Reg. No

B.Tech DEGREE EXAMINATION, NOVEMBER 2023

Sixth & Seventh Semester

18CSE382T - FORENSICS AND INCIDENT RESPONSE

(For the candidates admitted during the academic year 2020 - 2021 & 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** and **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
1.	Computer Security incident is always (A) Lawful (B) Authenticated (C) Unacceptable (D) Illegal	1	1	1
2.	Choose the proactive step that should be taken before the Computer Security Incident (A) Pre-Incident Preparation (B) Initial Response (C) Data Collection (D) Data Analysis	1	1	1
3.	Which of the Response Strategy can be considered for the DOS security attack? (A) Interview with suspect (B) Reconfigure router to minimize effect of the flooding (C) Make public affairs statement (D) Investigation of theft	1	1	1
4.	Who is solely responsible for the evidence collected and stored for examination? (A) Evidence Custodians (B) Evidence Examiners (C) Evidence Collectors (D) Evidence Analyzer	1	1	2
5.	The evidence collected should be maintained under ___________ to ensure that it is not accessed by the unauthorized users. (A) Chain of Custody (B) Access Specifiers (C) Access Control List (D) Evidence Duplication	1	1	2
6.	Non Content Monitoring does not include the content about _____ (A) Port (B) IP Address (C) Protocol (D) Application Software	1	1	2
7.	Which of the following utility is used to create forensics duplicate image? (A) ff (B) dd (C) ee (D) cc	1	1	2
8.	Independent structure that allows to store and retrieve data is called as ________ (A) File Structure (B) File System (C) File Map (D) File Slag	1	1	3
9.	The mapping of the files in the memory is done by ________ (A) MetaData (B) MicroData (C) File System (D) File Table	1	1	3
10.	A initial section of disk at each partition is set restricted to maintain the ______ (A) FAT (B) Linked List (C) Linked Array (D) Linked Stack	1	1	3

11. Which of the following is the most common activity performed to break the system? 1 1 3

(A) Escalating Privileges (B) Information Collection

(C) Password Cracking (D) Track Dislocation

12. A statement which is the result of an investigation of any matter on which definite information required is ________ 1 1 4

(A) Mail (B) Report

(C) Application (D) Contract

13. Identify the criteria which states the exact purpose of the report. 1 1 4

(A) Format (B) Specification

(C) Title (D) Revision Number

14. Rules created by the US supreme court that govern how evidence can be used in both civil and criminal cases 1 1 4

(A) Federated rules of Evidence Act (B) Federated rules of Proof Act

(C) Federated rules of Evidence (D) Federated rules of Governance

15. Which of the following contain the blueprint of how routers forward the packet? 1 1 4

(A) Firewall Entry (B) ISA

(C) Router Table (D) Index Table

16. Which of the forensics software freely available and open sourced? 1 1 5

(A) Autopsy (B) Encase

(C) FTK (D) MS Office

17. Which among the following cannot be considered as Digital Evidence? 1 1 5

(A) System Logs (B) Network Traffic

(C) Eye Witness (D) Application Logs

18. Why is the need of hashing in Digital Evidence? 1 1 5

(A) To encrypt the data for security purpose (B) To verify the integrity of the digital Evidence

(C) To delete all the unwanted files (D) To analyze the victim system

19. Which of the following analysis can be used to get an complete interconnection between all the evidence? 1 1 5

(A) Timeline Analysis (B) Log File Analysis

(C) Recycler Analysis (D) Route File Analysis

20. Which of the following tools should not be used to recover the deleted files? 1 1 1

(A) Using undelete tools (B) Recovering .tmp files

(C) Restoring files located in the Recycle Bin (D) Tools to retrieve data in Cache Memory

PART - B (5 × 4 = 20 Marks) Marks BL CO

Answer **any 5** Questions

21. Show how the Digital Evidence is stored. Explain in detail. 4 1 3

22. Explain the Pre-Incident preparation that has to be done in an Organization. 4 1 1

23. State the ACPO Principles of computer based Evidence. 4 1 2

24. Explain how to perform the Keyword Search effectively. 4 1 4

25. State the guidelines to be followed during report writing in forensics investigation 4 1 5

26. Explain any three specification that has to be present in the Evidence Custody Form. 4 2 2

27. Explain the different task performed by the computer forensics tools. 4 3 4

PART - C (5 × 12 = 60 Marks) Marks BL CO

Answer **all** Questions

28.	(a) Illustrate the concept and provide the steps of Incidence response methodology process.	12	2	1
	(OR)			
	(b) Explain the different types of Data Acquisition Formats along with its merits and demerits.			
29.	(a) What is Digital Evidence? State and Explain the general task that the Investigators perform when working with the Digital Evidence.	12	3	2
	(OR)			
	(b) Analyze and write short notes on (a) Forensic Duplication - 6 Marks (b) Forensic Investigation - 6 Marks			
30.	(a) Summarize the crucial role of File System in Cyber Forensics.	12	3	3
	(OR)			
	(b) Discuss in detail about the following Terms. (a) Disk Partitions - 6 Marks (b) FAT Disks - 6 Marks			
31.	(a) Why corporate Investigations are typically easier than LAW Enforcement Investigations. Recommend the process of Investigation and Justify the Solutions.	12	3	4
	(OR)			
	(b) Explain the various criteria in the investigation procedure of UNIX system.			
32.	(a) Explain the procedure for corporate investigations with respect to: a. Employee Termination Case - 6 Marks b. Email Abuse Case - 6 Marks	12	2	5
	(OR)			
	(b) State the purpose of Forensics Too;s and Differentiate between the Hardware Forensic Tools and Software Forensic Tools in Detail.			

*****