



SCHOOL OF COMPUTING AND ENGINEERING SCIENCES (SCES)
BACHELORS OF ELECTRICAL AND ELECTRONICS ENGINEERING
END OF SEMESTER EXAMINATION
MST 8506 SPECIAL TOPICS IN DIGITAL FORENSICS

DATE: 23rd April 2026

Time: 2 Hours

Question 1: Threat Analysis (10 points)

- Explain the concept of the “attack surface” in threat analysis and discuss how understanding it helps in minimizing security risks. (3 points)
- Define and describe the general phases of a cyber attack, ranging from the initial gathering of information to the final execution of objectives. (4 points)
- Explain the principles behind ping and port sweep activities and distinguish between the types of information they reveal about a target network. (3 points)

Question 2: Network Devices (10 points)

- Explain the principle and purpose of SPAN ports and distinguish between local SPAN and remote SPAN. (4 points)
- Characterize the three basic types of firewalls (Packet Filters, Session-Layer Proxies, and Application Proxies) and their role as a source of evidence. (3 points)
- Identify at least three types of volatile evidence and three types of persistent evidence that can be recovered from a network router. (3 points)

Question 3: Flow Analysis (10 points)

- Define a network flow record and describe the four main components of a flow-based monitoring system architecture. (4 points)
- Compare and contrast sFlow, NetFlow, and IPFIX in terms of their functionality, scalability, and suitability for digital forensics. (6 points)

Question 4: Web Proxies (10 points)

- Identify three typical scenarios where a web proxy server is involved in a digital forensic investigation. (3 points)
- Explain the caching mechanism supported by HTTP/1.1 (RFC 2616), specifically defining the expiration and validation models. (5 points)
- List different types of evidence available from a web proxy and explain their significance for reconstructing user activity. (2 points)

Question 5: Intrusion Detection Systems (10 points)

- Explain the role of an IDS in digital forensics and compare the strengths and limitations of signature-based versus anomaly-based detection. (5 points)
- Describe the function of the detection engine and define the structure of a SNORT rule. (5 points)