(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

(a) Select the correct alternative from the options given: (10M)

(i) In case of ---------, the evidence is collected from a system where the microprocessor is running.
(a) live acquisition (b) static acquisition
(c) sparse acquisition (d) offline acquisition

(ii) Packet Sniffers are software placed network to_____.
(a) Monitor Traffic (b) Analyzing attackers
(c) Obtaining information (d) provide security

(iii) You can use the ____ to help your attorney learn the terms and functions used in computer forensics.
(a) verbal report (b) preliminary report
(c) final report (d) examination plan

(iv) _____ is a famous technological medium for the spread of malware, facing problems of spam, & phishing attacks.
(a) Cloud (b) Pen drive
(c) Website (d) Email

(v) When a person is harassed repeatedly by being followed, then he/she is a target of_____
(a) Phishing (b) Stalking
(c) Bullying (d) Identity threat

(vi) Which of the following is not a type of cybercrime?
(a) Data theft (b) Forgery
(c) Damage to data and systems (d) Installing antivirus for protection

(vii) Attorneys can now submit documents electronically in many courts; the standard format in federal courts is ____.
(a) Portable Document Format (PDF) (b) Microsoft Word (DOC)
(c) Encapsulated Postscript (EPS) (d) Postscript (PS)

(viii) An ____ is a document that lets you know what kind of questions to expect when you are testifying.
(a) written report (b) affidavit
(c) Examination Plan (d) subpoena

(ix) A written report is frequently an ____ or a declaration.
(a) subpoena (b) Affidavit
(c) deposition (d) Perjury

(x) Most federal courts have interpreted computer records as ____ evidence.
(a) conclusive (b) Regular
(c) hearsay (d) Direct

(b) **Fill in the blanks by selecting from the pool of options:** (5M)
(computer forensic science, computer crime, DoS attack, Phishing, Active Acquisition, Flow analysis, Spam,Malware, Reverse Engineering, Stealing cookies)

(i) Computer forensics also known as?

(ii) Which of the following is a class of computer threat?

(iii) Evidence collected from network device logs

(iv) Unsolicited commercial email is known as _____

(v) Which of them is not a major way of stealing email information?

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

(a) Explain procedures for Corporate High-tech Investigations with respect to:
i) Employee Termination Cases
ii) Email Abuse Investigation

(b) Explain the Investigation Triad

(c) What is data acquisition? What are its types? What is its goal? Explain.

(d) Explain acquiring data with dd command and dcfldd in Linux?

(e) What are the different acquisition tools in forensics? Explain any 5.

(f) What is network forensics? Explain the 3 modes of protection in DiD Strategy.

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

(a) Write a short note on Email Servers

(b) Write a short note on Ping and Port Scan

(c) What tcpdump and pcap? Explain.

(d) State and Explain the different types of content posted on social media?

(e) Explain Browser History and Browser Cache

(f) Explain the following:
   i) Web Server Logs
   ii) Virtual Hosts

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

(a) Write a short note on Corporate Investigations.
(b) What is authorized requestor? Why should companies appoint them for computer investigations?
(c) List the guidelines to document and prepare evidence
(d) What is deposition? Explain its types and any two guidelines for testifying at a deposition
(e) Explain Digital Signature and Electronic Signature
(f) Explain the following:
   i) Attribution of Electronic Records
   ii) Acknowledgment of Electronic Records
   iii) Dispatch of Electronic Records

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

(a) Define Computer Forensics.
(b) In the company-policy violation case, What are some initial assessments you should make for a computer investigation?
(c) Explain the role of e-mail in investigations.
(d) Write a short note on Traceroute
(e) Explain the following terms:
Affidavit b) exculpatory Evidence c) inculpatory Evidence
(f) List the general guidelines for Testifying
(g) What are the requirements to set up a workstation for computer forensics?
(h) Explain the trial process.

****