| Reg. No. | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|

**B.Tech. DEGREE EXAMINATION, MAY 2024**
Sixth & Seventh Semester

18CSE382T – FORENSICS AND INCIDENT RESPONSE
*(For the candidates admitted during the academic year 2018-2019 to 2021-2022)*

**Note:**
(i) **Part - A** should be answered in OMR sheet within first 40 minutes and OMR sheet should be handed over to hall invigilator at the end of 40th minute.
(ii) **Part - B & Part - C** should be answered in answer booklet.

Time: 3 hours Max. Marks: 100

**PART – A (20 × 1 = 20 Marks)**
Answer **ALL** Questions

| | Marks | BL | CO | PO |
|---|---|---|---|---|
| 1. Identify the one which is not involved in phases of initial response?<br>(A) Assemble CSIRT (B) Ensure the incident<br>(C) Assessing the impact (D) Measuring data | 1 | 1 | 1 | 5 |
| 2. Evidence collected from network device logs are known as _____.<br>(A) Flow analysis (B) Active acquisition<br>(C) Model of detection (D) Packet analysis | 1 | 2 | 1 | 1 |
| 3. Recovering and analyzing digital evidence from network resources<br>(A) TCP port scan (B) Protocol analysis<br>(C) Web proxies (D) Network forensics | 1 | 1 | 2 | 5 |
| 4. Which of the following describe malicious computer programs such as viruses, worms and trojan horses?<br>(A) Software piracy (B) Malware<br>(C) Larceny (D) Arson | 1 | 1 | 1 | 3 |
| 5. Which of the following techniques are not used during computer forensics investigations?<br>(A) Cress drive analysis (B) Live analysis<br>(C) Deleted files (D) Fuzzy logic tools | 1 | 2 | 2 | 5 |
| 6. _____ is related to the verification process which involved sorting and searching through investigation files to separate the normal and suspicious data<br>(A) Kali Linux (B) Validation<br>(C) Reporting (D) Filtering | 1 | 2 | 2 | 1 |
| 7. _____ is used to identify compromised hosts, confirm or disprove data leakage, and for individual profiling<br>(A) Protocol analysis (B) Statistical flow analysis<br>(C) Network forensics (D) Packer analysis | 1 | 3 | 3 | 4 |
| 8. Volatile data NOT resides in?<br>(A) Registries (B) Cache<br>(C) RAM (D) ROM | 1 | 2 | 3 | 2 |

9. NTFS stands for _____. 1 1 2 1

(A) Network File System (B) Nano Technology File System
(C) New Technology File System (D) Network Technology File System

10. Mapping of file is managed by _____. 1 1 3 5

(A) File metadata (B) Page table
(C) Virtual memory (D) File system

11. Smallest addressable storage unit on hard disk typically 512 byte addresses are CHS and LBA. 1 2 3 5

(A) FAT (B) Bit
(C) Sector (D) MBR

12. Independent organizational structure that allows the user to store and retrieve data is called _____. 1 2 2 5

(A) File system (B) Files
(C) File stack (D) File system area

13. What is an unauthorized movement of data? 1 1 3 2

(A) Data cracking (B) Data infiltration
(C) Data exfiltration (D) Database hacking

14. If your actions are the result of misleading, intentional actions or inaction including misleading statements and the omission of relevant information to gain an advantage, then you have committed. 1 2 4 3

(A) Perjury (B) Contempt
(C) Treason (D) Fraud

15. _____ is an equitable remedy designed to deter future violations of the securities law and to deprive defendants of the proceeds of their wrongful contact 1 2 2 1

(A) Disgorgement (B) Penalty
(C) Insider information (D) Proceedings

16. Cyber trails are advantages because _____. 1 2 3 3

(A) They are not connected to the physical world (B) Nobody can be harmed by crime on the internet
(C) They are easy to follow (D) Offenders who are unaware of them leave behind more clues than they otherwise would have

17. A report or account is an _____. 1 3 2 3

(A) Informational work (B) Technical work
(C) Professional work (D) Analytical report

18. Report uses the features of 1 2 4 6

(A) Mobile (B) Graphics and images
(C) Method (D) Account

19. In report writing, the language used to be is _____. 1 1 3 2

(A) Loudly (B) Unclear
(C) Whispers (D) Ambiguous

| | | | | | |
|---|---|---|---|---|---|
| 20. | The length of informal report should be _____.<br>(A) 13 pages (B) 1-3 pages<br>(C) 1/5 - page (D) Full page | | 1 | 2 | 3 | 8 |

**PART – B (5 × 4 = 20 Marks)**
Answer **ANY FIVE** Questions

| | | Marks | BL | CO | PO |
|---|---|---|---|---|---|
| 21. | Discuss on the process of crafting a response toolkit specially tailored for Linux systems. | 4 | 2 | 1 | 1 |
| 22. | Write down the procedures necessary for pre-incident preparation. | 4 | 1 | 1 | 2 |
| 23. | Explain the understanding storage formats for digital evidence in detail. | 4 | 2 | 2 | 3 |
| 24. | Write a short notes on NTFS metadata category. | 4 | 1 | 3 | 3 |
| 25. | Explain in detail about detecting loadable kernel modules. | 4 | 2 | 2 | 5 |
| 26. | Discuss in detail about the guidelines for writing reports. | 4 | 2 | 4 | 6 |
| 27. | Explain in detail computer forensics hardware tools. | 4 | 2 | 5 | 1 |

**PART – C (5 × 12 = 60 Marks)**
Answer **ALL** Questions

| | | Marks | BL | CO | PO |
|---|---|---|---|---|---|
| 28. a. | Discuss on the process of developing a windows response toolkit. | 12 | 2 | 2 | 2 |
| | **(OR)** | | | | |
| b. | Illustrate how will the processing of an incident or a crime scene takes place in cyber forensics. | 12 | 2 | 2 | 3 |
| 29. a. | Describe in detail about using specialized E-mail forensics tools. | 12 | 2 | 2 | 5 |
| | **(OR)** | | | | |
| b. | Explain the types of evidence handling in detail. | 12 | 2 | 3 | 1 |
| 30. a. | Explain in detail about how the understanding of file systems plays a crucial role in cyber forensics. | 12 | 2 | 2 | 3 |
| | **(OR)** | | | | |
| b. | Demonstrate the most common method of evidence presentation during on incident response. | 12 | 2 | 2 | 2 |
| 31. a. | Analyze briefly about the forensic duplication and investigation. | 12 | 4 | 3 | 1 |
| | **(OR)** | | | | |
| b. | Explain about an identifying unauthorized user accounts groups of investigation system. | 12 | 4 | 3 | 4 |

| | | | | | | |
|---|---|---|---|---|---|---|
| 32. a. | Describe the validating and testing computer forensics software in detail. | 12 | 2 | 4 | 5 |
| | **(OR)** | | | | |
| b. | Outline the importance of forensic report writing. | 12 | 2 | 5 | 5 |

* * * * *