(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) What in an evidence custody form? What information does it contain?
(b) Explain the various storage Formats for Digital Evidence?
(c) Differentiate between public sector and Private sector investigations?
(d) Explain the necessary requirements for data recovery workstations and software?
(e) Write short note on Contingency Planning for Image acquisition?
(f) How will you analyse memory dump of a running computer system using FTK tool?

Q. 2 Attempt ANY FOUR from the following: (20M)
(a) What is the best way to determine the tools which you need for the digital investigation?
(b) Explain the necessary guidelines of seizing digital evidence at the scene?
(c) Describe how to collect evidence at private sector from incident scenes?
(d) Write a short note on recovering graphics files?
(e) Briefly explain copyright with graphics?
(f) How to detect hidden information or files within digital images using steganhide steganography tool and examine hidden content?

Q. 3 Attempt ANY FOUR from the following: (20M)
(a) Write short note on the network forensic?
(b) What is the general procedure for given live acquisition?
(c) Write a note on SIM card?
(d) Explain email header analysis?
(e) Explain the guidelines for report writing?
(f) How will you use the wireshark tool for identifying the live network, capture packets, analyse capture packets?

Q. 5 Attempt ANY FIVE from the following: (15M)
(a) Explain in detail advance forensic format?
(b) Explain short note on bitstream copies
(c) Explain types of data acquisition in detail?
(d) Explain the importance of investigation report?
(e) Explain acquisition procedures for mobile devices?
(f) Explain the technologies where the 4G networks can be used?

****

40181