(A) Written informal report (B) Written formal report
(C) Verbal informal report (D) Verbal formal report

PART – B (5 × 10 = 50 Marks) | Marks | BL | CO | PO
Answer **ALL** Questions

26. a. Write the goals of incident response in forensic science and discuss major components of incident response. | 10 | 2 | 1 | 1

(OR)

b. Explain in detail about creating tool kit in Unix, volatile data collection and strong collected data. | 10 | 2 | 1 | 1

27. a. Explain in detail about Association of Chief Police Officers (ACPO) principles of computer based evidence. | 10 | 2 | 2 | 1

(OR)

b. Analyze, how the following techniques are used | | 2 | 3 | 1
(i) Documents evidence in the lab | 5
(ii) Processing and handling digital evidence | 5

28. a. Describe in detail about key capabilities of effective managed file transfer and list the benefits of managed file transfer. | 10 | 2 | 4 | 1

(OR)

b. With the diagrammatic representation, explain in detail about the working methodology of file allocation and file deletion in NTFS big picture with an example. | 10 | 2 | 4 | 1

29. a. Outline the problems and challenges of forensic examiners face when preparing and processing investigation. | 10 | 3 | 5 | 4

(OR)

b. Your organization believes that a system with the IP address of 172.16.4.31 has been compromised by a computer with the IP address of 172.16.3.61 you are uncertain how the system may be compromised or what service was exploited. However you do know that the system's log files on 172.16.4.31 have been deleted. And that no person was logged into the system locally when the files were deleted. What fileting would you perform to minimize the traffic intercepted. | 10 | 3 | 4 | 5

30. a. Explain in detail about the task performed by computer forensics tools. | 10 | 2 | 6 | 1

(OR)

b. Write short notes on the following | | 2 | 6 | 6
(i) Understanding the importance of reports | 3
(ii) Guidelines for writing report | 3
(iii) Generating report, finding with forensics software tools | 4

* * * * *

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

B.Tech. DEGREE EXAMINATION, NOVEMBER 2022
Sixth/ Seventh Semester

18CSE382T – FORENSICS AND INCIDENT RESPONSE
(For the candidates admitted from the academic year 2018-2019 to 2019-2020)

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** should be answered in answer booklet.

Time: 2½ Hours Max. Marks: 75

PART – A (25 × 1 = 25 Marks) | Marks | BL | CO | PO
Answer **ALL** Questions

1. Which of the following is a security incident indication? | 1 | 1 | 1 | 1
(A) A system alarm or similar indication from an intrusion detection (B) DoS attack or user not able to log into an account
(C) System crashes or poor system performance (D) Attempt to logon to a new user account

2. Which of the following is not correct about a computer incident response team? | 1 | 1 | 1 | 1
(A) A group that handles event involving computer security breaches
(B) A non profit professional organization made up of member incident response teams
(C) A concrete organizational entity, that is assigned the reasonability of providing part of the incident management capability for a particular organization
(D) The collected information about incident is irrelevant to be used to determine trends and patterns of intruder activity and recommend corresponding preventative strategies for whole consistency

3. What information is gathered during a live response? | 1 | 1 | 1 | 1
(A) Current network connections running processes and open files (B) Files transferred
(C) Data created and deleted (D) File executed

4. Which type of data is collected in volatitling data collection? | 1 | 1 | 1 | 1
(A) Random access memory (B) Read only memory
(C) Virtual memory (D) Secondary memory

5. In Unix, which command is used to change the permission of a file? | 1 | 1 | 1 | 1
(A) CHOWN (B) CHGRP
(C) CHMOD (D) CH

6. The storage device that uses rigid, permanently installed magnetic disk to store data is — 1 1 2 1
   (A) Floppy disk (B) Permanent disk
   (C) Optical disk (D) Hard disk

7. Forensic duplicate image means an exact _____ copy of a piece of digital evidence. — 1 1 3 1
   (A) Bit-for-Bit (B) Byte-for-Byte
   (C) Word-for-Word (D) Sector-for-Sector

8. What tool below was written for MS-DOS and commonly used for other operating system manual digital investigation? — 1 1 2 1
   (A) Smart (B) Norton diskedit
   (C) Byte back (D) Data lifter

9. Which of the following is not type of volatile evidence — 1 1 3 1
   (A) Routing tables (B) Main memory
   (C) Log files (D) Cached data

10. A digital investigator pursuing a line of investigation in a case because that line of investigation proved successful in two previous cases in an example of — 1 2 3 1
   (A) Logical reasoning (B) Common sense
   (C) Preconceived theory (D) Investigation intuition

11. Fat 32, supports partitions upto _____ in size. — 1 1 4 1
   (A) 4 GB (B) 2 GB
   (C) 256 GB (D) 2047 GB

12. Fat can support upto a maximum of ____ of allocation units on a hard disk. — 1 1 4 1
   (A) 64 bytes (B) 512 bytes
   (C) 64 kilobytes (D) 512 kilobytes

13. The "Big picture" diagram of a system is the _____. — 1 1 4 1
   (A) Block diagram (B) Logic diagram
   (C) System flow chart (D) Program flow chart

14. Which of the following NTFS folder permission give users only the right to view the name of sub folder and files in a folder? — 1 1 4 1
   (A) Read (B) Write
   (C) Read and execute (D) List folder contents

15. Which feature create a log file to keep track of file information such as additions, deletion and modification for each NTFS volume? — 1 2 4 1
   (A) Native structured storage (B) Disk quotas
   (C) Change journal (D) Line tracking and object identifiers

16. Which of the following are true about consistency semantics.
   S1: In unis file system: write to an open file are immediately visible to any user who has file open
   S2: In Andrew file system: write to an open file are immediately visible to other users
   (A) S1 only (B) S2 only
   (C) S1 and S2 are true (D) S1 and S2 are not true

17. Which of the following allow user to modify a shared file permission? — 1 1 5 1
   (A) Modify (B) Change
   (C) Read (D) Full control

18. Forensic investigators perform except the following — 1 1 5 1
   (A) Detect the extent of a security breach (B) Recover found data
   (C) Recover lost data (D) Determine how an intruder got past security mechanism

19. Choose the correct methodology based on the given terms. — 1 2 5 4
   File manipulation: file name, extn, hidden property
   Disk manipulation: hidden partitions / bad clusters
   Encryption: bit shifting/ stenography
   (A) Windows registry (B) Examination plan
   (C) Virtual machine (D) Data hiding techniques

20. You want to create roaming profile for user in the sales department, they frequently log on at computer in a central area. The profile should be configured as mandatory and roaming profiles, which user are able to manage mandatory profile on windows computer. — 1 2 5 4
   (A) The user who uses the profile (B) Server operators
   (C) Power users (D) Administrators

21. Why would hackers want to cover their tracks? — 1 1 6 1
   (A) To prevent another person from using the programs they have installed on a target system (B) To prevent detection of discovery
   (C) To prevent hacking attempts (D) To keep other hackers from using their tools

22. Why it is necessary to clear the event log after using the auditpol command to turn off logging? — 1 1 6 1
   (A) The auditpol command places an entry in the event log (B) The auditpol command doesnot stop logging until the event log has been cleared
   (C) Auditpol relies on the event log to determine whether logging is taking place (D) The event log does not need to be cleared after running the auditpol command

23. Which type of hacker represent the highest risk to your network? — 1 1 6 1
   (A) Black hat hackers (B) Grey hat hackers
   (C) Script kiddies (D) Disgruntled employees

24. The most popular software forensic tools include all of the following except — 1 1 6 1
   (A) Forensic autopsy® (B) Quicken®
   (C) Forensic toolkit® (D) Smart®

25. The forensic report writing is classified into four types and which of the following report type is less structured than a formal report and is delivered in person usually in an attorney's office or police station. — 1 1 6 6