Universiti Tun Hussein Onn Malaysia

UNIVERSITI TUN HUSSEIN ONN MALAYSIA

FINAL EXAMINATION
SEMESTER II
SESSION 2023/2024

COURSE NAME	:	COMPUTER CRIME AND DIGITAL FORENSICS
COURSE CODE	:	BIS 30803
PROGRAMME CODE	:	BIS
EXAMINATION DATE	:	JULY 2024
DURATION	:	3 HOURS
INSTRUCTIONS	:	1. ANSWER ALL QUESTIONS 2. THIS FINAL EXAMINATION IS CONDUCTED VIA ☐ Open book ☒ Closed book 3. STUDENTS ARE **PROHIBITED** TO CONSULT THEIR OWN MATERIAL OR ANY EXTERNAL RESOURCES DURING THE EXAMINATION CONDUCTED VIA CLOSED BOOK

THIS QUESTION PAPER CONSISTS OF **SIX (6)** PAGES

PART A

Choose the **BEST** answer for each of the following questions.

Q1 Which of the following technique is **NOT** Windows non-volatile data?

(a) System version and patch level.

(b) History of login.

(c) Cached NetBIOS Name Table.

(d) Internet Information Services (IIS) log.

(2 marks)

Q2 Which root key in the Windows Registry contains configuration settings for hardware devices and drivers?

(a) HKEY_LOCAL_MACHINE.

(b) HKEY_CURRENT_CONFIG.

(c) HKEY_CLASSES_ROOT.

(d) HKEY_CURRENT_USER.

(2 marks)

Q3 What happens if the thumbnail cache becomes corrupted?

(a) Images will load faster.

(b) Images will fail to load properly or load slowly.

(c) Security of files will be enhanced.

(d) Thumbnails will be displayed in higher resolution.

(2 marks)

Q4 Which of the following is a crucial aspect of evidence handling as outlined in a forensic lab Standard Operating Procedures?

(a) Sharing evidence with unauthorized personnel.

(b) Altering evidence to fit a narrative.

(c) Maintaining the integrity and chain of custody of evidence.

(d) Discarding evidence after initial examination.

(2 marks)

Q5 What precaution should be taken before performing file carving in HxD editor?

(a) Disconnecting from the internet.

(b) Creating an image of the storage device.

(c) Disabling antivirus software.

(d) Increasing system RAM.

(2 marks)

PART B

Q6 Consider the following scenario:

A large financial institution has experienced a significant cybersecurity breach, resulting in the compromise of sensitive customer data and potential financial losses. The breach was discovered when the institution's IT security team noticed unusual network activity and suspected unauthorized access to critical systems.

As part of the investigation, forensic investigators are called in to analyze the Windows Registry on the affected machines to uncover evidence of the attack and identify the perpetrators. They aim to uncover any changes or anomalies in the registry that may indicate malicious activity, such as unauthorized user accounts, modified system configurations, or the presence of malware.

(a) Give **TWO (2)** reasons why registry is important to be used as digital evidence.

(4 marks)

(b) Identify **TWO (2)** artifacts that can be found in registry based on your answer in **Q6(a)**.

(4 marks)

(c) In windows registry, there are only **TWO (2)** root keys that have hives. Identify the keys and locate the hives.

(6 marks)

(d) One file named "malware.xlsx" related to the evidence is stored in one targeted machine. The size of the file is 2012 bytes.

By assuming that one cluster contains 3 sectors while one sector consists of 512 bytes, illustrates file slack, drive slack and ram slack of the file.

(6 marks)

Q7 Based on the given scenario, answer the following questions.

A large financial institution, FinanceSecure Sdn. Bhd. experiences a significant cyberattack resulting in the compromise of customer data and financial records. The attack is sophisticated, involving multiple vectors such as malware, phishing, and social engineering. FinanceSecure's digital forensics team is tasked with investigating the incident to determine the extent of the breach, identify the attackers, and gather evidence for potential legal action. They found an unknown old mobile phone disposed nearby the server room. They also found a trace of IP address from Nigeria. The team decided to sit together to plan the next move for the investigation.

(a) Discuss **FOUR (4)** challenges that the team will face during the investigation.

(8 marks)

(b) Propose **TWO (2)** mitigation strategies for the challenges.

(5 marks)

(c) Do you think law enforcement should have the authority to conduct searches without a warrant? Justify your answer.

(3 marks)

(d) Does the issue relate to forensic accounting? Justify your answer.

(3 marks)

Q8 Consider the following scenario:

In the early 2010s, the world witnessed a groundbreaking event in the realm of cyber warfare: Operation Stuxnet. This secret operation, believed to be a joint effort between American and Israeli intelligence agencies, aimed to sabotage Iran's nuclear program by targeting its uranium enrichment facilities.

At the heart of Operation Stuxnet was a highly sophisticated computer worm, named Stuxnet. Disguised as a seemingly harmless file, Stuxnet exploited multiple zero-day vulnerabilities in Microsoft Windows and Siemens industrial control systems, allowing it to infiltrate Iran's nuclear infrastructure undetected.

Once inside the target network, Stuxnet sought out specific Siemens programmable logic controllers (PLCs) used in centrifuge machines for uranium enrichment. It then proceeded to manipulate the PLCs' operations, causing them to spin at erratic speeds and ultimately sabotaging the delicate process of uranium enrichment. By exploiting trusted channels such as USB drives, Stuxnet managed to infect numerous systems within the Iranian nuclear facilities.

The consequences of Operation Stuxnet were profound. Iran's uranium enrichment efforts suffered significant setbacks, with reports suggesting that thousands of centrifuges were rendered inoperable. The incident dealt a severe blow to Iran's nuclear ambitions and sent shockwaves throughout the global cybersecurity community.

However, Operation Stuxnet also marked a turning point in the landscape of cyber warfare. It demonstrated the potential of offensive cyber capabilities to disrupt critical infrastructure and highlighted the growing significance of cyber-attacks as a tool of geopolitical warfare.

In the aftermath of Operation Stuxnet, nations worldwide began investing heavily in cybersecurity measures to protect their critical infrastructure from similar attacks. The incident served as a stark reminder of the vulnerabilities inherent in our interconnected digital world and underscored the need for constant vigilance in the face of evolving cyber threats.

(a) Define zero-day attack.

(2 marks)

(b) Cyber warfare is politically motivated hacking to conduct attacks on a target's strategic or tactical resources for the purposes of espionage or sabotage. In the given scenario, Cyber warfare demonstrated the potential of offensive cyber capabilities to disrupt critical infrastructure and highlighted the growing significance of cyber-attacks as a tool of geopolitical warfare.

(i) List **FIVE (5)** top Critical Infrastructures in Malaysia.

(5 marks)

(ii) Draw an architecture to differentiate offensive and defensive information warfare.

(6 marks)

Q9 Consider the following scenario:

CYberCorg Corporation is a multinational manufacturing company focusing on manufacturing smart appliances. CYberCorg relies heavily on IoT devices and cloud services to streamline operations, monitor equipment performance, and collect real-time data for analysis. However, CYberCorg experiences a significant security breach involving their IoT devices and cloud infrastructure. Malicious actors exploit vulnerabilities in the IoT devices to gain unauthorized access to sensitive data stored in the cloud. CYberCorg 's digital forensics team is tasked with investigating the breach to identify the root cause, assess the extent of the damage, and gather evidence for remediation and legal action.

(a) Analyze **FOUR (4)** difficulties that the team is likely to encounter throughout the investigation.

(8 marks)

(b) While implementing private investigation, propose **TWO (2)** methods of proficiency test that are needed to ensure the competency of the forensic investigator assigned by CyberCorg in handling the digital evidence.

(4 marks)

(c) Do employing physical and logical image acquisition methods are appropriate for this investigation? Discuss your answer.

(3 marks)

(d) Illustrate physical and logical image acquisition in hard disk drive architecture.

(3 marks)

- END OF QUESTIONS -