Module 4 (Text Book: Chapter 5, Chapter 7, Chapter 12: B. Nelson, A. Phillips, and C. Steuart, Guide to Computer Forensic and Investigations, 4th Edition, Course Technology, 2010)

Question No.	Question	Marks	Bloom's Level
1	What are the three rules for a forensic hash?	2	BL1
2	Define commingling evidence in a corporate setting.	2	BL1
3	State two hashing algorithms commonly used for forensic purposes.	2	BL1
4	What is the purpose of hashing in digital forensics?	2	BL1
5	List three items that should be in an initial-response field kit.	2	BL1
6	True or False: Small companies rarely need investigators.	2	BL2
7	What is the main information you look for in an e-mail message during an investigation?	2	BL1
8	List any two subfunctions of the extraction function in forensic tools.	2	BL1
9	What is the e-mail storage format used in Novell Evolution?	2	BL1
10	True or False: The plain view doctrine in computer searches is well-established law.	2	BL2
11	True or False: Building a forensic workstation is more expensive than purchasing one.	2	BL2
12	List two data-copying methods used in software data acquisition.	2	BL1
13	True or False: Internet e-mail accessed with a Web browser leaves files in temporary folders.	2	BL2
14	What information is typically included in an e-mail header?	2	BL1
15	Name any two techniques used in covert surveillance.	2	BL2
16	Define the term "collision" in the context of forensic hashes.	2	BL1
17	True or False: Many newer GUI forensic tools use significant system resources.	2	BL2
18	State one benefit of using drive-imaging tools in digital investigations.	2	BL2
19	True or False: NIST testing procedures are valid only for government agencies.	2	BL2
20	True or False: You can view e-mail headers in all popular e-mail clients.	2	BL2
21	What is the purpose of the syslog.conf file in UNIX-based e-mail systems?	2	BL1
22	True or False: If a suspect computer is located in an area with toxic chemicals, you should coordinate with the HAZMAT team.	2	BL2
23	Define "logical acquisition" in digital forensics.	2	BL1

Question No.	Question	Marks	Bloom's Level
24	What does MIME stand for in the context of e-mail standards?	2	BL1
25	True or False: Router logs can provide message content in e-mail investigations.	2	BL2
26	Explain why corporate investigations are easier than law enforcement investigations.	5	BL4
27	How does a forensic investigator ensure that original evidence is not corrupted during an investigation?	5	BL3
28	Describe what should be videotaped or sketched at a computer crime scene.	5	BL3
29	What precautions must you take when handling a running computer at a crime scene?	5	BL3
30	Explain the concept of validation and discrimination in digital forensics tools.	5	BL2
31	How can you trace an IP address in an e-mail header? Provide relevant methods.	5	BL3
32	List the steps to validate the results of forensic analysis using hashing.	5	BL3
33	Discuss the challenges of performing live acquisitions in digital investigations.	5	BL4
34	Explain how covert surveillance techniques, such as keylogging and data sniffing, are applied in corporate investigations.	5	BL4
35	Describe the purpose and significance of the plain view doctrine in computer searches.	5	BL2
36	What measures should you take when dealing with an e-mail server that no longer contains required log data?	5	BL3
37	Explain how the use of hashing algorithms ensures data integrity in forensic investigations.	5	BL3
38	Describe the process of extracting evidence from e-mail headers in digital investigations.	5	BL3
39	Explain why administrators might disable or configure circular logging on an e-mail server.	5	BL4
40	Discuss the role of Sleuth Kit and Autopsy in forensic investigations.	5	BL4
41	How do router logs help verify data in e-mail investigations?	5	BL3
42	What is the significance of MIME in e-mail communication and forensics?	5	BL4
43	Describe the steps to collect and analyze evidence from a laptop running during a field investigation.	5	BL3

Question No.	Question	Marks	Bloom's Level
44	Discuss the advantages and disadvantages of GUI-based forensic tools compared to command-line tools.	5	BL4
45	Why is it important to restore an e-mail server from a backup during investigations?	5	BL5
46	Discuss the legal and ethical implications of conducting covert surveillance on employees in corporate investigations.	10	BL5
47	Explain the process of reconstructing drives and its subfunctions in forensic analysis.	10	BL4
48	Analyze the importance of a company's computing use policy in protecting employee privacy and enabling investigations.	10	BL4
49	Compare and contrast logical and physical acquisition methods in forensic data collection.	10	BL4
50	Evaluate the challenges of investigating crimes involving e-mail communication and propose solutions to overcome them.	10	BL5
51	Critically assess the role of NIST testing procedures in validating forensic tools for different applications.	10	BL5
52	Discuss the importance of forensic hashing and how it is used to ensure the authenticity and integrity of digital evidence.	10	BL5
53	Explain the process of investigating a fatal car crash involving a running laptop and the steps to preserve evidence.	10	BL3
54	Analyze the implications of commingling evidence in corporate investigations and how it affects legal proceedings.	10	BL4
55	Describe the tools and techniques used to recover deleted e-mails from both servers and client machines.	10	BL3
56	Discuss the impact of the plain view doctrine on evidence admissibility in court during digital investigations.	10	BL5
57	Analyze the limitations of circular logging in e-mail servers and how it affects forensic investigations.	10	BL4
58	Compare the efficiency of drive-imaging tools with traditional backup methods in preserving digital evidence.	10	BL5
59	Evaluate the role of hashing algorithms in filtering known good files from potentially suspicious data.	10	BL4
60	Explain the legal considerations when transitioning a corporate investigation into a criminal investigation involving law enforcement.	10	BL5