CBCS SCHEME

USN | | | | | | | | | | |

22SCS322

# Third Semester M.Tech. Degree Examination, Dec.2023/Jan.2024
## Cyber Forensics

Time: 3 hrs. Max. Marks: 100

***Note: 1. Answer any FIVE full questions, choosing ONE full question from each module.***
***2. M : Marks , L: Bloom's level , C: Course outcomes.***

| | | Module – 1 | M | L | C |
|---|---|---|---|---|---|
| Q.1 | a. | Define Digital Forensic. Briefly explain the investigation triad. | 10 | L2 | CO1 |
| | b. | Briefly explain the steps involved in conducting an investigation. | 10 | L2 | CO1 |
| | | **OR** | | | |
| Q.2 | a. | In detail explain different types of digital investigation. | 10 | L2 | CO1 |
| | b. | Mention the different types of courses to be acquired to become professionals and briefly explain them. | 10 | L2 | CO1 |
| | | **Module – 2** | | | |
| Q.3 | a. | What are RAID and what is the role of RAID in digital forensic? | 10 | L3 | CO2 |
| | b. | Briefly explain commercial acquisition tools used in digital forensic. | 10 | L2 | CO2 |
| | | **OR** | | | |
| Q.4 | a. | Explain the concept of identifying digital evidence and collecting evidence in private sector incident scene. | 10 | L2 | CO3 |
| | b. | Illustrate static acquisition method and live acquisition method used in digital forensic. | 10 | L3 | CO2 |
| | | **Module – 3** | | | |
| Q.5 | a. | Briefly explain with diagram type 1 and type 2 hypervisor used in virtual machine. | 10 | L2 | CO4 |
| | b. | Mention the procedure that should be followed when Forensic analysis of VM's is crucial. | 10 | L2 | CO4 |
| | | **OR** | | | |
| Q.6 | a. | Briefly explain the steps involved to acquire an image in virtual machine. | 10 | L2 | CO4 |
| | b. | Using packet analyzer, explain the method to develop network forensic with diagram. | 10 | L2 | CO4 |
| | | **Module – 4** | | | |
| Q.7 | a. | Mention different types of ethical hacks and briefly explain them. | 10 | L2 | CO5 |
| | b. | Describe the ways to conduct ethical hacking and also create a security evolution plan. | 10 | L3 | CO5 |
| | | **OR** | | | |
| Q.8 | a. | List different stages involved in ethical hacking and briefly explain them. | 10 | L2 | CO5 |
| | b. | Describe the information gathering methodology used in foot printing. | 10 | L3 | CO5 |
| | | **Module – 5** | | | |
| Q.9 | a. | Briefly explain active online attacks and passive online attacks. | 10 | L2 | CO5 |
| | b. | Write a note on SMB redirection and SMB relay MITM attacks. | 10 | L2 | CO5 |
| | | **OR** | | | |
| Q.10 | | Write notes on: | 20 | L2 | CO5 |
| | a. | Offline attacks | | | |
| | b. | Non Electronic Attacks | | | |
| | c. | Password-Cracking Technique | | | |
| | d. | Password – Cracking Counter Measure | | | |

* * * * *