Exam.Code:1047
Sub. Code: 7636

2122

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. I which is compulsory and selecting two questions from each Unit.*

x-x-x

I. Attempt the following:-

a) List the steps for Forensic Readiness Planning?

b) What are the different types of digital evidences that can be acquired from crime scene?

c) Can we analyze the data on RAM of a digital system?

d) What is website penetration?

e) What are SQL injections? (5x2)

UNIT - I

II. Differentiate between NTFS and ext4 File system? What is the difference between Linux Loader Mac OS Loader and Windows Loader at boot time? (10)

III. a) How digital evidences are reported in court of Law? Describe the different parts of report in detail.

b) How can we recover deleted files? (7,3)

IV. a) What is difference between volatile and Non Volatile Information in Windows and Linux? Describe the role of FTK imager to retrieve this information.

b) What are the main features of KALI Linux? (7,3)

UNIT - II

V. What is packet Sniffing? Describe the use of Wireshark tool for Packet sniffing and analysis? Can we capture information from TCP DUMP? (10)

P.T.O.

VI. a) How Bulk extractor is used for data capturing? Describe how all evidences are audited?

b) What is significance of Log analysis? Which tool is preferred for Log Analysis? (2x5)

VII. a) What is the purpose of "John the Ripper"? How Rainbow tables are created?

b) What is MIME header? How Email investigations are conducted? How IP trace back is done? (2x5)

x-x-x