(b) Analysis tools and techniques for digital evidence at physical layer (10)

7. (a) What is filtering and data reduction ? (10)

(b) Explain the role of internet in criminal investigations. (10)

Section-D

8. Write short notes on :

(a) Location as alibi (10)

(b) Cyber stalking (10)

9. (a) What do you mean by intrusion ? Explain intrusion handling process. (10)

(b) Explain forensic preservation of volatile data. (10)

Roll No. ....

23588

M.Tech. 3rd Semester (Forensics and Information Security) Examination– December, 2016

PRESERVING & RECOVERING DIGITAL EVIDENCE

Paper : MTCF-301

Time : 3 hours ***Max. Marks : 100***

Before answering the questions, candidates should ensure that they have been supplied the correct and complete question paper. No complaint in this regard will be entertained after the examination.

Note: Question No. 1 is **compulsory**. Attempt **five** questions in total selecting **one** question from each section.

1. (a) Define the term 'digital evidences'. (2.5)

(b) What is a malware ? (2.5)

(c) What do you mean by recovery of evidence ? (2.5)

(d) How log files are helpful in digital investigation ? (2.5)

(e) What do you mean by location as alibi ? (2.5)

(f) What is internet trace file ? (2:5)

(g) Define the term 'IRC'. (2.5)

(h) What do you mean by forensic investigation ? (2.5)

Section-A

2. What do you mean by digital investigation ? Explain one digital investigation process model. (20)

3. (a) Explain various crime scene characteristics. (10)

(b) Explain various technologies for digital investigation. (10)

Section-B

4. Write notes on : (20)

(a) Digital evidence processing tools

(b) Role of trace files in digital investigation

(c) Data hiding

5. (a) Explain the process of forensic examination of Windows system. (10)

(b) Explain data recovery process in Mac OS. (10)

Section-C

6. Writes notes on :

(a) TCP/IP related digital evidence (10)