Exam.Code: 1047
Sub. Code: 35464

2125

M.E. Computer Science and Engineering (Cyber Security)
Third Semester
CSN 8302: Digital Forensics

Time allowed: 3 Hours Max. Marks: 50

NOTE: Attempt five questions in all, including Question No. 1 which is compulsory and selecting two questions from each Unit.

x-x-x

1. Attempt the following:-
   a) What is the role of GRUB in Linux?
   b) Give differences between FAT32 and NTFS (any three points).
   c) What is forensic readiness? Mention two steps in forensic-readiness planning.
   d) What is remote imaging in digital forensics?
   e) What is RAM dump analysis? (5x2)

UNIT - I

2. a) Describe NTFS and ext4 file system layout in detail.
   b) What are the key features of FTK Imager that make it suitable for static data acquisition in digital forensic investigations? (2x5)

3. a) Write differences between Linux and Windows boot processes.
   b) Discuss the steps involved in recovering deleted or damaged partitions in Windows. (2x5)

4. Write a note on the following:-
   a) Post and boot loader
   b) Bulk extractor
   c) Mac OS boot sequence.
   d) OSI layers in network forensics (4x2½)

UNIT - II

5. a) What features of Wireshark make it a powerful tool for forensic packet analysis? Discuss essential TCP dump commands used in packet capture.
   b) What are the key features of E3 in performing remote disk imaging? (2x5)

P.T.O.

6. a) Describe volatile and non-volatile digital evidences. Explain how logs (system logs, security logs, firewall logs) are used as evidences.

   b) Compare the advantages of using Kali Linux over Windows for forensic investigations. (2x5)

7. a) What is Single Crack mode in John the Ripper, and why is it typically used first during password recovery?

   b) Explain the functional role of MIME headers in digital communication and the significance of Rainbow Tables. (2x5)

x-x-x