Department of Computer Science and Engineering
CS6004 - Cyber Forensics
Question Bank (2017-18 ODD)

Unit 3. INTRODUCTION TO COMPUTER FORENSICS

Part – A

1. What is cyber crime?
2. List the reason for not reporting a cyber crime
3. List the Jurisdictional concern in cyber crime
4. What is Phreaking?
5. What is Hacking?
6. What is data piracy?
7. What is cyber-punk?
8. Explain the difference between hackers and crackers.
9. List any four computer crimes.
10. Research criminal law related to computer crime in a jurisdiction – Identify cases that have been tried using these law
11. How the corporate take-up the email-abuse investigation.
12. What are the three storage formats for digital evidence?
13. What are the advantages and disadvantages of using raw format?
14. Name few tools that support proprietary format.
15. What are the problems with proprietary format?
16. Name some of the forensics analysis tools.
17. What is the goal of using a advance forensics format
18. What is the difference between static and live acquisition?
19. What are the different types of acquisition?
20. Name the type of acquisition methods to collect the forensics data.
21. List some of the forensics tools.
22. What is meant by logical acquisition?
23. What is sparse acquisition?
24. What are the special software drivers designed to write data from a suspect drive?
25. How will you copy from the encrypted drives?
26. Name the drawbacks while using windows acquisition tools.

Part – B

1. Discuss the traditional problems associated with computer crime
2. Discuss the four categories of cyber criminals in today's society.
3. How will you take a systematic approach to investigate a computer crime?
4. How to develop formal procedures and informal check list to cover all issues important to high-tech investigation?
5. How will you set up a workstation for computer forensics?
6. How will you plan your crime investigation?
7. Discuss the forensics format used in data acquisition tools. (5)
8. How will you acquire data and validate it in windows? (5)
9. How will you acquire data and validate it in Linux? (5)
10. How will you acquire data from a RAID disk? (5)
11. How will you acquire data remotely using different acquisition tools ? (10)