

JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT

TEST -3 EXAMINATION- 2025

M.Tech-II Semester (IS)

COURSE CODE (CREDITS): 18M11CI214

MAX. MARKS: 35

COURSE NAME: Digital Forensics

COURSE INSTRUCTORS: RVS

MAX. TIME: 2 Hours

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

(b) The candidate is allowed to make Suitable numeric assumptions wherever required for solving problems

Q.No	Question	CO	Marks
Q1	Explain the role of digital forensics in criminal and corporate investigations, auditing, and in the general area of IT security.	1	4
Q2	Explain ways to determine the best acquisition method. Describe contingency planning for data acquisition.	1	4
Q3	Describe how to secure a computer incident or crime scene and Explain guidelines for seizing digital evidence at the scene.	2	4
Q4	Explain how Hard Disk Drive (HDD) and Solid-State Drive (SSD) operate. List some options for decrypting drives encrypted with whole disk encryption.	3	4
Q5	Explain how to evaluate needs for computer forensics tools. Describe available computer forensics software and hardware tools.	2	4
Q6	Discuss the standard procedures being used for conducting virtual machines forensic analysis and explain the live acquisition process.	3	4
Q7	Explain the standard procedures to acquire data from smartphones.	4	3
Q8	Describe the importance of reports for the digital investigation.	4	3
Q9	a) An affidavit is an example of a written report. (T/F) b) When acquiring a mobile device at an investigation scene, you should leave it connected to a laptop or tablet so that you can observe synchronization as it takes place. (T/F) c) TCP can be used to retrieve specific timeframes of packet captures. (T/F) d) Digital investigators usually apply static data acquisition when the suspect's computer operating system is write-protected and can't be altered. (T/F) e) Computer forensics and data recovery refer to same activities. (T/F)	1-4	5