(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 ANY FOUR from the following: **(20M)**

(a) Explain role of maintaining Professional Conduct in cyber crime investigation?
(b) Explain testing procedures for private sector High tech investigations as an investigator.
(c) How to setup workstation for digital forensics.
(d) Describe the RAID Acquistions method.
(e) Write a note on Digital Evidence and its storage formats.
(f) Explain how we can acquire Hidden data from an image using steganography?

Q. 2 Attempt ANY FOUR from the following: **(20M)**

(a) Describe available digital forensics software tools.
(b) What are the steps in preparing for an evidence search
(c) Describe the types of graphics in file formats.
(d) Describe how to secure a computer incident or crime scene.
(e) How does the Windows Registry works?
(f) How to perform live network acquisition using wireshark tool

Q. 3 Attempt ANY FOUR from the following: **(20M)**

(a) What are the standard procedures for conducting forensic analysis of virtual machines?
(b) Describe standard procedures in network forensics and network-monitoring tools.
(c) What are the guidelines should follow for Writing Reports?
(d) Explain what is the roles of client and server in e-mail?
(e) Explain the use of E-mail server logs?
(f) Explain using FTK how will you perform email forensics on any give email .pst backup files.

Q. 4 Attempt ANY FIVE from the following: **(15M)**

(a) Define and explain digital forensics.
(b) Write note on "Evidence and its types".
(c) What are the procedures for acquiring data from mobile devices?
(d) Write the list of other forensics tools available for data acquisitions.
(e) Explain what are the methods for validating and testing forensics tools?
(f) Where are the legal challenges faced in conducting cloud forensics?