence transmitted across the network, or normal traffic sent by the investigator's operating system, may be trivially captured by anyone else on the local network. It may be appropriate to take advantage of a hub that is already installed on a network but installing a hub for the purposes of traffic capture can introduce new risks.

9.6.4 Switches:

Switches operate at Layer 2 (datalink), and sometimes Layer 3 (network). Switches populate CAM table by listening to arriving traffic. When a switch receives a frame from a device, it looks at the source MAC address and remembers the port associated with that MAC address. Later, when the switch receives a packet destined for that device, it looks up the MAC address and corresponding port in the CAM table. It then sends the packet only to appropriate port, encapsulated with the correct Layer 2 Ethernet address. In this way, a switch segments the traffic endpoint-by-endpoint, even while technically sharing the same physical medium. One can capture network traffic using switches.

Even though by default switches only send traffic to the destination port indicated in the frame, switches with sufficient software capabilities can be configured to replicate traffic from one or more ports to some other port for aggregation and analysis. Different vendors have different terminology for this capability - a common term is Cisco's Switched Port Analyzer (SPAN) and Remote Switched Port Analyzer (RSPAN). The most vendor-neutral term for this is "port mirroring."

The safest way to obtain traffic from a switch is to coordinate with a network administrator to configure "port mirroring," in which traffic from ports of interest is mirrored to a port that is used by the investigator. Switches can also be attacked in several ways to try to facilitate sniffing. The most common are MAC flooding (which attacks the switch's CAM table directly) and ARP spoofing (which attacks the ARP tables of the hosts on the LAN). These are methods for facilitating traffic capture on switched networks when port mirroring or tapping a cable is not an option

9.7 TRAFFIC ACQUISITION SOFTWARE

9.7.1 Libpcap and WinPcap

The most common software libraries used for recording, parsing, and analyzing captured packet data are libpcap and WinPcap. Both libpcap and WinPcap are free software released under the "BSD license," which has been approved by the Open-Source Initiative. Libpcap is a UNIX C library that provides an API for capturing and filtering data link layer frames from arbitrary network interfaces. It was originally developed at the Lawrence Berkeley National Laboratory (LBNL), and initially released to the public

in June 1994. In 1999, the Computer Networks Group (NetGroup) in the Politecnico di Torino published WinPcap, a library based on libpcap that was designed for Windows systems. Since then, many people and companies have contributed to the WinPcap project. The code is hosted at a site maintained by Riverbed Technology. WinPcap has been the packet capture and filtering engine for many open source and commercial network tools, including protocol analyzers, network monitors, network intrusion detection systems, sniffers, traffic generators and network testers. Some of these networking tools, like Wireshark, Nmap, Snort, and ntop are known and used throughout the networking community.

Details of Libpcap is available on official website https://www.tcpdump.org/. Details of WinPcap is available on official website https://www.winpcap.org/

9.7.2 The Berkeley Packet Filter (BPF) Language:

Libpcap includes a filtering language called the "Berkeley Packet Filter" (BPF) syntax. Using BPF filters, one can decide which traffic to capture and inspect and which traffic to ignore. BPF filters traffic basis value comparisons in fields for Layer 2, 3, and 4 protocols. It includes built-in references called "primitives" for many commonly used protocol fields. BPF invocations can be extremely simple, constructed from primitives such as "host" and "port" specifications, or very arcane constructions involving specific field values by offset. BPF filters can also consist of elaborate conditional chains, nesting logical ANDs and ORs. Some commonly used BPF primitives include:

- host id, dst host id, src host id
- net id, dst net id, src net id
- ether host id, ether dst host id, ether src host id
- port id, dst port id, src port id
- gateway id, ip proto id, ether proto id
- tcp, udp, icmp, arp
- vlan id

9.7.3 Tcpdump:

Tcpdump is a tool for capturing, filtering, and analyzing network traffic. It was developed at Lawrence Berkeley National Laboratory (LBNL), and first released to the public in January 1991. There are two ways that tcpdump is most employed. First, it is used to facilitate on-the-fly analysis for troubleshooting network issues in a tactical way. This typically encompasses capture, filtering, and analysis, all performed simultaneously. However, it tends to be suitable only when a quick glance at the data will suffice. Tcpdump is also frequently used to capture traffic of interest passing on a target segment over a longer period and store it for

offline analysis and perhaps even future correlation with other data. Depending on throughput and utilization of network segment and amount of each packet retained, the volume of data captured can be enormous.

One reason that tcpdump is a powerful tool is it can capture traffic with high fidelity, to the degree that resulting packet capture can constitute evidence admissible in court. However, quality of packet capture can be impacted by hardware limitations and configuration constraints. One crucial configuration option for capturing packets using tcpdump is the snapshot length, known as "snaplen." Snaplen represents the number of bytes of each frame that tcpdump will record. It is calculated from the zero-byte offset of the data link-layer frame.

Filtering during capture is very important because resources such as disk space, CPU cycles, and traffic aggregation capacity are always limited. Filtering indiscriminately, however, can cause loss of evidence, which can never be recaptured. You only get one chance to capture a frame now it zips past on wire (or through air).

Below are five common invocations of tcpdump, which illustrate some of the basic functionality:

- **tcpdump -i eth0 -w great_big_packet_dump.pcap**

This is the case of listening on interface eth0 and writing all the packets out to a single monolithic file.

- **tcpdump -i eth0 -s 0 -w biggest_possible_packet_dump.pcap**

This instance is like the one above, except that by setting the snaplength to zero, we are telling tcpdump to grab the entire frame regardless of its size (rather than the first 68 bytes only). (Note that specifying -s 0 is not necessary for newer versions of tcpdump, because the command functionality was updated to make this behavior default.)

- **tcpdump -i eth0 -s 0 -w targeted_full_packet_dump.pcap 'host 10.10.10.10'**

A BPF filter to grab and store in their entirety only those packets sent to or from the host at the address "10.10.10.10."

- **tcpdump -i eth0 -s 0 -C 100 -w rolling_split_100MB_dumps.pcap**

Host-based targeting is abandoned, and every frame is grabbed, but splitting the captures into multiple files no larger than 100MB each.

- **tcpdump -i eth0 -s 0 -w RFC3514_evil_bits.pcap 'ip[6] & 0x80 != 0'**

Here, target is the first byte of the IP fragmentation fields (byte offset 6). Bitmask is employed to narrow inspection to single highest order bit, also known as the IP "reserved bit," and capture and store packet only if the reserved bit is nonzero.

9.7.4 Wireshark:

Wireshark (originally named "Ethereal") was initially released in 1998 by Gerald Combs, is a graphical, open-source tool designed for capturing, filtering, and analyzing traffic.

Wireshark captures packets on any system network interface which has appropriate permissions to do so along with network card supporting sniffing. Wireshark displays packets as they are captured in real time. Details of using Wireshark is available on their official website https://www.wireshark.org/docs/

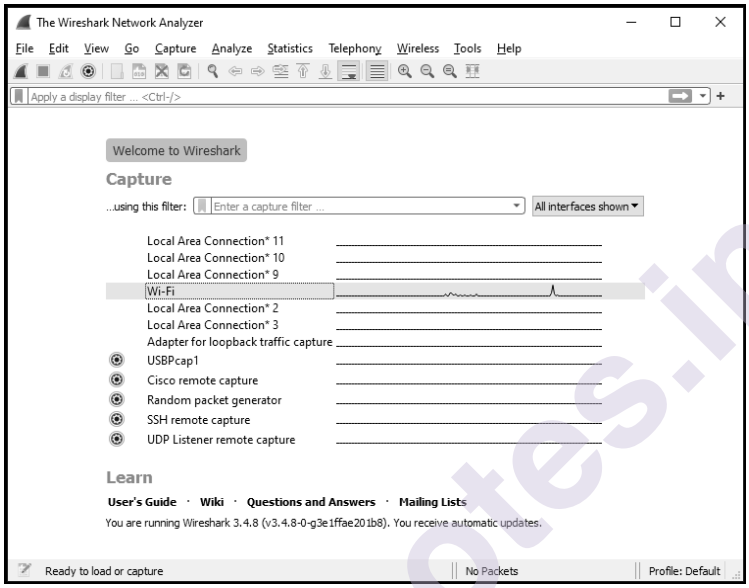


Figure 1.2: Default screen of Wireshark application version 3.4.8 installed on this chapter's author's computer

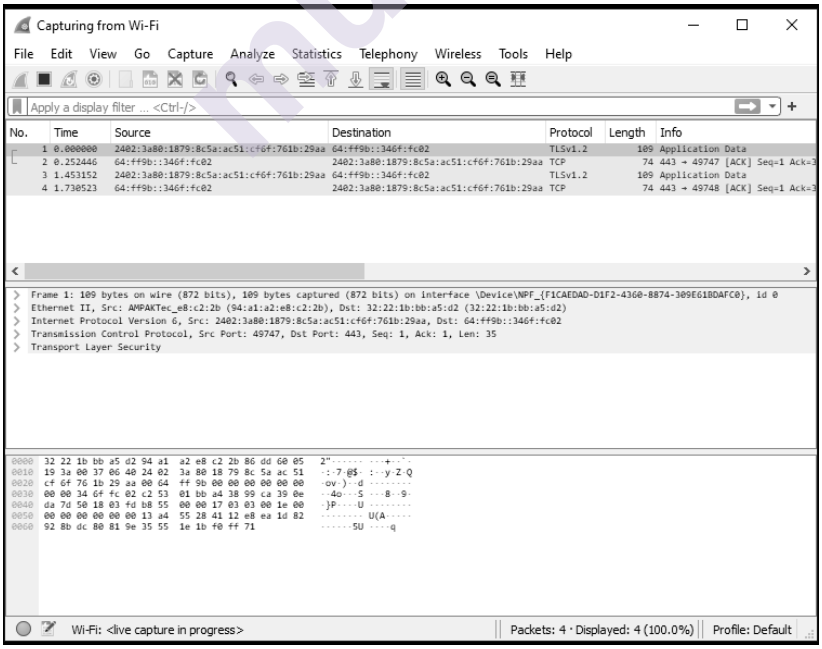


Figure 1.3: Wireshark capturing information from Wi-Fi of this chapter's author's computer

Some sample captures of Wireshark are also available at https://gitlab.com/wireshark/wireshark/-/wikis/SampleCaptures

9.7.5 Tshark:

Tshark is a command-line network protocol analysis tool that is part of the Wireshark distribution. Like Wireshark, it is libpcap-based, and can read and save files in the same standard formats as Wireshark. In addition to analysis, you can also use tshark to capture packets. The example below shows tshark capturing traffic on the network interface "eth0," filtering out all port 22 traffic, and storing the results in the file "test22.pcap."

 # tshark -i eth0 -w test22.pcap 'not port 22 '

Capturing on eth0

9.7.6 Dumpcap:

The Wireshark distribution also comes with a command-line tool, "dumpcap," which is specifically designed to capture packets. Since it is a specialized tool designed just for capturing packets, it takes up fewer system resources, maximizing capture capabilities. It automatically writes packet captures to a file. Following is an example using dumpcap to capture traffic on the interface eth0, filter out all port 22 traffic, and save the results in the file "test.pcap":

$ dumpcap -i eth0 -w test . pcap 'not port 22 '

File : test . pcap

Packets : 12

Packets dropped : 0

9.8 ACTIVE ACQUISITION

Active evidence acquisition amends the environment. Hence, one should be aware of various ways in which live acquisition modifies devices and environment under investigation, and work to minimize impact.

9.8.1 Common Interfaces:

Common ways to gain access to live network-based devices include:

Console:

The console is an input and display system, usually a keyboard and monitor connected to a computer. Many network devices have a serial port that you can use to connect a terminal to the console. It is possible to connect modern laptops and desktops to the serial console of network devices using USB-to-serial adapters.

Whenever possible, it is best to connect directly to the console of a network device rather than connecting remotely over the network. When you connect to a device over the network, you create additional traffic and often unintentionally change the state of local networking devices (such as CAM tables, log files, etc.). When you connect directly to the console, you can dramatically reduce your footprint.

Figure 1.4: Sample USB-to-serial adapter creative commons image

(**source:** https://i.stack.imgur.com/fRU7P.gif)

Secure Shell (SSH):

The Secure Shell protocol (SSH) is a common way for investigators to gain remote command-line access to systems containing network-based evidence. Developed as a replacement for the insecure Telnet and rlogin, SSH encrypts authentication credentials and data in transit. This means that even if the SSH traffic is intercepted, an attacker would be unable to recover the username, password, or contents of the communication. OpenSSH is a widely used implementation of SSH, which has been released free and opensource under a BSD license. Most modern network devices now support SSH as a method for remote command-line interaction. Following is an example using SSH to log into a system remotely on TCP port 4022, using account "kvk":

$ ssh -p 4022 kvk@remote.yttehsakitin.com

In following example, a command is executed to retrieve hostname of remote server (which is named "remote"):

$ ssh -p 4022 kvk@remote.yttehsakitin.com 'hostname' remote

Secure Copy (SCP) and SSH File Transfer Protocol (SFTP):

SSH implements the Secure Copy Protocol (SCP), which is a command-line utility designed to transfer files between networked systems. Local files can be referred to by their local paths, while remote files are specified by the username, hostname, and path to the file on the remote system, as in the following example:

$ scp -P 4022 dak@remote.gkcmp.com:/etc/passwd .

Here we copied /etc/passwd file from remote server to current working directory on our local system, using account "dak". Note the single dot argument at the end of the line, which specifies that we want to copy in our local directory. Also note uppercase "P" used to specify the port (in contrast, the "ssh" command uses a lowercase "p" for this purpose). The SSH File Transfer Protocol, or SFTP, is an alternative protocol used in conjunction with SSH for secure file transfer and manipulation. Although it is more portable as also offers more capabilities than SCP, but file transfer tends to be slower.

Telnet:

In addition to connecting to Telnet servers, the Telnet client can be used to interact with a wide variety of servers, such as SMTP and HTTP. In some cases, Telnet is an option for remote access to network device because some devices have limited hardware/software capacities so they cannot upgrade to more secure remote access tools such as SSH. Following is a sample in which Telnet connects to a remote HTTP server on port 80:

$ telnet daksecurit.com 80

Trying 204.11.246.1...

Connected to daksecurit.com.

Escape character is '^] '.

GET / HTTP /1.1

Host : daksecurit.com

HTTP /1.1 200 OK

Date : Sun , 26 Sep 2021 21:39:33 GMT

Server : Apache /2.2.9 (Debian) PHP /5.2.6 -1+ lenny10 with Suhosin - Patch mod_python /3.3.1 Python /2.5.2 mod_ssl /2.2.9 OpenSSL /0.9.8 g mod_perl /2.0.4 Perl /v5 .10.0

Last - Modified : Thu , 23 Sep 2021 22:40:55 GMT

ETag : "644284 -17 da -4 a668c728ebc0 "

Accept - Ranges : bytes

Content - Length : 6106

Content - Type : text / html

Simple Network Management Protocol (SNMP):

SNMP is frequently used as a medium for communicating and aggregating both network management information (often of interest to the forensic analyst) and security event data. In network forensics, SNMP is commonly used in one of two ways: event-based alerting and configuration queries.

A list of the basic SNMP operations is mentioned below:

- **Polling:** GET, GETNEXT, GETBULK
- **Interrupt:** TRAP, INFORM
- **Control:** SET

SNMPv1 and SNMPv2 use "community strings" for authentication, which are sent in plain text across the network. As a result, there is significant risk of credential theft if the community strings are intercepted as they are sent across the network. Commonly, the community string "public" has read-only access to the MIB, and "private" has read-write access. SNMPv3 supports strong encryption algorithms that can be used to encrypt authentication data and packet contents if these options are selected.

Trivial File Transfer Protocol (TFTP):

The Trivial File Transfer Protocol (TFTP) was first published in 1980, and designed as a simple, automated means of transferring files between remote systems. Like Telnet, TFTP was designed before most people were concerned about "bad actors" on the network. Consequently, it fit a useful niche: file transfer without the burden of authentication. One of the design goals was to keep the service very small so that it could run on systems with extremely limited storage space and memory. It runs over UDP on port 69.

Despite the lack of security, TFTP remains in widespread use today (generally restricted to internal networks). It has been incorporated into many network devices, from Voice over IP phones to firewalls to desktop BIOSs. TFTP is often used as a means through which distributed devices can download updates from a central server within an organization. On many routers and switches, it is used to back up and restore files. It was also used for payload propagation in both the CodeRed and Nimda outbreaks. Forensic analysts may need to use TFTP to export files from a router, switch, or other device that does not support SCP or SFTP for such operations.

Web and proprietary interfaces:

Usually, web interfaces are available by default as unencrypted HTTP sessions, in which case the login credentials and any data transferred over the connection is unencrypted and easily intercepted. Many vendors also offer SSL/TLS-encrypted web interfaces, although the certificates used with these services often have errors, which cause problems with validation. Web interfaces are popular because they are very portable; they do not require the user to install a special client to access the device.

9.8.2 Inspection Without Access:

In many cases, it is desirable to gain information about a device's configuration or state without accessing the device at all via an interface. There are also times when the password to user interfaces is not available.

It is possible to gather extensive information about a device's configuration and state through external inspection, using port scanning, vulnerability scanning, and other methods.

Port Scanning:

Port scanning, using a tool such as nmap, is an effective way to retrieve information about open ports and software versions of a device. Note that port scanning is an active process, meaning that you will generate network traffic and, in the process, modify the state of the targeted device.

Vulnerability Scanning:

Vulnerability scanning is the next level of active external inspection. In addition to port scanning, vulnerability scanners test target systems for a wide variety of known vulnerabilities. If you are concerned that your target of interest may be compromised, this can sometimes provide strong clues as to how the compromise may have occurred. Vulnerability scanning generates network traffic and modifies the state of the targeted device. In some cases, it can even crash the targeted device.

Be cautious and understand the options you have selected before running a vulnerability scanner against your target of interest.

9.8.3 Strategy:

- Refrain from rebooting or powering down the device.
- Connect via the console rather than over the network.
- Record the system time.
- Collect evidence according to level of volatility.
- Record your investigative activities.

9.9 SUMMARY

- A wiretapping can provide real-time network data. Taps can range from "vampire" taps, which literally puncture the insulation and contact copper wires, to surreptitious fiber taps, which bend the cable and cut the sheathing to reveal the light signals as they traverse the glass.
- In the clear, wireless access points advertise their names, presence, and capabilities; stations probe for access points; a MAC addresses of legitimate authenticated stations, unauthenticated stations and suspicious stations that may be attacking the wireless network.

- Packet sniffing is a technique in which attackers surreptitiously insert a software program at remote network switches or host computers
- Given a specific device's MAC address, network investigators can examine the switch to determine the corresponding physical port, and potentially trace that to a wall jack and a connected station
- One of the primary logs used in computer forensics is syslog, the main system log containing a variety of important messages
- When DHCP servers assign (or "lease") IP addresses, they typically create log of the event, which includes the assigned IP address, the MAC address of the device receiving the IP address, and the time the lease was provided or renewed.
- DNS server may contain logs that reveal connection attempts from internal to external systems, including web sites, SSH servers, external email servers, and more
- Applications and transaction systems ideally request a centralized authentication server to confirm or deny a user's identity
- When a firewall blocks a connection, it will save the destination port number to its logfile.
- If the web proxy is configured to cache web pages, it is even possible to retrieve the content that an end-user viewed or carve malware out of a cached web page for further analysis
- The Internet Protocol (IP) is designed to handle addressing and routing
- IPv4 uses 32-bit address space to identify source, destination systems.
- IPv6 protocol was developed with 128 bits for each of the source and destination addresses.
- TCP is a connection-oriented protocol. It indicates the state of transmissions using flags in the TCP header.
- The User Datagram Protocol (UDP) is designed to facilitate multiplexing of process communications on the host, without any of the reliability, sequencing, connection setup and teardown, or any of the frills of TCP.
- The two most widely used types of copper cabling used in the modern era are coaxial cable and twisted pair.
- An inline network tap is a Layer 1 device, which can be inserted in-line between two physically connected network devices
- "Vampire taps" are devices that pierce the shielding of copper wires to provide access to the signal within

- Induction coils transform the magnetism of weak signals to induce a much stronger signal in an external system
- Inline network taps work for fiber optic cables and copper cables.
- IEEE 802.11 is the most common wireless protocol beyond debate. It is being used in almost every part of our lives, from home security systems to cell phones, on a wide variety of devices and diverse application domains.
- A network hub is a Layer 1 device that physically connects all stations on a local subnet to one circuit.
- Switches operate at Layer 2 (datalink), and sometimes Layer 3 (network).
- The most common software libraries used for recording, parsing, and analyzing captured packet data are libpcap and WinPcap.
- Libpcap includes a filtering language called the "Berkeley Packet Filter" (BPF) syntax
- Tcpdump is a tool for capturing, filtering, and analyzing network traffic.
- Wireshark captures packets on any system network interface which has appropriate permissions to do so along with network card supporting sniffing.
- Tshark is a command-line network protocol analysis tool that is part of the Wireshark distribution
- The Wireshark distribution also comes with a command-line tool, "dumpcap," which is specifically designed to capture packets
- The Secure Shell protocol (SSH) is a common way for investigators to gain remote command-line access to systems containing network-based evidence
- Telnet is an option for remote access to network device because some devices have limited hardware/software capacities so they cannot upgrade to more secure remote access tools such as SSH
- SNMPv1 and SNMPv2 use "community strings" for authentication, which are sent in plain text across the network
- The Trivial File Transfer Protocol (TFTP) was first published in 1980, and designed as a simple, automated means of transferring files between remote systems.
- Port scanning is an active process, meaning that you will generate network traffic and, in the process, modify the state of targeted device

- Vulnerability scanning generates network traffic and modifies the state of the targeted device.
- Network Forensic strategy includes Refrain from rebooting or powering down the device., Connect via the console rather than over the network, Record the system time, Collect evidence according to level of volatility, Record your investigative activities.

9.10 REVIEW QUESTION

1. Explain few sources of network-based evidence.
2. State principles of internetworking
3. What are the commonalities and differences between IP and TCP?
4. What is UDP?
5. Write a note on cables and taps
6. What are hubs and switches?
7. Explain some traffic acquisition software.
8. Write a note on SSH.
9. Share a sample code of telnet
10. How can an inspection happen without access?
11. State some strategies for conducting network forensic investigation.

9.11 REFERENCES

1. Network Forensics: Tracking Hackers through Cyberspace, by Sherri Davidoff, Jonathan HAM, Prentice Hall, 2012. ISBN-13: 978-0-13-256471-7 (Majority part of this chapter has been referenced from book's Part I – Chapter 2 and 3)
2. Computer Forensics Computer Crime Scene Investigation, John R. Vacca, Second Edition, 2005. ISBN-13: 978-1-58450-389-7
3. Gokhan Kula & Y. Deniz Irenb. (WCIT-2011). Wireless network forensics: sources of digital evidence. Digital version is available at https://www.academia.edu/35457721/Wireless_network_forensics_sources_of_digital_evidence

*****

UNIT IV

10

THE MOBILE FORENSICS PROCESS: STEPS AND TYPES

Unit Structure

10.1 INTRODUCTION: IMPORTANCE OF MOBILE FORENSICS

The term "mobile devices" encompasses a wide array of gadgets ranging from mobile phones, smartphones, tablets, and GPS units to wearables and PDAs. What they all have in common is the fact that they can contain a lot of user information.

Mobile devices are right in the middle of three booming technological trends: Internet of Things, Cloud Computing, and Big Data. The proliferation of mobile technology is perhaps the main reason, or at least one of the main reasons, for these trends to occur in the first place. In 2015, 377.9 million wireless subscriber connections of smartphones, tablets, and feature phones occurred in the United States.

Nowadays, mobile device use is as pervasive as it is helpful, especially in the context of digital forensics, because these small-sized machines amass huge quantities of data on a daily basis, which can be extracted to

facilitate the investigation. Being something like a digital extension of ourselves, these machines allow digital forensic investigators to glean a lot of information.

10.2 INFORMATION THAT RESIDES ON MOBILE DEVICES (A NON-EXHAUSTIVE LIST)

- Incoming, outgoing, missed call history
- Phonebook or contact lists
- SMS text, application based, and multimedia messaging content
- Pictures, videos, and audio files and sometimes voicemail messages
- Internet browsing history, content, cookies, search history, analytics information
- To-do lists, notes, calendar entries, ringtones
- Documents, spreadsheets, presentation files and other user-created data
- Passwords, passcodes, swipe codes, user account credentials
- Historical geolocation data, cell phone tower related location data, Wi-Fi connection information
- User dictionary content
- Data from various installed apps
- System files, usage logs, error messages
- Deleted data from all of the above

Source:

One good display of the real-life effectiveness of mobile forensics is the mobile device call logs, and GPS data that facilitated solving the 2010 attempted bombing case in Times Square, NY.

10.3 WHAT IS THE MOBILE FORENSICS PROCESS?

Crimes do not happen in isolation from technological tendencies; therefore, mobile device forensics has become a significant part of digital forensics.

Most people do not realize how complicated the mobile forensics process can be in reality. As the mobile devices increasingly continue to gravitate between professional and personal use, the streams of data pouring into them will continue to grow exponentially as well. Did you know that 33,500 reams of paper are the equivalent of 64 gigabytes if printed? Storage capacity of 64 GB is common for today's smartphones.

The mobile forensics process aims to recover digital evidence or relevant data from a mobile device in a way that will preserve the evidence in a forensically sound condition. To achieve that, the mobile forensic process needs to set out precise rules that will seize, isolate, transport, store for analysis and proof digital evidence safely originating from mobile devices.

Usually, the mobile forensics process is similar to the ones in other branches of digital forensics. Nevertheless, one should know that the mobile forensics process has its own particularities that need to be considered. Following correct methodology and guidelines is a vital precondition for the examination of mobile devices to yield good results.

Among the figures most likely to be entrusted with the performance of the following tasks are Forensic Examiners, Incident Responders, and Corporate Investigators. During the inquiry into a given crime involving mobile technology, the individuals in charge of the mobile forensic process need to acquire every piece of information that may help them later – for instance, device's passwords, pattern locks or PIN codes.

10.4 WHAT ARE THE STEPS IN THE MOBILE FORENSICS PROCESS?

10.4.1 Seizure:

Mobile phone evidence box

Credit: mobile phone evidence box by jon crel / (CC BY-ND 2.0)

Digital forensics operates on the principle that evidence should always be adequately preserved, processed, and admissible in a court of law. Some legal considerations go hand in hand with the confiscation of mobile devices.

There are two major risks concerning this phase of the mobile forensic process: Lock activation (by user/suspect/inadvertent third party) and Network / Cellular connection.

Network isolation is always advisable, and it could be achieved either through 1) Airplane Mode + Disabling Wi-Fi and Hotspots, or 2) Cloning the device SIM card.

Airplane mode:

Mobile devices are often seized switched on; and since the purpose of their confiscation is to preserve evidence, the best way to transport them is to attempt to keep them turned on to avoid a shutdown, which would inevitably alter files.

Phone jammer

Credit: Got myself a Cell Phone Jammer by Baishampayan Ghose / (CC BY-ND 2.0)

A Faraday box/bag and external power supply are common types of equipment for conducting mobile forensics. While the former is a container specifically designed to isolate mobile devices from network communications and, at the same time, help with the safe transportation of evidence to the laboratory, the latter, is a power source embedded inside the Faraday box/bag. Before putting the phone in the Faraday bag, disconnect it from the network, disable all network connections (Wi-Fi, GPS, Hotspots, etc.), and activate the flight mode to protect the integrity of the evidence.

Faraday bag:

Last but not least, investigators should beware of mobile devices being connected to unknown incendiary devices, as well as any other booby trap set up to cause bodily harm or death to anyone at the crime scene.

10.4.2 Acquisition:

/Identification + extraction/

The goal of this phase is to retrieve data from the mobile device. A locked screen can be unlocked with the right PIN, password, pattern, or biometrics (Note that biometric approaches while convenient are not always protected by the fifth amendment of the U.S. Constitution). According to a ruling by the Virginia Circuit Court, passcodes are protected, fingerprints not. Also, similar lock measures may exist on apps, images, SMSs, or messengers. Encryption, on the other hand, provides security on a software and/or hardware level that is often impossible to circumvent.

It is hard to be in control of data on mobile devices because the data is mobile as well. Once communications or files are sent from a smartphone, control is lost. Although there are different devices having the capability to store considerable amounts of data, the data in itself may physically be in another location. To give an example, data synchronization among devices and applications can take place directly but also via the cloud. Services such as Apple's iCloud and Microsoft's One Drive are prevalent among mobile device users, which leave open the possibility for data acquisition from there. For that reason, investigators should be attentive to any indications that data may transcend the mobile device as a physical object, because such an occurrence may affect the collection and even preservation process.

Since data is constantly being synchronized, hardware and software may be able to bridge the data gap. Consider Uber – it has both an app and a fully functional website. All the information that can be accessed through the Uber app on a phone may be pulled off the Uber website instead, or even the Uber software program installed on a computer.

Regardless of the type of the device, identifying the location of the data can be further impeded due to the fragmentation of operating systems and item specifications. The open-source Android operating system alone comes in several different versions, and even Apple's iOS may vary from version to version.

Another challenge that forensic experts need to overcome is the abundant and ever-changing landscape of mobile apps. Create a full list of all installed apps. Some apps archive and backup data.

After one identifies the data sources, the next step is to collect the information properly. There are certain unique challenges concerning gathering information in the context of mobile technology. Many mobile devices cannot be collected by creating an image and instead they may have to undergo a process called acquisition of data. Thera are various

protocols for collecting data from mobile devices as certain design specifications may only allow one type of acquisition.

The forensic examiner should make a use of SIM Card imagining – a procedure that recreates a replica image of the SIM Card content. As with other replicas, the original evidence will remain intact while the replica image is being used for analysis. All image files should be hashed to ensure data remains accurate and unchanged.

10.4.3 Examination and analysis:

Flasher box forensics. Using a UFS box to access mobile phone

As the first step of every digital investigation involving a mobile device(s), the forensic expert needs to identify:

- Type of the mobile device(s) – e.g., GPS, smartphone, tablet, etc.
- Type of network – GSM, CDMA, and TDMA
- Carrier
- Service provider (Reverse Lookup)

The examiner may need to use numerous forensic tools to acquire and analyze data residing in the machine. Due to the sheer diversity of mobile devices, there is no one-size-fits-all solution regarding mobile forensic tools. Consequently, it is advisable to use more than one tool for examination. AccessData, Sleuthkit, and EnCase are some popular forensic software products that have analytic capabilities. The most appropriate tool(s) is being chosen depending on the type and model of mobile device.

Timeline and link analysis available in many mobile forensic tools could tie each of the most significant events, from a forensic analyst's point of view.

Intel Computer Stick imaged and analyzed

All of the information, evidence, and other findings extracted, analyzed, and documented throughout the investigation should be presented to any other forensic examiner or a court in a clear, concise, and complete manner.

The New digital reality of mobile forensics

"On May 17, 2015, a biker gang shootout erupted at the Twin Peaks Restaurant near Waco, Texas, killing nine and injuring dozens. More than a hundred mobile phones were recovered from the incident, setting the wheels in motion for one of the state's largest and most challenging investigations to date.

The events that unfolded at the Twin Peaks restaurant thrust McLennan County law enforcement into a new urgent reality.

Within days of the decision to deploy, [the **Cellebrite's New UFED Analytics Platform]** allowed both investigators and prosecutors to import and decode all extracted mobile digital forensics data from one centralized location for fast and efficient analysis. Call records, text messages, photos, videos and social media posts could be filtered by keywords and tagged for other members of the investigative team to view instantly.

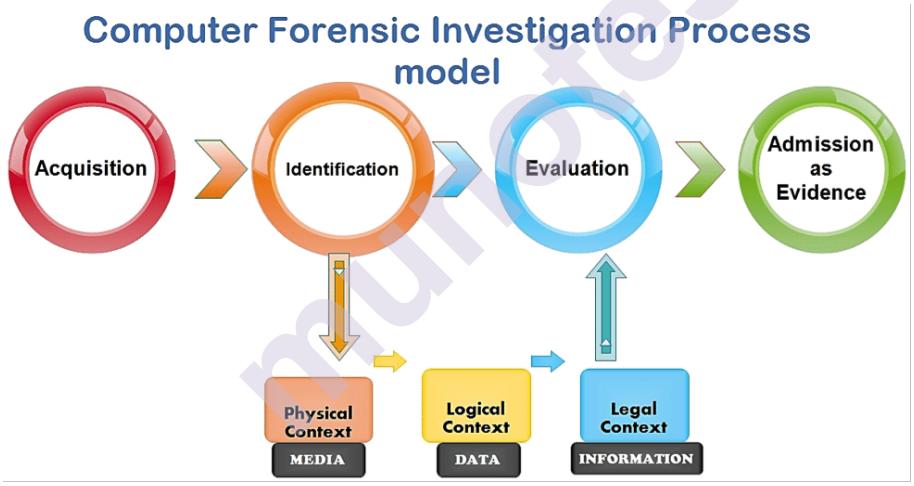
"… [the solution] allowed us to go back and more quickly comb through the data to find the bigger picture details we needed to confirm the motives, plans and goals of these motorcycle organizations [,]" said the McLennan County prosecutor.**"**

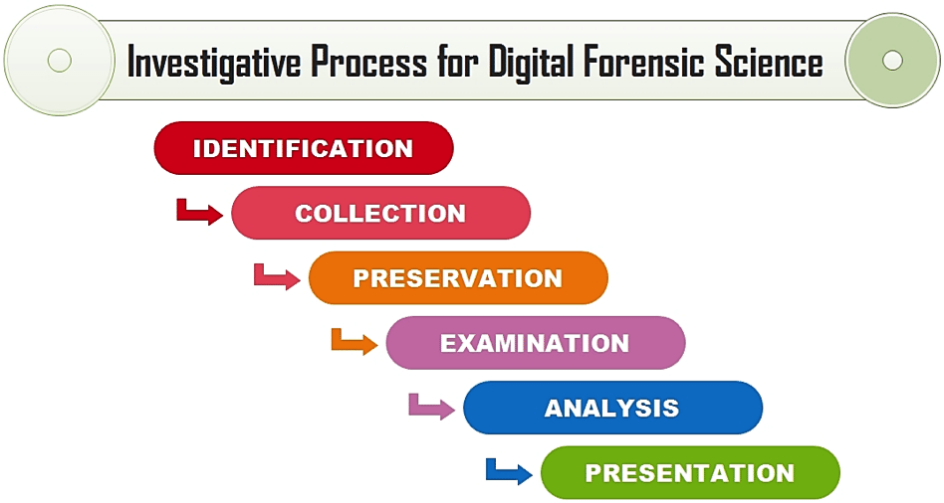
Source: Removing the Burden of Finding Digital "Proof"

Quick Question: What procedure could the McLennan County law enforcement have used immediately at the crime scene to reduce the large backlogs of digital forensics casework at the outset (provided that they had the experts to carry out that procedure)?

Find the answer below the Reference List.

10.5 WHAT OTHER MODELS ARE AVAILABLE?



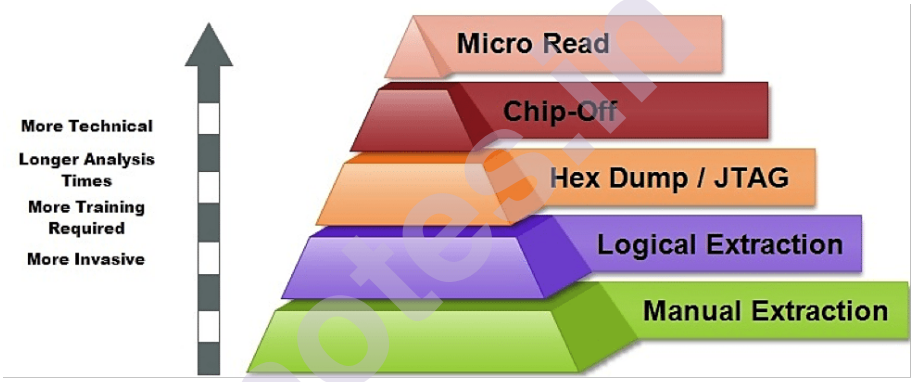


10.6 NON-INVASIVE VS. INVASIVE FORENSICS

No matter what your actual mobile forensic method is, it is imperative to create a policy or plan for its execution and follow all its steps meticulously and in the proper sequence. Not following the protocol may entail grave consequences. One should start with non-invasive forensic techniques first as they tend to endanger a device's integrity to a lesser degree. Be careful with built-in security features – "[f]or example, collecting a physical image before a logical image on certain devices can completely wipe a phone of all data, as can attempting to access a locked device and making too many password attempts." /Source: Mobile Device Forensics by Scott Polus/

From the legal point of view, the level of the interaction between the user and the device is critical.

Mobile forensics – tool classification pyramid:



10.6.1 Non-invasive methods:

Non-invasive methods can deal with other tasks, such as unlocking the SIM lock or/and the operator lock, the operating system update, IMEI number modification, etc. These techniques are virtually inapplicable in cases where the device has sustained severe physical damage. Types of non-invasive mobile forensic methods:

- **Manual extraction:**

The forensic examiner merely browses through the data using the mobile device's touchscreen or keypad. Information of interest discovered on the phone is photographically documented. This process of manual extraction is simple and applicable to almost every phone. While there are some tools designed to make this process easier, it is not possible, however, to restore deleted data this way.

- **Logical extraction:**

This approach involves instituting a connection between the mobile device and the forensic workstation using a USB cable, Bluetooth, Infrared or RJ-45 cable. Following the connecting part, the computer sends command requests to the device, and the device sends back data

from its memory. The majority of forensic tools support logical extraction, and the process itself requires short-term training. On the downside, however, this technique may add data to the mobile device and may alter the integrity of the evidence. Also, deleted data is rarely accessible.

- **JTAG method:**

JTAG is a non-invasive form of physical acquisition that could extract data from a mobile device even when data was difficult to access through software avenues because the device is damaged, locked or encrypted. The device, however, must be at least partially functional (minor damages would not hinder this method).

The process involves connecting to the Test Access Ports (TAPs) on a device and instructing the processor to transfer raw data stored on connected memory chips. This is a standard feature that one could come across in many mobile phone models, which provides mobile phone manufactures a low-level interface outside the operating system. Digital forensic investigators take an interest in JTAG, as it can, in theory, allow direct access to the mobile device's memory without jeopardizing it. Despite that fact, it is a labor-intensive, time-consuming procedure, and it requires advance knowledge (not only of JTAG for the model of the phone under investigation but also of how to arrange anew the resulting binary composed of the phone's memory structures).

- **Hex dump:**

Similar to JTAG, Hex dump is another method for physical extraction of raw information stored in flash memory. It is performed by connecting the forensic workstation to the device and then tunneling an unsigned code or a bootloader into the device, each of them will carry instructions to dump memory from the phone to the computer. Resulting image is fairly technical—in binary format—and it requires a person having the technical education to analyze it. Furthermore, the examiner comes into possession of an abundant amount of data, since deleted data can be recovered, and, on top of that, the entire process is inexpensive.

10.6.2 Invasive methods:

Typically, they are longer and more complex. In cases where the device is entirely non-functional due to some severe damage, it is very likely the only way to retrieve data from the device might be to manually remove and image the flash memory chips of the device. Even if the device or item is in good condition, circumstances may require the forensic expert to acquire the chip's contents physically.

- **Chip-off:**

A process that refers to obtaining data straight from the mobile device's memory chip. According to the preparations pertinent to this level, the chip is detached from the device and a chip reader or a second phone is

used to extract data stored on the device under investigation. It should be noted that this method is technically challenging because of the wide variety of chip types existing on the mobile market. Also, the chip-off process is expensive, training is required, and the examiner should procure specific hardware to conduct de-soldering and heating of the memory chip. Bits and bytes of raw information that is retrieved from the memory are yet to be parsed, decoded, and interpreted. Even the smallest mistake may lead to damages to the memory chip, which, in effect, would render the data irrevocably lost. Consequently, experts advise having recourse to chip-off when: a) other methods of extraction are already attempted, b) it is important to preserve the current state of device's memory, c) the memory chip is the only element in a mobile device that is not broken.

The whole process consists of five stages:

1. Detect the memory chip typology of the device
2. Physical extraction of the chip (for example, by unwelding it)
3. Interfacing of the chip using reading/programming software
4. Reading and transferring data from the chip to a PC
5. Interpretation of the acquired data (using reverse engineering)

6. Sources of network forensic evidence:

One of the key aspects of any successful forensic investigation is the evidence collection phase. Identifying the sources of evidence while investigating an attack is crucial for the investigation to be successful. Once the sources are identified, the evidence such as logs should be collated and used for further analysis. This article provides an overview of various sources of network forensic evidence an investigator may be interested in. Sources of evidence

Depending on the type of attack being investigated, a complex network may have several places where evidence can be collected from. Let us discuss some of the common sources where we may find evidence during an investigation.

10.7 APPLICATION AND OS LOGS

There are various logs that will be generated in different locations depending on the events occurring. Application logs such as access logs and database logs, event logs generated by the operating systems in use(Windows event logs and Linux syslog), logs from network devices such as firewalls and routers are some examples of various log locations to look at.

When it comes to Windows event logs, there are three major categories of logs that can be found in Windows event logs.

Application: The Application logs contain the logs of the events generated by the applications running on the Operating System.

Security: As the name indicates, security logs contain events related to security. This includes logs such as valid and invalid logon attempts.

System: System logs contain events logged by system components. This includes events such as operating system reboot due to a system failure or crash.

When it comes to event logs on Linux based systems such as Ubuntu, most of the events can be seen in a single location and the location may vary depending on the Linux flavor. In case of Ubuntu, authentication logs, kernel logs, system logs and even some application specific logs such as Apache logs will be available in /var/log/ directory.

Intrusion Detection System/Intrusion Prevention System (IDS/IPS) alerts:

Many investigations begin from an alert from IDS or IPS. These logs from IDS or IPS usually include alert data such as an identifier that has caused the alert and the description of the alert. In addition to it, we may find packet headers and payload in the alert. Depending on the tool being used, these logs may be extracted from various locations such as a file on the disk, web gui or email. The following figure shows alerts from Snort IDS being run in pfSense.

Routers, Firewalls and proxy logs:

Routers are used to route the traffic from one network to another and they are the most commonly used devices in enterprise networks and they often contain many features that are of interest during a network forensic investigation.

Firewalls perform packet filtering based on a predefined ruleset. For example, let us assume that a rule has been defined to block any incoming traffic on port 3389. Any firewall will be able to do this as specified in the firewall rules. Modern firewalls can do much more than just packet filtering. They are often termed as Next Generation Firewalls and come with additional features such as VPN, Intrusion Prevention Systems, Intrusion Detection Systems, Anti Virus, Web Application Firewalls and more. Often, the goal of these modern firewalls is to effectively monitor the content within the packets and determine whether to allow the packets or not and thus they contain logs of our interest.

In addition to the routers and firewalls, web proxies in enterprise environments contain interesting logs at a large scale. Web traffic constitutes the major share of an enterprise's network traffic. Employees browsing activities in an enterprise environment almost always get recorded in web proxies. So, Web proxies can be a goldmine for investigators.

Captured Network traffic:

When an alert is generated by tools like IDS/IPS, a packet capture can be recorded and saved for further analysis in many tools. Most of these captures can be analysed using tools like Wireshark later. Additionally, in the event of suspicion of an ongoing attack, tools like tcpdump for Wireshark can be used for packet capturing and analysis.

10.8 ROUTERS, SWITCHES & FIREWALLS

Integrated devices:

Just like home devices, business devices have become more and more consolidated over time but not to the extent that the home devices have. Network administrators in a business network are more comfortable having separate devices and even like the idea. This is because network administrators like to be able to isolate problems down to a certain device and they like to be able to know the performance capabilities of every device. If you use an integrated router, switch, and firewall all into one device, troubleshooting, managing, and understanding the performance capabilities of that device gets complicated. I'm not saying that this isn't done. You can buy a big & expensive, chassis-based, Cisco 6500 series switch and have almost all these functions on different blades of the switch. This may be fine for a larger business with a group of administrators but to a medium size business and a single network administrator, many times, this is a scary thought.

Keep in mind that for a medium or large size business, these integrated home devices won't work because they don't offer all the features required. The standalone routers, switches, and firewalls have many more features than these integrated devices do. Router

A router is a hardware device and has the function of routing packets between networks. A router works at Layer 3 of the OSI model – the Network Layer. This is the layer that the IP protocol works at. Most routers today are IP routers that examine the source and destination IP addresses of each packet, look up the destination of the packet in the router's IP routing table, and route that packet on its way. In the event that the destination is not listed in the routing table, the router will either send the packet to a default router (if it has one) or drop the packet. Routers are usually used to connect a local area network to a wide-area network (a LAN to a WAN) but can also be used to segment large local area networks (LAN's).

Routers prevent broadcasts. Another way of saying this is that routers form a broadcast domain. So, if your network is being deluged by IP broadcasts, you need to subnet your network into two or more smaller networks. Those networks would be connected by a router and that router wouldn't allow broadcast traffic to flow between subnets.

Routers use routing dynamic protocols like OSPF, RIP, or BGP to learn routes from other routers. Router can also use static routes that are entered by the administrator.

Routers replace the Ethernet MAC address of the source device with their own MAC address when they send a packet out an interface. When the response to that packet comes back, the new source of the packet is sending the response to the destination of the router. The router receives this, replaces the source address, changes the destination address to the original address, and sends the packet back to the original sender. This is a complex topic that we could spend a whole article covering so this is only meant to provide the most basic understanding of how this works.

Switch:

A switch is a hardware device that works at Layer 2 of the OSI model – data link. The data link layer is where the Ethernet protocol works.

A switch switches Ethernet frames by keeping a table of what MAC addresses have been seen on what switch port. The switch uses this table to determine where to send all future frames that it receives. In Cisco terminology, this table is called the CAM table (content addressable memory). In general, the proper term for this table is the bridge forwarding table. If a switch receives a frame with a destination MAC address that it does not have in its table, it floods that frame to all switch ports. When it receives a response, it puts that MAC address in the table so that it won't have to flood next time.

A switch is a high-speed multiport bridge. This is why bridges are no longer needed or manufactured. Switches do what bridges did faster and cheaper. Most routers can also function as bridges.

You might be asking how a hub fits into this mix of devices. A hub is a multiport repeater. In other words, anything that comes in one port of a hub is duplicated and sent out all other ports of the hub that have devices attached. There is no intelligence to how a hub functions. A switch is a vast improvement over a hub in terms of intelligence, for many reasons. The most important of those reasons is how the bridge forwarding table works. Intelligent (smart) switches have made hubs obsolete because they can do more at the same cost of a dumb hub. For this reason, hubs are rarely used or sold any longer.

To see this bridge forwarding table (CAM table) on a Cisco switch just type: **show mac-address-table**

Firewall:

A firewall is used to protect more secure network from a less secure network. Generally, firewalls are used to protect your internal/private LAN from the Internet.

A firewall generally works at layer 3 and 4 of the OSI model. Layer 3 is the Network Layer where IP works and Layer 4 is the Transport Layer, where TCP and UDP function. Many firewalls today have advanced up the OSI layers and can even understand Layer 7 – the Application Layer.

There are a variety of different types of firewalls and we won't go into that in this article so let's just talk about the most popular type of firewall – a stateful packet inspection (SPI) hardware firewall. An example of a SPI hardware firewall is a Cisco PIX firewall. This is a dedicated appliance and it looks a lot like a Cisco router.

A SPI firewall is stateful because it understands the different states of the TCP (transmission control protocol) protocol. It knows what is coming and what it going and keeps track of it all. Thus, if a packet tried to come in but it wasn't requested, the firewall knows that and drops it.

10.9 WEB PROXIES

10.9.1 Introduction:

- Due to the growth in web traffic, firewalls, routers, and switches are no longer sufficient to protect enterprise parameters
- Over the last five to seven years, web proxying and caching have become increasing popular for both filtering traffic and improving efficiencies in marketing
- The good news for forensic investigators is that web proxies can provide granular logs and caches that can be used to support forensic investigations.

10.9.2 What is a Web Proxy Server?:

The internet works intricately, and people rarely think about it. The risk of that is the looming danger of crimes such as identity theft and data security breaches. Different individuals use proxy servers or **Virtual Private Networks (VPN)** to protect themselves. A proxy server is a web server that acts as a gateway between a client application, for example, a browser, and the real server. It makes requests to the real server on behalf of the client or sometimes fulfills the claim itself.

Web proxy servers have two primary purposes, namely to filter requests and improve performances. Additionally, there are proxy servers that sit between web servers and web clients known as a reverse proxy. Reverse proxy servers pass on requests from web clients to web servers. They are

used to cache images and pages to reduce the load on web servers significantly.

What are web proxy servers used for?

There are several reasons to use web proxy servers as an individual or an organization.

10.9.3 Control internet access:

As an individual, you can use proxy servers to control and monitor your children's internet access. It works to block unfavorable sites and lock them out of adult content. Organizations also use proxy servers to limit and control internet access. They do this to avoid employees looking at various sites while at work. Alternatively, they log all web requests, which indicates what sites employees are visiting and how much time they spend cyberloafing.

Privacy benefits:

Proxy servers allow users to browse the internet more privately by changing your IP address and other identifying data on your computer. Proxy servers keep your personal information private, so the server does not know who has made the request and thus keeps your browsing activities and browsing history private.

Access to blocked sites:

Content providers put restrictions on their content for various reasons, such as locations, which is essentially the IP addresses. However, a web proxy server allows you to log on to a restricted server by making it seem like you are at a different location.

Improved speeds and bandwidth savings:

Organizations can save on bandwidth and improve loading speeds by using efficient web proxy servers. Proxy servers cache images and web data to keep the latest copy of a website. The caches allow a proxy server to retrieve the most recent copy of popular sites, which saves on bandwidth and improves network performance.

Improved security:

Efficient proxy servers encrypt your web requests to protect them from prying eyes and protect your transactions. Proxy servers also work to prevent intrusion from known **malware sites**. Organizations also add to **VPN's to increase security and allow remote users to access** the company network.

Web proxy servers play a significant role in **cybersecurity** for both individual and organizational use. With increased internet use, there is a rising need to protect your data, keep away malware and viruses, protect

personal information and data, and enable access to a wide range of information. Web proxy servers help increase browsing speeds by caching web pages, offering bandwidth, and providing heightened security measures.

*****