

Short Answer

Answer each question in 3–5 complete sentences.

1. Explain the difference between public-sector and private-sector investigations. Give one example of each.
2. What is the role of the Fourth Amendment in digital investigations, and why is it significant?
3. Define chain of custody and explain why it is critical in both legal and corporate investigations.

Application Scenarios

Read each scenario and respond in 1–2 paragraphs.

1. You are a Digital Evidence First Responder (DEFR) called to a suspected insider data theft at a company. Describe the first three steps you would take.
2. A company has a bring-your-own-device (BYOD) policy. An employee's personal laptop is suspected of being used for industrial espionage. How would you handle the investigation while respecting both company policy and personal property rights?
3. During an investigation, you discover that the IT manager accessed an employee's emails without proper authorization. Discuss the ethical and legal implications of this situation.

Technical Understanding

1. List at least five essential components of a digital forensics workstation and explain why each is necessary.
2. What is the difference between a bit-stream copy and a regular backup? Why is a bit-stream copy required in forensic investigations?