B.E-VIII | COMP/DF/ 12-05-2017
CBGS

Digital forensic

QP Code : 11996

(3 Hours) Total Marks: 80

N.B.: (1) Question No.1 is compulsory.
(2) Attempt any three questions from the remaining five questions.
(3) Make suitable assumptions wherever necessary but justify your assumptions.

1. (a) What is incident response? Explain goals of incident response. 05
   (b) Explain the term Cyber terrorism with examples. 05
   (c) What is Evidence? Explain the types of Evidence. 05
   (d) What is DOS attack? How to achieve recovery from DOS attack? 05

2. (a) Explain volatile data collection procedure for Windows system. 10
   (b) What are possible investigation phase carried out in Data Collection and Analysis. 10

3. (a) Explain Incident Response Methodology in detail. 10
   (b) What are the steps involved in computer evidence handling? Explain in detail. 10

4. (a) Explain importance of forensic duplication and its methods. 10
   (b) Describe levels of culpability. 10

5. (a) Explain various ethical issues concern in computer forensics. 10
   (b) How you will trace the crime which has been happened through email using tool. 10

6. Write a short note on 20
   (1) NTFS Disk
   (2) Laws related to computer forensic
