Reg. No.														

B.Tech. DEGREE EXAMINATION, MAY 2022
Sixth 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)
Answer **ALL** Questions

	Marks	BL	CO	PO
1. Volatile date resides in? (A) Registries (B) Running processes (C) Open network ports (D) System date and time	1	1	2	2
2. Physical forensics discipline include which of the following? (A) Blood stain (B) Eating (C) Searching (D) Watching	1	1	2	2
3. Which of the following techniques are not during computer forensics investigations? (A) Cross drive analysis (B) Live analysis (C) Deleted files (D) Fuzzy logic tools	1	1	1	3
4. Which method uses stochastic properties of the computer system to investigate activates lacking digitized anti facts? (A) Steganography (B) Stochastic forensics (C) Water marks (D) Data backup and recovery	1	1	2	5
5. What is used to validate the tools and verify the evidence integrity? (A) Hashing algorithms (B) Steganography (C) Water marks (D) Digital certificates	1	1	1	4
6. A digital investigator pursuing a line of investigation in a case because the line of investigation proved successful in pervious case is an example of. (A) Logical reasoning (B) Common sense (C) Preconceived theory (D) Investigators intuition	1	2	2	4
7. Regarding the admissibility of evidence, which of the following is not considered. (A) Relevance (B) Authenticity (C) Best evidence (D) Nominally prejudicial	1	2	2	4

PART – B (5 × 10 = 50 Marks)
Answer **ALL** Questions

	Marks	BL	CO	PO
26. a. Explain about the windows creating response toolkit in detail.	10	1	2	1
(OR)				
b. Give short notes on				
(i) Volatile data collection windows	5	2	3	2
(ii) In-depth data collection windows	5	2	3	5
27. a. Explain the following terms in detail				
(i) Understanding storage formats for digital evidence	5	2	5	3
(ii) Using/ usage of acquisition tools	5	2	4	5
(OR)				
b. Describe in detail about using specialized Email forensics tools.	10	2	5	1
28. a. Examine the FAT disk analysis and also explain FAT big picture in detail.	10	2	2	2
(OR)				
b. Give short notes on				
(i) Files in MFT attributes concepts	5	2	3	5
(ii) Other MFT attribute concepts	5	2	3	10
29. a. What is an Unix investigation? Describe the overview of Unix investigation steps in detail.	10	2	4	5
(OR)				
b. Explain about an identifying unauthorized user accounts groups of investigations system.	10	2	5	4
30. a. Write a short notes on forensics report writing in detail.	10	2	3	1
(OR)				
b. Explain in investigating hacker tools in detail.	10	2	2	2

* * * * *

8. In obtaining a warrant, an investigator must convince the judge on all of the following points except. 1 2 2 5

(A) Evidence of a crime is in existence
(B) A crime has been committed
(C) The owner or resident of the place to be searched is likely to have committed the crime
(D) The evidence is likely to exist at the place to be searched

9. If, while searching a computer for evidence of a specific crime, evidence of a new, unrelated crime is discovered, the best course of action is 1 2 2 5

(A) Abandon the original search and pursue the new line of investigation
(B) Continue with the original search but also pursue the nee inquiry
(C) Stop the search and obtain a warrant that addresses the new inquiry
(D) Continue with the original search, ignoring the new information

10. When assessing the reliability of digital evidence, the investigator is concerned with whether the computer that generated the evidence was functioning normally is 1 2 2 4

(A) Whether chain of custody was maintained
(B) Whether there are indications that the actual digital evidence was tampered
(C) Whether the evidence was property secured in transit
(D) Whether the evidence media was compatible with forensic machines

11. Volatile data does not reside in? 1 2 1 4

(A) Registries
(B) Cache
(C) RAM
(D) ROM

12. The smallest addressable storage unit on hard disk typically 512 bytes addresses are CHS and LBA are called as 1 2 2 10

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

13. Computer forensics also known as? 1 2 2 5

(A) Digital forensic science
(B) Computer crime
(C) Computer forensics science
(D) Computer forensics investigations

14. The one used by the user to identify and select the file, to the meta data area is referred as. 1 1 3 10

(A) Content area
(B) File name area
(C) File system area
(D) Meta data area

15. _____ is relating or dealing with the application of scientific knowledge to legal problems. 1 1 1 5

(A) Object
(B) Forensic
(C) File slack
(D) Files

16. A hacker who identifies and exploits weakness in telephone instead of computer is known as: 1 2 1 4

(A) Phreaker
(B) Hacktivist
(C) Ethical hacker
(D) Grey hat hacker

17. Who use their skill to identify security problem with computer network? 1 1 2 3

(A) Black hat hacker
(B) Ethical hacker
(C) Grey hat hacker
(D) Script kiddies

18. Cyber trails are advantagoues because 1 2 2 2

(A) They are not connected to the physical world
(B) No body can be hammed 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

19. The interrelationship among auditing fraud examination, and financial forensics is 1 1 1 1

(A) Established and maintained by legal structures and justice processes
(B) Constant even while social and cultural pressure are exerted on it
(C) Cased on the SOX act and SAS 99
(D) Dynamic and changes over time

20. Relationship of the management with auditors, bakers, lawyers, regulatory authorities etc is to be checked while analyzing. 1 2 1 4

(A) Management and directors
(B) Relationship with others
(C) Organization and industry
(D) Financial results and operating characteristics

21. In report writing the language used to be 1 3 2 5

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

22. The report is always written in 1 1 2 3

(A) Sequential manner
(B) Irregular manner
(C) Horizontal manner
(D) Data biased manner

23. The length of informal report should be 1 2 1 5

(A) 13 pages
(B) 1-3 pages
(C) 1/5 page
(D) Full page

24. Repeat discussed a particular problem in 1 2 2 1

(A) Less detail
(B) Detail
(C) Complicated
(D) Horizontal way

25. Which type of report is a report of action 1 2 2 2

(A) Analytical report
(B) Periodic report
(C) Recommendation report
(D) Analytical