Name:

Enrolment No:

UPES

End Semester Examination, December 2024.

Course: CYBER FORENSIC PROCEDURES AND ANALYSIS | Time: 03 hrs
Program: MCA-CSF | Max. Marks: 100
Course Code: CSCS8001P | Semester: 3

Instructions:

1. Attempt all questions.
2. Be precise and to the point.
3. Begin answer to each question on a new page of the answer sheet.
4. Provide the question number.
5. Handwriting should be clear.
6. No calculators, electronic gadgets, or graph sheets allowed.

NOTE: Answering both questions in a single choice will dismiss both answers.

S. No.	**SECTION A**	**Marks**	**CO**
Q1	What is the importance of preserving the integrity of evidence in cyber forensic investigations? Describe two methods used to ensure evidence integrity.	**2+2**	**1**
Q2	Explain how log analysis is used in cyber forensics. Mention two types of logs that are commonly analyzed and their relevance.	**2+2**	**2**
Q3	Define chain of custody in cyber forensics. Why is it important, and what are two key practices to maintain it?	**2+2**	**3**
Q4	What is the role of timeline analysis in cyber forensics, and how does it aid investigators? Provide an example of how it might be used in a case.	**4**	**4**
Q5	Describe two common challenges in cyber forensic investigations and explain how investigators can address them.	**2+2**	**5**

SECTION B

<u>Advanced Persistent Threat (APT) in a Government Network</u>

Background:

A government agency discovered that highly sensitive information related to national security had been exfiltrated. Upon investigation, it appeared that an Advanced Persistent Threat (APT) group had infiltrated their network undetected over several months. The attackers used sophisticated techniques, including zero-day exploits, encrypted communication channels, and lateral movement across multiple network segments. The forensic team faced challenges in identifying the attackers' methods, tracing the origin, and analyzing the scope of data stolen without tipping off the APT group, which had embedded backdoors to maintain persistent access.

Forensic Procedures Used:

- **Memory Forensics:** Collected memory dumps to analyze running processes, network connections, and other volatile data on compromised systems.
- **Endpoint Detection and Response (EDR):** EDR tools were used to monitor for signs of compromise across all endpoints as attackers stealthily moved across the network.
- **Encrypted Traffic Analysis:** Monitored encrypted traffic for unusual patterns indicating data exfiltration or command-and-control communication.
- **Artifact Analysis:** Examined artifacts like rootkits and backdoors to understand how the attacker’s evaded detection.
- **Threat Intelligence Correlation:** Correlated findings with global threat intelligence to identify the APT group, its typical methods, and potential geopolitical motivations.

Outcome:

The forensic investigation identified the APT group by correlating attack methods and tools with known threat actor profiles. While all compromised systems were isolated and remediated, the investigation revealed the attackers had exfiltrated classified data over several months. As a result, the agency

	implemented stricter network segmentation, improved threat detection capabilities, and adopted more rigorous cybersecurity policies.		
Q6	From the case study above: a) What unique challenges does an Advanced Persistent Threat (APT) pose for forensic investigators? b) How do memory forensics assist in uncovering details of an APT's activities?	**5+5**	**1**
Q7	From the case study above: a) Why is it necessary to analyze encrypted traffic patterns, and what might this reveal in an APT case? b) How does correlating with threat intelligence benefit an investigation involving an APT?	**5+5**	**2**
Q8	Define in brief the flowchart of digital evidence collection flow.	**10**	**3**
Q9	What is a cache memory? Explain in brief the difference between L1, L2 and L3 cache **OR** Give the flow-diagram of Memory hierarchy. Explain each level in brief	**10**	**4**
SECTION-C			
Q10	<u>**Data Breach in a Financial Institution**</u> **Background:** A large financial institution detected unusual activity in its network. The personal data of its clients was found to have been accessed and exfiltrated over a series of weeks. Upon discovery, the bank's cybersecurity team initiated a forensic investigation to trace the origin and scope of the breach, identify the attackers, and assess the impact. **Forensic Procedures Used:** • **Data Collection:** Gathered logs from firewalls, servers, and employee devices to trace suspicious activity. • **Disk Imaging:** Created disk images of affected machines to preserve data integrity. • **Log Analysis:** Analyzed server and firewall logs to identify IP addresses and possible attacker entry points. • **Network Traffic Analysis:** Monitored data flow in and out of the network, focusing on unusual data spikes. • **Malware Analysis:** Identified and dissected any malicious software found to understand its functionality. **Outcome:** The forensic investigation revealed that attackers had exploited a vulnerability in the company's VPN software. After identifying the specific malware used, the company patched the vulnerability, implemented multi-factor authentication, and enhanced monitoring to prevent similar breaches. **Questions:** a) What initial steps should the cybersecurity team take upon discovering unusual network activity? b) Why is disk imaging an essential step in forensic investigations? c) How can analyzing network traffic aid in identifying the attacker's methods? d) What role does malware analysis play in understanding the scope of a cyber attack? e) How could implementing multi-factor authentication reduce the risk of similar breaches?	**4+4+4 +4+4**	**5**
Q11	Explain in brief all the steps of SOP. **OR** <u>**Ransomware Attack on a Healthcare Organization**</u> **Background:** A healthcare organization suffered a ransomware attack, where patient data was encrypted, and a ransom	**4+4+4 +4+4**	**5**

	was demanded. The organization contacted cybersecurity experts to perform a forensic investigation to determine how the ransomware infiltrated the system, assess data damage, and prevent future attacks. **Forensic Procedures Used:** • **Endpoint Analysis:** Inspected devices for signs of malware and indicators of compromise. • **Log Review:** Checked login records, server logs, and access logs to trace the ransomware's point of entry. • **File System Analysis:** Analyzed the encrypted files and attempted to detect any remnants of the original data. • **Timeline Analysis:** Established a timeline of events from initial infection to encryption to understand the attack’s progression. • **Decryption Tool Research:** Looked into known decryption methods or tools to recover data without paying the ransom. **Outcome:** The forensic team identified a phishing email as the ransomware’s entry vector, likely due to an employee unknowingly clicking on a malicious link. The organization improved its email filtering, implemented employee security training, and adopted stronger backup practices to mitigate the effects of potential future incidents. **Questions:** a) What are the primary goals of forensic investigation after a ransomware attack? b) How does endpoint analysis contribute to identifying the attack vector? c) Why is it essential to establish a timeline of events in cyber forensic investigations? d) What measures could be implemented to avoid similar ransomware incidents in the future? e) How can educating employees improve a company’s cybersecurity posture?		