Question Bank Cyber Forensics

Unit I:

(BOOK: - GUIDE TO COMPUTER FORENSIC AND INVESTIGATION)

1. Define Computer Forensics. (pg 2)
2. Explain the Investigation Triad (pg 4,5)
3. List standard systems analysis steps to be applied when preparing a for forensic investigation case. (pg30,31)
4. What are some initial assessments you should make for a computer investigation? (pg 32)
5. What in an evidence custody form? What information does it contain? (pg 33-35)
6. What is the procedure for securing the evidence? (pg 35,36)
7. Explain procedures for Corporate High-tech Investigations with respect to: (pg 37-43)
    a. Employee Termination Cases
    b. Internet Abuse Investigation
    c. Email Abuse Investigation
    d. Attorney-client Privilege investigations
    e. Media Leak investigation
    f. Industry Espionage investigations
8. What are the requirements to set up a workstation for computer forensics? (pg 45,46)
9. What are the resources required for forensic investigation? (pg 46)
10. Write a short note on Bit-stream Copies (pg 47)
11. Explain the following terms: (pg 60)
a. Bit-stream image b. Chain of custody c. Evidence custody form d. Evidence bags
e. Repeatable findings f. forensic workstations
12. What is data acquisition? What are its types? What is its goal? Explain. (pg 100)
13. Explain different types of data acquisition formats along with its advantages and disadvantages. (pg 101,102)
14. What are the different data collection methods? Explain (pg 103)
15. Explain acquiring data with dd command and dcfldd in Linux? (pg 116,119)
16. What are the different acquisition tools in forensics? Explain (pg 120-123)(pg138-139)
17. What are the different ways to validate the acquired data? Explain. (pg 126-129)
18. What are the different remote network acquisition tools? Explain.(134-137)
19. Why should the computer incident or crime scene be secured? Who is responsible for securing the scene? (pg 168,169)
20. Enumerate the guidelines for seizing digital evidence at the scene. (pg 169-174)
21. What are the different types of computer forensics tools? Explain. (pg 261)
22. State and Explain different tasks performed by Computer Forensic tools. (pg 261-271)
23. What is Validation & Discrimination? Explain their subfunctions. (pg 264,266)
24. Explain the following terms: (pg 266-269)
a. Data viewing b. Keyword searching c. Decompressing d. Carving e. Book marking
25. What are the subfunctions of reconstruction? Explain (pg 269,270)
26. Explain the command line and GUI computer forensics software tools. (pg273-278)
27. What is a forensics workstation? State and explain its different categories? What is a write blocker? (pg 278,279)
28. What is network forensics? Explain the 3 modes of protection in DiD Strategy. (pg 428,429)
29. What is Live Acquisition? How is it performed? (pg430,431)
30. What is the standard procedure used for network forensics? (pg 432)
31. List the different network tools and explain any two. (pg 435,436,439,440)
32.Explain the following terms: (pg 445)
a. Packet sniffer b. Order of volatility c. honeypot d. honeystick e. DDoS
33. State and explain different types of digital networks. (pg 497)
34. List & explain the technologies used by 4G network. (pg 498)
35. What are the different components found inside a Mobile device (pg 499)
36. Write a short note on:

a. PDA (pg 500) b. SIM (pg 499,500) c. Iphone Forensics (pg 504)
37. What are different Mobile Forensic tools? Explain. (pg 504,505)

Unit II

1. Explain the role of e-mail in investigations. (pg452)
2. Describe client and server roles in e-mail. (pg453)
3. Describe tasks in investigating e-mail crimes and violations. (pg 454-467)
4. Write a short note on Email Servers (pg 467-468)

(BOOK: - [André_Årnes]_Digital_Forensics)

5. Write a short note on DNS (7.4.2.1)
6. What is Onion Routing (7.4.3.2)
7. Explain Web shells (7.4.3.3)
8. List and Explain different ways to trace information on the internet. (7.5.1-7.5.5)
9. Write a short note on Collection Phase-Local Acquisition (7.6)
10. What tcpdump and pcap? Explain (7.7.1)
11. Explain DHCP Logs and Netflow in brief (7.7.1.1,7.7.2)
12. Explain the following:
a. Web Server Logs (7.8.1.1) b. Virtual Hosts (7.8.1.3)

(BOOK: -[Jennifer_Golbeck]_Introduction_to_Social_Media)

13. State and Explain the different types of content posted on social media? (pg 10)
14. What are the different categories of social media? Explain (pg 10-12)
15. Write a note on Social Connections and Associates (pg 19)
16. Explain different types of Personal information shared on social media (pg 17-25)
17. What are privacy controls? Explain its importance. (pg 31-35)
18. What are the different techniques for finding people on social media (pg 39-43)
19. Write short note on Location data of social media (47-50)

(BOOK: -[John_Sammons]_The_Basics_of_Digital_Forensics)

20. Explain the following terms: (pg119-123)
a. Cookies b. Web Cache c. INDEX.DAT d.P2P e. NTUSER.DAT
21. What are the different Email Protocols? How can email be used as an evidence (pg 126-128)
22. What is Messenger forensic? State the different types of evidence that can be collected from a messenger? Where can such files be found on computer?

Unit III

1. Explain the legal process to conduct computer investigation for potential criminal violations of law. (pg 12,13)
2. Write a short note on Corporate Investigations. (pg14)
3.What is authorized requestor? Why should companies appoint them for computer investigations? (pg 17)
4. Explain the following terms: (pg21,22)
a. Affidavit b. exculpatory c. inculpatory d. line of authority e. warrant f. police blotter g. silver-platter doctrine h. litigation
5. What is digital evidence? State and explain general tasks that the investigators perform when working with digital evidence. (pg 150,151)
6. List any five rules of evidence. (pg 152)
7. How to collect evidence in Private Sector Incident Scenes (pg 157-160)
8.Explain the following terms:
Plain view doctrine, Fourth amendment, probable cause, limiting phrase, (161-163) commingled data (pg 160)
9. Explain the tasks to be completed before searching for evidence. (pg 163-168)
10. What are the steps to create image files of digital evidence? (pg 174)
11. How is digital evidence stored? Explain. (pg 174-177)
12. Explain various ways in which data integrity can be verified? (pg 177,178)
13. Explain different types of reports. (pg 518,519)

14. List various guidelines for writing reports (522-527)
15. Explain the structure of report (pg 521)
16. What are the four criteria based on which the quality of a report is judged? (pg522)
17. Explain the following terms: (pg 534)
Deposition banks, high risk document, spoliation, lay witness
18. Briefly explain what is an expert witness and scientific witness (pg 542)
19 List the guidelines to document and prepare evidence (pg 543)
20. Explain the trial process. (pg 546)
21. List the general guidelines for Testifying (pg 549)
22. What is deposition? Explain its types and any two guidelines for testifying at a deposition (pg 554,555)
23. Explain the following terms: (pg 562,563)
Hearing, voir dire, motion in limine, conflicting out

(BOOK: - IT ACT [AMENDMENTS])

24. Define the following terms as per IT Act:

- Access
- Addressee
- Adjudicating Officer
- Certifying Authority
- Computer
- Computer Network
- Computer Resource
- Computer System
- Cyber Safe
- Cyber Security
- Digital Signature
- Electronic Form
- Intermediary
- Secure System
- Communication Device

25. Explain Digital Signature and Electronic Signature (pg-4,5)
26. Write a Short note on Electronic Governance
27. Explain the following:
    - Attribution of Electronic Records
    - Acknowledgment of Electronic Records
    - Dispatch of Electronic Records
28. Explain the following:
    - Penalties
    - Compensation
    - Adjudication
29. Explain the Power of police officer and other officer w.r.t IT Act (pg-32)

Note: Rest of the page numbers are from Guide to Computer Forensics and Investigation-Edition fourth