

Digital forensic

/comp (CBBS)

sem- VIII / 12-05-16

Q.P.Code : 725000

(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 Cyber Crime? How do we classify Cyber Crimes? 05
- (b) What is some of the volatile information you would retrieve from a computer system before powering it off? 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) What is Digital Forensics? What are the phases of Digital Forensics process? 10
- (b) Define Forensic Duplicate? How you will create Forensic Duplicate of a hard drive. 10
3. (a) Briefly explain the process of collecting the volatile data in digital forensics. 10
- (b) What are the steps involved in computer evidence handling? Explain in detail. 10
4. (a) What are the tools used in Network forensics. 10
- (b) Discuss the techniques of tracing an e-mail message. 10
5. (a) Explain how law enforcement is done in computer forensics. 10
- (b) Worksource Private Limited is a business process outsourcing (BPO) outfit handling business process outsourcing for various clients in North America and Europe. The employees of Worksource become privy to confidential customer information during the course of their work. The nature of this information ranges from medical records of individuals to financial data of companies. The unprocessed data is transmitted from the client's location to Worksource offices in Gurgaon, Pune and Hyderabad through the Internet using VPN (Virtual Private Network) connections on broadband. Worksource allows clients to transfer information via dedicated FTP servers on the Internet, which can then be accessed and processed by its employees. Worksource, through its website, worksource.com allows its clients to log in and view billing and other information specific to them. Access to this information is restricted through the usual user name - password combination found on most websites.

Looking at the above scenario, discuss the threats Workforce faces to its information and suggest controls which it may put in place to secure its information from such threats.

6. Write a short note on

(1) NTFS Disk

(2) Windows Registry

20