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

Unit 4. EVIDENCE COLLECTION AND FORENSICS TOOLS

Part – A

1. Define Digital evidence.
2. Name the two groups that set standards for recovering, preserving, and examining digital evidence.
3. List the general tasks investigators perform when working with digital evidence.
4. What steps you perform to boot a suspect's computer?
5. What are different computer records used as digital evidence?
6. Define Federal Rules of Evidence
7. List few situations where you cannot produce original as evidence
8. What is Plain view doctrine?
9. What are the media you use to store digital evidence?
10. How will you determine the file system type to investigate?
11. How to determine the encryption method used?
12. How CMOS and BIOS help to collect data?
13. List out the disk drive components?
14. Define track density and Areal density.
15. What are the different Microsoft file structures available?
16. List out the versions of FAT.
17. List out the items stored in the FAT database.
18. What is a data run?
19. Define MBR and MFT.
20. What is drive slack?
21. Is it possible to load an image of a suspect drive on a virtual machine? Yes or No, Justify.
22. Which files does EFS can encrypt?
23. How NTFS data stream might add evidence value to an investigation?
24. How NTFS encrypt data?
25. What information does the Registry of windows hold?
26. In what scenario the virtual machine may be added benefit?
27. List the types of computer forensics tools?
28. Name the five function performed by a forensic tool?
29. Define write-blocker?
30. What is CFTT?
31. What is NSRL?

Part – B

1. Describe the process of collecting evidence in private-sector incident scenes. (5)
2. How you will be preparing for a search in computing investigations? (10)
3. Brief the concept of securing a computer incident or crime scene. (5)
4. Explain how you will seize Digital Evidence at the Scene for investigation? (10)
5. How to store digital evidence you have collected after investigation? (5)
6. How Hexworkshop help to determine the unknown disk OS? (5)
7. Explain the steps involved in examining NTFS disks.
8. Does NTFS is friendly to collect the evidence of a crime? State your reasons. (5)
9. If the owner uses NTFS EFS, state your reason to retrieve the files? (5)
10. Why the computer forensics examiner should be aware of whole disk encryption tool? State your reasons. (5)
11. How does the registry aid to recover the files? (5)
12. Discuss the advantages of using virtual machines to restore the files for investigation? (5)
13. Discuss how to apply the function of acquisition in computer forensics? (5)
14. Discuss how to apply the function of validation in computer forensics ?(5)
15. Discuss how to apply the function of extraction in computer forensics? (5)
16. Discuss how to apply the function of reconstruction in computer forensics? (5)
17. Discuss how to apply the function of reporting in computer forensics? (5)
18. Prepare a detailed table about forensics tool that is provided by different vendor. (5)
19. List the computer forensics software tools. Discuss the advantages and disadvantages of the tools. (10)
20. Discuss the hardware tools used for forensics investigations?
21. How will you evaluate the forensics software? Which standard is responsible for validating the software tool? (5)