No. of Printed Pages : 4

MSEI–027

MASTER OF SCIENCE (INFORMATION SECURITY)/ P. G. DIPLOMA IN INFORMATION SECURITY (MSCIS/PGDIS)

Term-End Examination

June, 2026

MSEI-027 : DIGITAL FORENSICS

Time : 2 Hours *Maximum Marks : 50*

***Note** : (i) All questions are compulsory.*

*(ii) Attempt any **two** out of three in question No. 3*

---

1. Attempt all questions : 5×2=10

   (a) The tool used to create a bit-by-bit copy of a digital storage device for forensic analysis is called as …… .

(b) …….. analysis involves examining the data that is hidden or not immediately available and visible, such as deleted file or file slack space.

(c) To ensure that digital evidence has not been altered or tampered with, forensics experts use a technique called ……..… .

(d) The ……. is the process of retrieving data from damaged or corrupted storage devices, often requiring specialized techniques and tools.

(e) The ……. process is a standard used to manage and control digital evidence in a way that maintains its integrity and authenticity throughout the forensic process.

2. Attempt all *four* short answer type questions : 4×5=20

   (a) What does a forensic image of a digital storage device represent ?

   (b) Analyse the impact of emerging technologies (IoT, Blockchain) on digital forensics.

   (c) What type of data does network forensics focuses on ?

   (d) How does mobile device forensics differ from traditional digital forensics ?

3. Attempt any *two* out of three long answer type questions. 2×10=20

   (a) Explain the steps involved in the digital forensic life cycle starting from evidence collection to presentation in court.

(b) Discuss the challenges faced in recovering data from encrypted devices and the methods forensic investigator use to overcome these challenges.

(c) Analyse the impact of cloud computing on digital forensic investigation and the strategies used to address these impacts.

× × × × ×