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

Unit 5. ANALYSIS AND VALIDATION

Part – A

1. Name the CF tool which provides automate of image files.
2. How will you automate hashing of image file?
3. How FDK Imager use the hashing function?
4. What is Scope creep?
5. What is KFF?
6. How the NSRF supports hashing?
7. What is Auto Image Checksum Verification?
8. Name a few disk-partitioning utilities.
9. What is data hiding?
10. How will you view the hidden partition in disc manager?
11. How Norton Disk Edit provides data hiding?
12. What is bit shifting?
13. How will you examine an encrypted file?
14. Name the shareware programs used for remote acquisition.
15. What are the critical aspects of computer forensics in validating digital evidence?
16. What is key escrow?
17. What is Steganography?
18. Which FTK search option is more likely to find text hidden in unallocated space: Live search or indexed search?
19. What is network Forensics?
20. What is DiD?
21. What data are available in network logs?
22. Determine the causes of abnormal traffic?
23. What is Network Forensics?
24. What is ESMTP?
25. How will you retrieve e-mail header?
26. What is a firewall log?
27. What is an e-mail log?
28. Name the files used for e-mail investigation.
29. Name few forensic tools to recover deleted e-mails.
30. Compare POP3 with SMTP.
31. How will you examine the e-mail message?
32. How will you investigate e-mail abuse?
33. Where is information stored in mobile device?
34. Name the different digital networks that are used in mobile phone industry.

35. Name the technologies used in 4G.
36. Name three components that are used for communication in mobile devices.
37. Name the peripheral memory card used with PDA.
38. Name the places where you can retrieve data from a mobile phone?
39. What data you can retrieve from SIM card?
40. List the mobile forensics tool.
41. Why mobile phone should be connected to power source to retrieve data?
42. What is the most popular cellular network worldwide?

Part – B

1. How will you use hashing functions of HexWorkshop to verify the data after an acquisition?
2. Discuss ProDiscover's build in validation features for data acquisition.
3. How will you validate forensics data after data acquisition?
4. Discuss on various Data-hiding Techniques.
5. What are the Techniques and Tools used to recover password?
6. How remote acquisition
7. Explain in detail the shareware programs used for remote acquisition.
8. How will you secure a network?
9. How Ethereal tool is used in network forensics?
10. Discuss the standard procedure followed in network forensics.
11. Discuss the roles of client and server in e-mail.
12. How will you investigate e-mail crime and violations? (16)
13. How will you examine the e-mail server logs?
14. Discuss the e-mail forensics tools.
15. How will you copy and examine e-mail header?
16. Discuss the mobile forensics acquisition procedures you will apply to collect data? (10)