Code No:158AQ **R18**

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

B.Tech IV Year II Semester Examinations, July - 2023

CYBER FORENSICS

(Common to CSE, IT)

Time: 3 Hours **Max. Marks: 75**

Note: i) Question paper consists of Part A, Part B.

ii) Part A is compulsory, which carries 25 marks. In Part A, Answer all questions.

iii) In Part B, Answer any one question from each unit. Each question carries 10 marks and may have a, b as sub questions.

PART – A

(25 Marks)

1.a)	What is computer security incident?	[2]
b)	Write the role of corporate computer security incident response team.	[3]
c)	What is forensic duplication?	[2]
d)	List the Windows NT system processes.	[3]
e)	What is sniffer?	[2]
f)	Write the goals of networking monitoring.	[3]
g)	List computer software forensic tools.	[2]
h)	Explain different files in SIM.	[3]
i)	What is windows registry?	[2]
j)	What is FAT?	[3]

PART – B

(50 Marks)

2.a)	Write the goals of incident response.	
b)	Describe different phases in data collection in forensic analysis.	[5+5]
	OR	
3.a)	Compare Incident Response Vs Computer Forensics.	
b)	Explain the role of computers in digital crime.	[5+5]
4.a)	Explain steps to collect Volatile data from Unix system.	
b)	Steps to obtain system logs in live response of Windows System.	[5+5]
	OR	
5.a)	Explain how to create forensic duplicate of a hard drive.	
b)	Explain mirror image and restored image.	[5+5]
6.a)	Explain types of networking monitoring.	
b)	Describe different data hiding techniques.	[5+5]
	OR	
7.a)	Explain the role of evidence custodian auditor.	
b)	Give the steps to collect network based log files.	[5+5]

8.a) Explain different computer forensic hardware tools.
b) What is the need of e-mail investigation for computer forensics? [5+5]

OR

9.a) Write the functions of computer forensic tools.
b) Explain the information in e-mail header for forensic analysis. [5+5]

10.a) Discuss about Microsoft file structure.
b) Explain startup tasks of MS-DOS system. [5+5]

OR

11.a) Explain NTFS system files in detail.
b) Write the steps to get windows registry. [5+5]

---ooOoo---