b.	Explain in detail about overview of evidence handling procedure and report creation.	12	4	2	2
30. a.	Summarize the steps involved in examining NTFS disks and explain.	12	5	3	1
	(OR)				
b.	Generalize the following mechanisms in detail		6	3	1
	(i) NTFS data stream, encrypting file system	7			
	(ii) NTFS compressed files	5			
31. a.	Correlate the following proceeds for corporate high tech investigation		4	5	1
	(i) E-mail abuse investigation	6			
	(ii) Media leak investigation	6			
	(OR)				
b.	Discuss in detail about the following		4	5	1
	(i) Systematic approach in computer investigation	6			
	(ii) Conducting an investigation in computer investigation	6			
32. a.	Elaborate an investigating hacker tool in detail.	12	4	6	1
	(OR)				
b.	Analyze and explain in detail about the following		5	6	1
	(i) Computer forensics software tools	6			
	(ii) Computer forensics hardware tools	6			

* * * * *

Reg. No.														

B.Tech. DEGREE EXAMINATION, JUNE 2023

Sixth 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

		Marks	BL	CO	PO
	PART – A (20 × 1 = 20 Marks) Answer **ALL** Questions				
1.	Choose the method which is used to access the audit log records from the system? (A) gpedit-enabler (B) gedit-enabler (C) getpedit-enabler (D) getped-enabler	1	1	1	1
2.	Evidence collected from network device logs are known as (A) Flow analysis (B) Active acquisition (C) Mode of detection (D) Packet analysis	1	1	1	1
3.	PsLoggedOn tools extract (A) All the users connected locally and remotely (B) Users connected locally (C) Users connected remotely (D) Users who are not connected physically	1	2	1	1
4.	Cite the security algorithm will be mostly used to check the integrity of the document in the response toolkit. (A) Block sha (B) MD5 (C) Crypt hash (D) SHA551	1	2	1	1
5.	Private networks can be a richer source of evidence than the internet because (A) They retain data for longer period of time (B) Owners of private networks are more cooperative with law enforcement (C) Private networks contain a higher concentration of digital evidence (D) Nobody can be harmed by crime on the internet	1	2	2	2
6.	The first us law to address computer crime was _____. (A) Computer Fraud and Abuse Act (CFAA) (B) Florida Computer Crime Act (C) Computer Abuse Act (D) A weapon or tool designed to commit a crime	1	1	2	1

7.	_____ is related to the verification process which involved sorting and searching through investigation files to separate good and suspicious data. (A) Kali Linux (B) Validation (C) Reporting (D) Filtering	1	2	2	2
8.	Regarding the admissibility of evidence which of the following is not a consideration. (A) Relevance (B) Authenticity (C) Best evidence (D) Nominally prejudicial	1	1	2	1
9.	NTFS stands for _____. (A) Network file system (B) Nano technology file system (C) New technology file system (D) Network technology file system	1	1	3	1
10.	Mounting of file system indicates _____. (A) Creating a file system (B) Deleting of a file system (C) Attaching portion of the file system into a directory structure (D) Removing the portion of the file system into a directory structure	1	1	3	1
11.	This is the table that contains information about the clusters that are set up by the file system is called _____. (A) File name area (B) File to file (C) File allocation table (D) File system area	1	1	3	1
12.	Smallest addressable storage unit on the hard drive disk (typically 512 bytes) (A) Cylinder (B) Row (C) Sector (D) Track	1	1	3	1
13.	IDIP stands for (A) Integrated Digital Investigation Process (B) Integrated Data Investigator Process (C) Integrated Digital Investigator Process (D) Independent Digital Investigator Process	1	1	4	1
14.	In the past, the method for expressing an option has been to frame a _____ question based on available factual evidence. (A) Hypothetical (B) Nested (C) Challenging (D) Contradictory	1	2	4	1
15.	_____ phase includes putting the pieces of a digital puzzle together and developing investigative hypothesis. (A) Preservation phase (B) Survey phase (C) Documentation phase (D) Reconstruction phase	1	1	4	1
16.	A hacker who identifies and exploits weakness in telephones instead of computer is known as _____. (A) Phreaker (B) Hacktivist (C) Ethical hacker (D) Grey hat hacker	1	1	4	1

17.	A report or account is an _____. (A) Informational work (B) Technical work (C) Professional work (D) Analytical work	1	1	5	1
18.	The structured report writing is known as (A) Genre (B) Advanced (C) Difficult (D) Easy	1	1	5	1
19.	Which thing we need to take at most case while doing in writing report (A) Record the survey not carry out (B) Record deleted data (C) Record the object (D) Record updated data	1	1	5	1
20.	The report is always written in a (A) Sequential manner (B) Irregular manner (C) Horizontal manner (D) Data base manner	1	1	5	1

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

		Marks	BL	CO	PO
21.	Analyze the different types of data produced by windows data acquisition tool.	4	4	1	1
22.	Show the importance of collecting the event log during live response.	4	4	1	1
23.	What is an evidence custody form? What information does it contain?	4	2	2	1
24.	Show how to recover the deleted files in FAT file system? Brief it.	4	4	3	1
25.	How can the hackers gain advantage in stealing essentials of investigation in forensics?	4	6	4	1
26.	Explain briefly what are the goals of tool analysis?	4	4	6	1
27.	List out the file system types with its characteristics.	4	2	4	4

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

		Marks	BL	CO	PO
28. a.	Summarize in detail about incident response methodology and the six steps associated with it.	12	4	1	1
	(OR)				
b.i.	Discuss in detail about creating a windows response tool kit.	8	4	1	1
ii.	Summarize the basic steps of the forensic investigation process.	4	4	1	1
29. a.	Point out the features of forensic duplication and investigation and also outline the problems and challenges forensic examiners face when preparing and processing investigations, including the ideas and questions they must consider.	12	4	2	2
	(OR)				