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 : BTITCS-601-20

M.Code : 93412

Date of Examination: 29-05-2023

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 the digital forensics process differ from traditional forensic investigations?

b) What is the basic organization of a computer system, and how does it differ from other types of electronic devices?

c) What is hashing?

d) What are the advantages and limitations of using scientific models in digital forensics investigations?

e) How does data compression work?

f) What are the most common types of digital forensics tools?

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

h) How do rules of evidence apply to digital evidence?

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

j) What type of information can be extracted from Windows Registry?

SECTION-B

2. How do operating system logs provide insight into system events, errors, and user activity?

3. How do investigators draft a comprehensive report based on the digital evidence collected during a cyber crime investigation?

4. How has the field of digital forensics evolved over time, and what are some of the current challenges facing investigators?

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

6. What are some of the key artifacts left behind by social media networking sites, and how can these be used to identify user activity and behavior on these platforms?

SECTION-C

7. How can investigators use digital forensics tools to extract and analyze data from web browser history, email headers, and social media networking sites, and what are some of the challenges involved in this process? Discuss any two tools.

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. How does a file system manage data storage and retrieval on a computer's hard drive or other storage media? Explain the concept of Memory Organization.

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.