



Avinashilingam Institute for Home Science and Higher Education for Women
(Deemed to be University under Category 'A' by MHRD, Estd. u/s 3 of UGC Act 1956)
Re-accredited with A+ Grade by NAAC. Recognised by UGC Under Section 12B
Coimbatore - 641 043, Tamil Nadu, India
Continuous Internal Assessment –I - February 2024
Semester-II

Class: I PG

Branch : Information Technology

Time: 2Hours

Max. Marks: 60

23MITI01– CYBER FORENSICS

Course Outcomes:

CO1 : Describe the essential computer forensic technologies, services and vendors in the field of digital forensic science

CO2 : Demonstrate knowledge in numerous forensic tools and utilization of tools for data recovery and image verification procedures.

CO3 : Identify the significance of a systematic procedure to investigate electronic data in order to discover digital evidence of unlawful activity.

CO4 : Manage with threats related to security and information warfare

CO5 : Procure hypothetical knowledge in many areas of computer forensic investigations.

Part A

6 x 1 = 6

Choose the Correct Answer

- Computer evidence must be _____ CO1 K1
a. Convincing to juries b. Authentic c. Admissible d. All the above
- _____ are secure and tamperproof containers used to store digital evidence. CO2 K1
a. CFX b. Digital Diary c. Digital Space d. DEBs
- _____ creates copies or snapshots of a file system at a particular point in time. CO2 K2
a. Incremental Backup b. Image backup c. Remote backup d. None
- Which is the process of creating a replica system and luring the attacker into it for further monitoring? CO1 K2
a. Freezing the scene b. Honeypotting c. Sandboxing d. Remote Monitoring
- _____ is the leftover storage that exists on a computer's hard disk drive when a computer file does not need all the space it has been allocated by the operating system. CO1 K2
a. Unallocated Space b. Achieves c. Slack space d. None
- When collecting evidence, the investigator should always start from _____ CO1 K3
a. Most volatile b. Least volatile c. Both of them d. None

Part B

3 x 6 = 18

Answer ALL questions

Each answer should not exceed 400 words or two pages

- a. Identify who can use Computer Forensic Evidence CO1 K1
(Or)
- b. Describe the Military Computer Forensic Technology CO1 K2
8. a. Discuss about the Data Recovery CO2 K2
(Or)
- b. Demonstrate the Duplication and Preservation of Digital Evidence CO2 K3
9. a. Sketch the Time matters in Data Identification CO3 K3
(Or)
- b. Organize the rules to be considered when collecting digital evidence CO3 K4

Part C

3 x 12 = 36

Answer ALL questions

Each answer should not exceed 800 words or four pages

- 10.a. Recognize the types of Computer Forensics Technology CO1 K1
(Or)
- b. Illustrate the types of Vendor and Computer Forensics Services CO1 K3
- 11.a. Show Evidence Collection and Data Seizure CO2 K3
(Or)
- b. Explain detail about Computer Image Verification and Authentication CO2 K2
- 12.a. Construct various processes in discovery of electronic evidence CO3 K3
(Or)
- b. Analyze the Identification of data in Computer Forensic Analysis CO3 K4

No of Copies: 15

