

COMPUTER FORENSICS

UNIT I

PART A

- 1) What is computer forensics?
- 2) List the Difference between Computer Forensics and Computer Security.
- 3) Write the Benefits of Professional Forensics Methodology?
- 4) Define data recovery.
- 5) What is DIRT?
- 6) List out the Forensic Services.
- 7) What are the obstacles to back-up applications?
- 8) What is Data Archiving?
- 9) What are the many factors can be affect the back up to day?
- 10) Write short notes on conventional tape back-up in today's market?

PART B

- 11) Discuss with the use of computer forensics in law enforcement and Computer forensics assistance to human resources and employment proceedings.
- 12) Discuss the computer forensics specialists.
- 13) Discuss the any two issues for data back-up and recovery in computer forensics
- 14) Discuss the network path and recovery the data back-up window in computer forensics.
- 15) What is role of back up in data recovery and discuss the factors that affect the back up in computer Forensics?
- 16) Discuss the back up and data recovery solution for the information management system product in Computer forensics?

UNIT II

PART A

- 1) What is conventional evidence collection?
- 2) List out the Necessity of Evidence Collection.
- 3) Define Evidence Collection Options.
- 4) What are the reasons for Electronic crime is difficult to investigate and prosecute?
- 5) Define real Evidence in Computer Forensics.
- 6) What is meant by Hearsay?
- 7) List out proceed from volatile to persistence evidence.
- 8) Define Artefact.
- 9) What is freezing scene the form of evidence collection in computer forensics?
- 10) Write short notes on any two collection steps invoked in the evidence collection?

Part B

- 11) Discuss with the Obstacles in collection evidence of computer forensics. **Or**
- 12) Discuss with the rules of electronics evidence collections in computer forensics.
- 13) explain the Do's and Don'ts in the process of collecting electronics evidences. **Or**
- 14) Write short notes on
 - i) General four steps procedure in evidence collections.
 - ii) Method of collections.
- 15) Discuss with the guidelines control by contamination in the evidence collection. **Or**
- 16) Discuss with how to make duplication and preserving the digital crime in the evidence collection of computer forensics.

UNIT-III

PART A

1. What is validating forensic data?
2. What is addressing data hiding techniques?
3. What is a remote acquisition?
4. What is investigation
5. What is network forensic overview?
6. What is hash?
7. Explain about reviewing a case
8. How to collect evidence in private sector
9. What is network?
10. What is search?

PART B

1. Determining what data to collect and analyze? **or**
2. Explain seizing digital evidence at the scene? **or**
3. Examining the honey net project? **or**
4. Explain about storing digital evidence? **or**
5. Explain about security? **or**
6. Explain about Identifying digital evidence

UNIT IV

PART A

1. What are the two major categories Computer Forensics tools?
2. What are the five major functions are performed into the Computer forensics tools?
3. What are the sub functions of the validation and discrimination function in Computer forensics tools?
4. What is NSRL?
5. Write short notes on Data viewing?
6. Define Carving.
7. Define Distributed Network Attack.
8. What are the sub functions of reconstruction in acquisitions of Computer forensics tools?
9. What are the tools that perform an image-to-disk copy?
10. What are the sub functions of the reporting function in computer forensics?
11. Define Command-Line Forensics Tools.
12. Define Helix
13. Write short notes on Knoppix-STD.
14. What is the Role of E-mail in Investigations

PART-B

- 1) Briefly explain types of computer forensics tools and how they are performed by computer forensics tools.
- 2) Explain validation discrimination computer forensics
- 3) Explain computer forensics software tools?
- 4) How to retrieve information from cell phones or mobile device forensic, explain it.?
- 5) Explain the understanding acquisition procedure for cell phone mobile device?
- 6) Write short notes on
 - i) Mobile forensics equipment
 - ii) Sim card card reader

UNIT-V

PART –A

1. Define file system
2. What is disk partitions
3. What is NTFS file system
4. Define file attributes
5. List out the any five MS DOS commands
6. Define virtual machine
7. What is the two modes of windows XSOS?
8. Define windows registry
9. Define key
10. Define master BOOT record

PART-B

1. Discuss the file system in windows and DOS
2. Write a neat diagram, explain the the disk driver
3. Explain the examine FAT disk
4. Explain the MFT AND file attribute in windows and DOS systems
5. Discuss the registry in windows and DOS
6. Briefly explain the virtual machine