Module 1 (Text Book: Chapter 1 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 is Forensic Science? Explain any two laws of Forensic Science and provide a case study which will cover them.	2	BL1
2	What are the different computer forensic services ? Explain.	2	BL1
3	What is the purpose of affidavit?	2	BL1
4	List three items that should be on your case report.	2	BL1
5	List two types of digital investigations typically conducted in a business environment.	2	BL1
6	Why a proper forensic methodology should be followed regarding handling of datas ?	2	BL2
7	What are the differences between Criminal case and Civil case.	2	BL1
8	What are the differences between Seizure and Acquisition.	2	BL1
9	What is professional conduct and why is it important?	2	BL1
10	Why should you critique a case after its finished ?	2	BL1
11	What is forensic imaging ?	2	BL2
12	Under normal circumstances a private sector investigator is considered an agent of law enforcement. True or False?	2	BL1
13	A credit card fraud has occured and the victim has complained to the cyber crime department about the same. What will be the chain of custody for the investigation?	2	BL4
14	List three items that should be on evidence custody form	2	BL1
15	Why should evidence media be write protected ?	5	BL4
16	What are some ways needed to determine sources needed for an investigation ?	5	BL4
17	What is the need for risk assessment for an investigation ?	5	BL4
18	What are the necessary components of a search warrant ?	5	BL3
19	How computer forensics and network forensics differ? (Provide differences on basis of case studies)	5	BL2
20	Data collected before an attorney issues a memo for an attorney client privilege case is protected under the confidential work product rule. Why ?	5	BL5
21	Why antistatic material is needed for an evidence bag ?	5	BL3

Question No.	Question	Marks	Bloom's Level
22	What happens if you connect a hot-swappable device with evidence in a newer Linux kernel distribution?	5	BL4
23	What is the purpose of maintaining a network of digital forensics specialists?	5	BL5
24	What is the role of an authorized requester in investigation? Explain	5	BL4
25	What is the need for having proper forensic tools for investigation? Give a detailed case study to support your answer.	5	BL4
26	How professional and company property should be distinguished ?	5	BL3
27	Why a digital investigator should maintain professional conduct ?	5	BL4
28	How an internet abuse investigation handled?	5	BL3
29	What is an Attorney-Client Privilege investigation?	5	BL4
30	What is an Industrial Espionage investigation?	5	BL3
31	What are the differences between interview and investigation ?	5	BL4
32	Case Study 1: Cybercrime Investigation Scenario: A financial company reports unauthorized transactions amounting to $500,000 from multiple customer accounts. The cybersecurity team detected unusual login attempts from various IP addresses, but no malware was found on the system. The forensic team must determine whether this was an insider attack, credential theft, or a system vulnerability. Questions: 1. Describe the forensic investigation process you would follow to identify the cause of the unauthorized transactions. 2. What types of digital evidence should be collected, and how would you ensure its integrity? 3. If an employee is suspected, what legal considerations must be followed before taking action? 4. What forensic tools would be most effective for analyzing network logs and authentication records?	10	BL4
33	Case Study 2: Digital Evidence in Court Scenario: A suspect is accused of data theft and corporate espionage from a multinational company. The forensic team found an encrypted USB drive containing confidential data on the suspect’s laptop. However, the suspect claims that they never accessed or copied the files. The prosecution must prove that the suspect was responsible. Questions:	10	BL4

Question No.	Question	Marks	Bloom's Level
	1. What forensic techniques can be used to determine whether the USB drive was connected to the laptop? 2. How can metadata analysis help in proving or disproving the suspect’s claim? 3. Discuss the legal challenges of presenting this digital evidence in court. 4. If the files were steganographically hidden, how would you uncover them?		
34	Explain in brief the challenges faced by digital forensic investigators.	10	BL5
35	Provide a detailed systematic approach for a Hi Tech investigation.	10	BL4
36	Discuss in brief how you differentiate the process of private and public sector investigations.	10	BL5
37	Create a case study on Company Policy violation. Make a chain of custody on how the scenario can be handled.	10	BL4
38	“Digital Forensics is concerned with the identification, preservation, examination and analysis of digital evidence”. Provide a case study in support of the statement.	10	BL5
39	Compare the Law of Probability and Law of Circumstantial Facts.	10	BL4
40	Discuss the Locard’s Principle of Exchange.	10	BL5
41	Explain the significance of Principle of Comparison. Provide a case study in support of your answer.	10	BL5
42	Explain the significance of Law of Individuality. Provide a case study in support of your answer.	10	BL4
43	Explain the significance of Law of Progressive Change. Provide a case study in support of your answer.	10	BL5