17702

BRAINWARE UNIVERSITY

Term End Examination 2024-2025
Programme – M.Sc.(ANCS)-2024
Course Name – Digital Forensics
Course Code - MNC27202B (T)
(Semester II)

Full Marks : 40 **Time : 2:0 Hours**

[The figure in the margin indicates full marks. Candidates are required to give their answers in their own words as far as practicable.]

Group-A

(Multiple Choice Type Question) 1 x 10=10

1. *Choose the correct alternative from the following :*

(i) Identify the principle that emphasizes that every contact leaves a trace.
a) Principle of Exchange b) Principle of Comparison
c) Law of Individuality d) Law of Probability

(ii) Apply the concept of the chain of custody to forensic evidence.
a) Store evidence in random locations b) Ensure evidence integrity and proper documentation
c) Share evidence freely d) Avoid documenting evidence collection

(iii) Apply the concept of data preservation in forensic investigations.
a) Modify original data for analysis b) Always analyze the original data
c) Create bit-wise copies and protect originals d) Share data without documentation

(iv) Define jurisdiction in the context of cybercrimes.
a) Local laws applied universally b) Judicial authority within specific legal boundaries
c) Ignoring sovereignty in legal processes d) Global uniformity in cyber laws

(v) Recognize the importance of hashing algorithms.
a) Ensures data authentication b) Improves CPU performance
c) Encrypts system backups d) Simplifies file management

(vi) Recognize obstacles to data interleaving.
a) Requires high system throughput b) Limited system compatibility
c) Slow tape drives d) All of these

(vii) Apply NTFS file recovery techniques using forensic tools.

a) Search MFT records for deleted entries
b) Ignore all deleted files
c) Encrypt the recovered files
d) Look for cluster fragments

(viii) Select a forensic plan to monitor insider threats within a network.

a) Implement IDS and firewall rules
b) Monitor login activities
c) Analyze network traffic for anomalies
d) All of these

(ix) Formulate an incident response strategy.

a) Identify assets
b) Monitor network traffic
c) Create response teams
d) Implement access controls

(x) Construct a digital evidence chain of custody plan.

a) Document handling steps
b) Use encryption techniques
c) Involve law enforcement
d) Apply forensic hashing

Group-B

(Short Answer Type Questions) 3 x 5=15

2. Define computer forensics. (3)
3. List the four stages of the computer forensics process. (3)
4. What is forensic carving in digital forensics? (3)
5. Illustrate volatile evidence in digital forensics. (3)
6. Explain the difference between real evidence and testimonial evidence. (3)

OR

Explain the importance of timestamps in forensic investigations? (3)

Group-C

(Long Answer Type Questions) 5 x 3=15

7. Compare and contrast the tools and techniques used in acquiring and analyzing digital evidence. (5)
8. Predict the challenges in recovering hidden or fragmented files, and how can they be overcome? (5)
9. Evaluate the different types of computer forensic systems and their significance. (5)

OR

Illustrate the steps involved in the data recovery process and its importance in digital forensics. (5)

****