**QP CODE: 24900073**

24900073

Reg No:......................

Name:........................

# MAHATMA GANDHI UNIVERSITY, KOTTAYAM

## FIRST SEMESTER MGU-UGP (HONOURS) REGULAR EXAMINATION NOVEMBER 2024

**First Semester**

**Multi-Disciplinary Course - MG1MDCCFS100**

**FOUNDATION OF CYBER FORENSICS**

(2024 ADMISSION ONWARDS)

Duration: 1.5 Hours                                                        Maximum Marks: 35

**Remember (K), Understand (U), Apply (A), Analyse (An), Evaluate (E), Create (C), Interest (I), Appreciation (Ap), and Skill (S)**

*Students should attempt atleast one question from each course outcome to enhance their overall outcome attainability.*

[Learning Domain][CO No(s)]

**Part A**
Short Answer Type Questions
Answer any 10 questions
Each question carries 1 marks

| | | | |
|---|---|---|---|
| 1 | Discuss CFX-2000. | [U] | [1] |
| 2 | Discuss about Forensic Evidence Acquisition services. | [U] | [1] |
| 3 | Breakdown the key responsibilities of a computer forensics expert. | [An] | [2] |
| 4 | Compare the recovery of deleted files with analysis of hidden files during a forensic investigation. | [An] | [2] |
| 5 | Discuss about DIRT. | [U] | [1] |
| 6 | What is BAIT? | [An] | [2] |
| 7 | Identify any two Disk Imaging tools. | [U] | [3] |
| 8 | Identify any of the reporting tool in cyber forensics. | [U] | [3] |

9    How do we measure the importance of file system analysis tools?    [E]    [4]

10    Evaluate Encase registry viewer    [U]    [3]

11    Describe a situation where you would need to modify the registry.    [U]    [3]

12    How do you add, modify, and delete registry keys and values    [E]    [4]
      programmatically.

$(10 \times 1 = 10)$

**Part B**
Short  Essay Type Questions
Answer any 3 questions
Each question carries 5 marks

13    Examine different types of computer forensics technology.    [An]    [2]

14    Differentiate between data duplication and data preservation in computer    [U]    [1]
      forensics.

15    Explain  the various types of network capturing tools.    [U]    [3]

16    Discuss the process and importance of file system analysis in forensic    [U]    [3]

$(3 \times 5 = 15)$

**Part C**
Essay Type Questions
Answer any 1 questions
Each question carries 10 marks

17    Compare data recovery and computer forensics and discuss the role of    [U]    [1]
      computer forensics in law enforcement specifically in handling digital
      evidence at a crime scene.

18    Explain data back-up and recovery.    [An]    [2]

$(1 \times 10 = 10)$

# END OF THE QUESTION PAPER
**\*\*\***