(2 ½ Hours) **[Total Marks: 75]**

N.B. 1) All questions are compulsory.
2) Figures to the right indicate marks.
3) Illustrations, in-depth answers and diagrams will be appreciated.
4) Mixing of sub-questions is not allowed.

Q. 1 Attempt All (Each of 5Marks) **(15)**

(a) Multiple Choice Questions

i) ____ is a Sysinternals command that shows all Registry data in real time on a Windows computer.
a. PsReg b. RegMon
c. RegExplorer d. RegHandle

ii) _____ unique number is referred to as a "digital fingerprint."
a. commingled data b. hash values
c. acquired data d. file header

iii) Corporations often follow the ____ doctrine, which is what happens when a civilian or corporate investigative agent delivers evidence to a law enforcement officer.
a. silver-tree b. silver-platter
c. gold-tree d. gold-platter

iv) E-mail messages are distributed from one central server to many connected client computers, a configuration called ____.
a. client/server architecture b. client architecture
c. central distribution architecture d. peer-to-peer architecture

v) When you give ____ testimony, you present this evidence and explain what it is and how it was obtained.
a. technical/scientific b. lay witness
c. expert d. deposition

(b) Fill in the blanks

(3, voir dire, 4, image, motion in limine, linear, picture, key escrow, hierarchical, key splitting)

i) _____ is designed to recover encrypted data if users forget their passphrases or if the user key is corrupted after a system data failure.

ii) Most SIM cards allow _____ access attempts before locking you out.

iii) _____ is the process of qualifying a witness as an expert.

iv) The file where the bit-stream copy is stored; usually referred to as an/a ____

v) The file system for a SIM card is a ____ structure.

(c) Answer in 1 – 2 sentences

i) State two types of deposition

ii) What is meant by Chain of Custody?

iii) List two hashing algorithms commonly used for forensic purposes.

iv) Define Plain view doctrine

v) What is TOR?

Q. 2 Attempt the following (Any THREE) **(15)**

(a) Define Data Acquisition. State its types and goals

(b) What guidelines an investigator has to keep in mind while seizing digital evidence at the scene?

(c) List standard systems analysis steps to be applied when preparing a for forensic investigation case

(d) What is the standard procedure used for network forensics?

(e) State and explain various sub functions of extractions

(f) What is an Investigation triad? State and Explain its parts

Q. 3 Attempt the following (Any THREE) **(15)**

(a) State and explain any two ways to trace information on the internet

(b) What are the two most common caveats an Internet Forensics investigator will encounter? Explain any one in brief

(c) List the different fields of Web Server logs

(d) What are the different types of Personal Information that can be found on Social Media?

(e) Explain the following terms:
i) Web Cache ii) Geotagging iii) Web Shells iv) SMTP v) Traceroute

(f) Describe tasks in investigating e-mail crimes and violations

Q. 4 Attempt the following (Any THREE) **(15)**

(a) Explain the legal process to conduct computer investigation for potential criminal violations of law.

(b) What are the steps to create image files of digital evidence?

(c) What is an Expert Witness? State the four criteria based on which the quality of a report is judged?

(d) Briefly outline the steps of trial process

(e) Explain Digital Signature and Electronic Signature w.r.t to the IT Act

(f) Write a Short note on Electronic Governance

Q. 5 Attempt the following (Any THREE) **(15)**

(a) Write a short note on SIM & its structure

(b) State and explain various Cyber Forensic tools

(c) What are privacy controls? Explain its importance

(d) List various guidelines for writing reports

(e) Explain the following terms:
i) Affidavit ii) limiting phrase iii) deposition banks
iv)hearsay v) spoliation

****