Strathmore UNIVERSITY

**SCHOOL OF COMPUTING AND ENGINEERING SCIENCES**
**MSC IN INFORMATION SYSTEMS SECURITY**
**MST 8506 SPECIAL TOPICS IN DIGITAL FORENSICS**
**END OF SEMESTER EXAMINATION**

DATE: 30th May 2023 Time: 2 Hours

**Instructions**

- This examination consists of **FIVE** questions.
- The maximum number of points for the examination is **50**.

1. Protocol analysis techniques. **(10 points)**

   Explain the process of protocol analysis in computer networking. Describe the major steps in protocol analysis, including Protocol Identification, Packet Capture, Packet Decoding, and Analysis. Discuss the benefits and limitations of protocol analysis in network troubleshooting and security analysis.

   Discuss the benefits and limitations of protocol analysis in digital forensics.

2. Firewalls **(10 points)**

   Explain the role of a firewall as a potential source of evidence in a digital investigation. Discuss the types of information that can be obtained from firewall logs.

   Describe the challenges associated with using firewall logs as evidence, such as log tampering and the need for specialized skills to analyze the logs.

   Discuss the best practices for preserving and analyzing firewall logs as evidence in a digital investigation.

*3.* Covert channels **(10 points)**

   Explain what Covert Channels are in computer security and list the different types of Covert Channels that can be used to exfiltrate data from a system covertly.

   Discuss the challenges associated with detecting and preventing Covert Channel attacks, including encryption and steganography techniques.

   Describe some best practices for mitigating the risks posed by Covert Channels, including network monitoring, access controls, and threat intelligence.

4. Security Information and Event Management Systems **(10 points)**

   Explain the key features that a Security Information and Event Management System (SIEM) should have to monitor security threats in an organization.

   Discuss the advantages of using Security Information and Event Management Systems in an organization, including log management, improved efficiency, and data aggregation and visibility.

**5.** Wireless Access Point Analysis **(10 points)**

Discuss some of the common attacks that can be launched against a wireless access point and the best practices that can be put in place to prevent those attacks.

A wireless access point can easily be used to launch an attack within an organization. Discuss the advantages of analyzing wireless access points during a security incident investigation.