Roll No. .....

23588

M. Tech. 3rd Semester (Forensics and Information Security) Examination – December, 2014

PRESERVING & RECOVERING DIGITAL EVIDENCE

Paper : MTCF-301

Time : Three Hours] *[Maximum 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 examination.

Note : Question **1** is ***compulsory***. Attempt ***five*** questions in total selecting ***one*** from each Section.

1. Explain the following : $4 \times 5 = 20$

(a) Crime scene characteristics.

(b) Data recovery in mac os.

(c) Filtering and data reduction at network layer.

(d) Processing the digital crime scene.

SECTION – A

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

3. Explain the following :

(a) Modus operandi. 10

(b) Threshold assessments. 10

SECTION – B

4. Write notes on : 20

(a) Password protection and encryption

(b) Role of log file in digital investigation

(c) Data hiding

5. (a) Explain various digital evidence processing tools. 10

(b) Explain data recovery process in UNIX. 10

SECTION – C

6. Write notes on : 20

(a) Forensic science at network layer

(b) E-mail forgery and tracking

7. (a) Explain the use of internet as investigation tool. 10

(b) Explain various tools and techniques for digital evidence at transport layer. 10

SECTION – D

8. Write notes on : 20

(a) Time as alibi

(b) Cyber stalking

(c) Forensic preservation of volatile data

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

(b) Explain malicious program investigation process. 10