Code No.: R22CY603PC

R22	H.T.No.			8	R					

CMR ENGINEERING COLLEGE: : HYDERABAD
UGC AUTONOMOUS
III–B.TECH–II–Semester End Examinations (Regular) - June- 2025
CYBER CRIME INVESTIGATION AND DIGITAL FORENSICS
(CSC)

[Time: 3 Hours] **[Max. Marks: 60]**

Note: This question paper contains two parts A and B.
Part A is compulsory which carries 10 marks. Answer all questions in Part A.
Part B consists of 5 Units. Answer any one full question from each unit. Each question carries 10 marks and may have a, b, c as sub questions.

PART-A **(10 Marks)**

1. a)	Which device might store volatile digital evidence?	[1M]
b)	What does "integrity" of digital evidence mean?	[1M]
c)	If evidence is spread across multiple devices, how would you handle them?	[1M]
d)	How could failure in evidence preservation impact the case?	[1M]
e)	If a deleted photo is recovered, how might it aid the investigation?	[1M]
f)	How can location data support or challenge a suspect's statement?	[1M]
g)	Why might manual inspection be preferred over automated tools in some cases?	[1M]
h)	How would you examine deleted emails on a suspect's computer?	[1M]
i)	Which type of network evidence packet capture or flow data is more reliable and why?	[1M]
j)	Suggest a simple logging format for network traffic evidence.	[1M]

PART-B **(50 Marks)**

2. How might an investigator recognize the presence of digital evidence during a crime scene survey? [10M]

OR

3. What could be the reasons for digital evidence being considered more fragile than physical evidence? [10M]

4. How might a forensic analyst determine which model of investigation to use in a new case? [10M]

OR

5. What steps would you take to survey and secure a digital crime scene in a corporate breach? [10M]

6. How might digital evidence differ in cases of premeditated vs. impulsive violent crimes? [10M]

OR

7. What types of digital tools might be used in planning or executing a violent crime? [10M]

8. How do differences in file structure between Windows and Unix affect forensic data recovery? [10M]

OR

9. Write the procedure how you determine if forensic software has altered the original system data? [10M]

10. What are the strengths and limitations of applying traditional forensic tools to live network traffic? [10M]

OR

11. Create a policy for logging and preserving evidence during a suspected ransomware attack. [10M]

****