Name of Subject	Computer Forensics	**Subject Code**	DEIT-14718 (Elective-IV)
Batch	2014 and onwards	**Class**	D4IT

Each following question carries 02 marks.

1. Describe Your Home Network.
2. What Is The Difference Between Threat, Vulnerability And Risk?
3. If You Needed To Encrypt And Compress Data For Transmission, Which Would You Do First And Why?
4. What Are Some Tools Used To Recover Deleted Files?
5. How Would You Be Able To Tell At The Hex Level That A File Has Been Deleted In Fat12?
6. What Is An Acl?
7. Describe Some Of The Vulnerabilities Listed On The Owasp Top 10 Vulnerabilities List?
8. What Are Some Security Issues Related To The Cloud?
9. What Port Does Dns Run Over?
10. How Would You Handle Retrieving Data From An Encrypted Hard Drive?
11. Describe The Sha-1 Hash?
12. What Are Some Common Port Numbers?
13. What Is Steganography?
14. What Operating Systems Do You Use?
15. What Type Of Email Analysis Experience Do You Have?
16. What Is Data Mining?
17. Define key encryption algorithm identifier.
18. What Is Data Carving?
19. What Is A Sam File?
20. Define cryptographic message syntax.
21. What Is An .iso File?
22. What Is Md5 Checksum?
23. Name Some Common Encryption Algorithms That Are Used To Encrypt Data?
24. What are three main categories of firewall?
25. When is the best time to contact a forensic company?

26. How do I remove a computer that is turned on?
27. Can I just have an image taken of a device?
28. Can't my IT person or another employee look through the data?
29. What industries does Computer Forensics deal with?
30. Define firewall.
31. An employee departs the company, a few weeks later or less, the company notices a drastic drop in sales and/or clients.
32. An employee was fired for lack of production; now he/she is saying that they were wrongfully terminated.
33. An employee leaves the company and starts working for a competitor. In a short amount of time, the competitor releases a new formula that your company was working on for months/years.
34. Define an armor headline.
35. What Is Computer Forensics?
36. What is Shannon-Fano coding?
37. Why hire a computer forensics company or investigator?
38. Who can use the computer forensic evidence?
39. What is meant by trusted platform module?
40. What is meant by Huffman compression?
41. State the objectives of computer forensics.
42. What is a chain of custody?
43. Define packet headers.
44. What are the roles of a computer in a crime?
45. Define MIME.
46. Define computer crime and digital crime.
47. What do expert witness services provide?
48. What are the Federal Rules of Evidence?
49. Define FAT.
50. What is meant by encrypting file system?

Each following question carries 05 marks.

1. Computer forensics involves obtaining and analyzing digital information for use as evidence in civil, criminal, or administrative case.
2. State the types of computer records.

3. How Can Computer Forensics Help Me?
4. List some digital forensic tools.
5. Who needs computer forensics?
6. What is the difference between Computer Forensics and E-Discovery?
7. What types of devices can forensic evidence be found on?
8. Briefly describe the triad that makes up computer security
9. Briefly describe the main characteristics of public investigations
10. Briefly describe the main characteristics of private investigations.
11. What are the three levels of law enforcement expertise established by CTIN?
12. What are some of the most common types of corporate computer crime?
13. What is embezzlement?
14. Passwords are often used to protect access to computer resources. What is a brute-force attack in relation to passwords?
15. What is an affidavit?
16. What is attorney-client privilege (ACP)?
17. Companies often use forensics techniques in disaster recovery to retrieve information they have lost. Give 2 (two) things that companies should do or put in place that will assist this recovery before the disaster strikes.
18. What is steganography? Briefly describe how it is used to protect copyrighted material.
19. Differentiate between SSL protocol and TSL protocol.
20. When acquiring data in an investigation, there are situations when sparse Acquision is used. What is sparse acquisition? Describe the situation where sparse acquisition is used?
21. Distinguish between encryption and decryption.
22. What do you know about key management for IPSec?
23. Cell phones and mobile devices have often been used in committing crimes. What are the two main concerns in the search and seizure procedures for cell phones and mobile devices? Give reasons for these concerns. Is necessary for the mobile equipment to function. Give 4 (four) uses or purposes that the SIM card provides.
24. What do I do if I suspect wrong doing or inappropriate activity?
25. What do I do if I am facing an investigation?
26. Do I pay for services if the evidence I am looking for is not found?

Each following question carries 10 marks.

1. What Kinds of computer forensic investigations do you perform?
2. It is important for companies to formally establish and publish their policies regarding forensic investigations. Give 4 (four) aspects or areas where these policies should address.
3. Demonstrate the SET system participants with a diagram.
4. What are the steps in a computer forensic investigation?
5. Describe the transaction protocols required for secure payment processing.
6. Identify security associations with the help of three parameters.
7. What types of electronic data is considered evidence?
8. Evidence integrity is essential in order for digital evidence to be admissible in court and to carry weight as evidence. What is CoC (Chain of Custody) and why is it important for evidence integrity? Assuming that a forensic team follows the right steps for preserving evidence integrity and for keeping an unbroken CoC, what must they do in order to convince the court that they have done so? What is OOV (order of volatility), and how does it influence decisions regarding which evidence should be preserved first? List various data storage media as a function of their OOV.
9. Explain the di5erence between “live acquisition” and “post mortem acquisition”? What are the advantages and disadvantages of live and post mortem acquisition? Give an example when “live acquisition” is necessary.
10. Examine the traditional computer crimes associated with cyber forensics.
11. Explain in details about incident response methodology and six steps associated with it.
12. Analyze briefly about forensic duplication and investigation.
13. Demonstrate how to use remote network acquisition tools in cyber forensics?