Module-I

1. What is the significance of cyber laws in today's digital world?
2. Define cyber forensics and explain its role in the investigation of cybercrimes.
3. How are cyber laws different from traditional laws?
4. Classify cyber crimes under three broad categories: crimes against individuals, property, and the nation. Provide examples for each.
5. What are the common types of cyber crimes targeting individuals?
6. How do cyber crimes against property differ from those targeting the nation?
7. Why is digital forensics important in modern cybercrime investigations?
8. Explain how digital forensics aids law enforcement agencies in solving cybercrimes.
9. What are the major steps involved in the digital forensic investigation process?
10. Explain the role of evidence acquisition and preservation in digital forensics.
11. Why is the chain of custody crucial in digital forensic investigations?
12. Convert the decimal number 45 into binary and hexadecimal.
13. How is data represented using ASCII and Unicode? Explain with examples.
14. Why is hexadecimal representation preferred in computing over binary?
15. What are the key areas of focus in digital forensics? Briefly explain disk forensics and network forensics.
16. How does mobile forensics differ from computer forensics?
17. Explain the importance of wireless forensics in investigating network-related cybercrimes.
18. What are the key steps in incident handling and response?
19. Define forensic triage and explain how it helps in quick decision-making during an incident response.
20. What is ethical hacking, and how does it differ from malicious hacking?
21. Discuss the future challenges of cybercrime in the context of emerging technologies like AI and IoT.
22. How can ethical hacking be used to prevent cybercrime?

Module-II

1. What is Locard’s Exchange Principle, and how does it apply to digital forensics?
2. Give examples of how digital evidence is transferred or left behind, following Locard's principle, in a cybercrime investigation.
3. Describe the different digital forensic investigation models used in cybercrime investigations.
4. How do traditional forensic investigation models differ from digital forensic models?
5. What are artifacts in the context of digital forensics? Provide examples.
6. How can digital artifacts be used to trace cyber activities?
7. Differentiate between raw and proprietary forensic storage formats.
8. What are the advantages and disadvantages of using raw forensic formats compared to proprietary formats?
9. Define slack space and explain its importance in digital forensics.
10. What is swap space, and how can it be used to gather digital evidence?
11. How can steganography be detected and analyzed in digital forensic investigations?
12. What are the key techniques used to recover deleted files in digital forensics?
13. Explain the process of recovering hidden or corrupt data during an investigation.
14. What are standard file formats in the context of digital forensics? Give examples of some file headers used for identification.
15. What is forensic file carving, and how is it useful in recovering evidence from storage devices?
16. What are the critical steps in planning a digital forensic investigation?
17. How does proper planning help in ensuring the success of a forensic investigation?
18. What is the order of volatility in digital forensics? Why is it important to follow this order during an investigation?
19. Define forensic triage and discuss how it assists in prioritizing the analysis of digital evidence.
20. Explain the role of file systems in digital forensic investigations.
21. How do file systems like NTFS, FAT32, and EXT differ in terms of their forensic analysis?