Roll No. | | | | | | | | | | | | **Total No. of Pages : 02**

Total No. of Questions : 09

B.Tech. CSE (Internet of Things and Cyber Security including Block Chain Technology) (Sem.–6)

DIGITAL FORENSICS

Subject Code : BTITCS601-20

M.Code : 93412

Date of Examination : 23-05-2025

Time : 3 Hrs. **Max. Marks : 60**

INSTRUCTIONS TO CANDIDATES :

1. **SECTION-A is COMPULSORY consisting of TEN questions carrying TWO marks each.**
2. **SECTION-B contains FIVE questions carrying FIVE marks each and students have to attempt any FOUR questions.**
3. **SECTION-C contains THREE questions carrying TEN marks each and students have to attempt any TWO questions.**

SECTION - A

1. Write briefly :

a. How does Hashing help maintain the integrity of digital evidence?

b. What are the different types of memory used in a computer system?

c. How does Locard's exchange principle apply to digital evidence?

d. What are the most common types of digital forensics tools?

e. How do rules of evidence apply to digital evidence?

f. What are the legal requirements for obtaining a warrant to collect digital evidence?

g. How do investigators extract data from operating system artifacts?

h. How do investigators choose the right tool for a given digital forensics investigation?

i. What are some of the key artifacts left behind by web browsers?

j. How do email headers provide information about the sender, recipient, and routing of an email message?

SECTION - B

2. How can digital forensics tools be used to recover deleted files and other types of data, and what are the limitations of this approach?

3. What are the key steps involved in conducting a digital forensics investigation?

4. What are some of the ethical considerations involved in conducting a digital forensics investigation?

5. How do legal and ethical considerations impact the reporting of digital forensics findings, and what are some of the key elements that should be included in a digital forensics report to ensure its admissibility and credibility in court?

6. What are some of the common artifacts left behind by operating systems, and how do investigators use these artifacts to reconstruct user activity and system events?

SECTION - C

7. How do investigators use social media metadata to reconstruct the timeline of events and user activity on these platforms? How can investigators use this information to track down the source of a message and behavior of user?

8. What are some of the challenges involved in investigating cybercrime scenes? How does the chain of custody help maintain the integrity of digital evidence and what are some of the best practices for preserving this chain throughout an investigation?

9. What is the role of Restore points, hibernating files and windows registry in operating systems and how they help to investigators?

NOTE : Disclosure of Identity by writing Mobile No. or Making of passing request on any page of Answer Sheet will lead to UMC against the Student.