(b) Analysis tools techniques for digital evidence at ph l layer (10)

7. (a) What is filteri i data reduction ? (10)

(b) Explain the r f internet in criminal investigations. (10)

Se ı-D

8. Write short notes

(a) Location as al (10)

(b) Cyber stalkin (10)

9. (a) What do yo ean by intrusion ? Explain intru andling process. (10)

(b) Explain foren reservation 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 n by recovery of evidence ? (2.5)

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

(e) What do you me location as alibi ? (2.5)

(f) What is internet file ? (2.5)

(g) Define the term (2.5)

(h) What do yo ean by forensic investigation ? (2.5)

Sect

2. What do you mean gital investigation ? Explain one digita vestigation process model. (20)

3. (a) Explain vari 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)