(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

1) Validate your tools and verify your evidence with_____to ensure its integrity.
a. hashing algorithms b. watermarks
c. steganography d. digital certificates

2) A written report is frequently a(n)_____or a declaration.
a. subpoena b. deposition
c. affidavit d. perjury

3) In Microsoft Outlook, you can save sent, drafted, deleted, and received e-mails in a file with a file extension of____.
a. .ost b. .pst
c. both a & b d. none of the above

4) _____can help you determine whether a network is truly under attack or a user has inadvertently installed an untested patch or custom program.
a. Internet Forensics b. Network Forensics
c. Computer Forensics d. Traffic Forensics

5) The majority of digital cameras use the_____format to store digital pictures.
a. EXIF b. PNG
c. TIFF d. GIF

(b) Fill in the blanks
[network, steganography, RegMon, investigation plan, Plaintiff, Encryption, Exculpatory]

1. _____has also been used to protect copyrighted material by inserting digital watermarks into a file.
2. You begin any computer forensics case by creating a(n)_________.
3. Most packet sniffers operate on data link layer or_____of the OSI model.
4. _____is a Sysinternals command that shows all Registry data in real time on a Windows computer.
5. _____ Evidence is evidence that exonerates or diminishes the defendant's liability.

(c) Short Answers

1. Define damaged data.
2. What are e-mail headers?
3. What is INDEX.DAT with respect to Internet Explorer?
4. Define the term "computer" as per IT Act.
5. What is the need of privacy controls with respect to social media posts?

Q. 2 Attempt the following (Any THREE)(Each of 5Marks) (15)

(a) What is computer forensics? Why computer forensics is important?

(b) Define Live Acquisitions? Explain how Live Acquisitions are performed in network forensics?

(c) List the storage formats for Digital Evidence. Explain any one in brief.

(d) Discuss on the Remote Network Acquisition tools.

(e) What are the different components found inside a Mobile device?

(f) Explain procedures for Corporate High-tech Investigations with respect to:

a. Employee Termination Cases
b. Internet Abuse Investigation

Q. 3 Attempt the following (Any THREE) (Each of 5Marks) (15)

(a) What are E-mail servers? With respect to investigate e-mail abuse explain how an e-mail server records and handles the e-mail it receives.

(b) Define Onion Routing? List the features and explain how does the process of Onion Routing work.

(c) Explain the role of e-mail in investigations.

(d) Briefly explain tcpdump and pcap with respect to Collection Phase in Network Acquisition.

(e) What is Messenger forensic? State the different types of evidence that can be collected from a messenger? Where can such files be found on computer?

(f) Write short note on Location data of social media.

Q. 4 Attempt the following (Any THREE) (Each of 5Marks) (15)

(a) Who is an authorized requestor? Why should companies appoint them for computer investigations?

(b) Write a short note on Report structure in Computer forensics.

(c) Explain the following terms:
Hearing, voir dire, motion in limine, conflicting out.

(d) Elaborate on the “Digital Signature and Electronic Signature” section of the IT Act, 2008.

(e) What are the penalties, compensation, and adjudication as per the IT Act, 2008?

(f) Describe the Power of police officer and other officer w.r.t IT Act

Q. 5 Attempt the following (Any THREE) (Each of 5Marks) (15)

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

(b) Write a short note on Web shells.

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

(d) Discuss on the procedure for securing the evidence.

(e) Explain different types of Personal information shared on social media.

****