UNIVERSITI KUALA LUMPUR
MALAYSIAN INSTITUTE OF INFORMATION TECHNOLOGY

FINAL TEST
MARCH 2026 SEMESTER

COURSE CODE	:	IKB31404
COURSE NAME	:	CYBER FORENSICS
PROGRAMME NAME	:	BIT (HONS) IN COMPUTER SYSTEM SECURITY
DATE	:	25 JUNE 2026
TIME	:	9:00 AM-11:00 AM
DURATION	:	2 HOURS

INSTRUCTIONS TO CANDIDATES

1. Please CAREFULLY read the instructions given in the question paper.
2. This question paper has information printed on both sides of the paper.
3. This question paper consists of TWO (2) sections; Section A and Section B.
4. Answer ALL questions in Section A and Section B.
5. Please write your answers on the answer booklet provided.
6. Answer all questions in English language ONLY.

THERE ARE 12 PAGES OF QUESTIONS, INCLUDING THIS PAGE.

SECTION A (Total: 30 marks)

INSTRUCTION: Answer ALL questions.
Please use the answer booklet provided.

1. You are contracted to work as a computer forensics investigator for a regional bank that has four 30 TB storage area networks that store customer data.
What method would be most efficient for you to acquire digital evidence from this network?
   A. create a compressed copy of the file with DoubleSpace
   B. create a sparse data copy of a folder or file
   C. make a bit-stream disk-to-image file
   D. make a bit-stream disk-to-disk file

2. You are working for a large clothing manufacturer as a computer forensics investigator and are called in to investigate an unusual case of an employee possibly stealing clothing designs from the company and selling them under a different brand name for a different company. What you discover during the course of the investigation is that the clothing designs are actually original products of the employee and the company has no policy against an employee selling his own designs in his own time. The only thing that you can find that the employee is doing wrong is that his clothing design incorporates the same graphic symbol as that of the company with only the wording in the graphic being different. What area of the law is the employee violating?
   A. trademark law
   B. copyright law
   C. printright law
   D. brandmark law

3. Which type of attack aims to make a system or network resource unavailable to its intended users by overwhelming it with a flood of malicious traffic or exploiting vulnerabilities, thereby disrupting normal operations?
   A. SYN Flood Attack
   B. denial of service (DOS)
   C. Ping of Death Attack
   D. Man in the Middle Attack

4. The offset in a hexadecimal code is:
   A. The last byte after the colon
   B. The 0x at the beginning of the code
   C. The 0x at the end of the code
   D. The first byte after the colon

5. When reviewing web logs, you see an entry for resource not found in the HTTP status code field. What is the actual error code that you would see in the log for resource not found?
   A. 202
   B. 404
   C. 606
   D. 999

6. A master boot record (MBR) is the first sector ("sector zero") of a data storage device. What is the size of the MBR?
   A. Depends on the capacity of the storage device
   B. 1048 Bytes
   C. 4092 Bytes
   D. 512 Bytes

7. Which of the following artifacts is often used to track USB device connections on a Windows system?
   A. RecentDocs
   B. Ntuser.dat
   C. USBStor key in the registry
   D. Pagefile.sys

8. Which of the following is an anti-forensic technique used to prevent the recovery of deleted files?
   A. File slack manipulation
   B. File fragmentation
   C. Data wiping
   D. File carving

9. Which of the following is NOT an anti-forensic method used to avoid detection of deleted files?
   A. File slack space manipulation
   B. Encryption of deleted files
   C. File system timestamps modification
   D. Creating disk images for analysis

10. Which of the following file systems is most associated with the challenges of file carving?
   A. FAT32
   B. NTFS
   C. EXT4
   D. All of the above

11. Which of the following is an anti-forensic technique used to hide the presence of files or data?
   A. Data obfuscation
   B. File carving
   C. Disk encryption
   D. File compression

12. What does the primary purpose of the Windows "Prefetch" folder in digital forensics?
   A. To store temporary system files
   B. To track recently executed programs for performance optimization
   C. To log security events
   D. To store deleted files for recovery

13. What layer of the OSI model does TCP and UDP utilize?
   A. Data Link
   B. Network
   C. Transport
   D. Session

14. File carving typically operates on which type of data?
    A. Encrypted files only
    B. Raw disk images or unallocated space
    C. System logs
    D. Compressed files

15. E-mail logs contain which of the following information to help you in your investigation?
    I. user account that was used to send the account
    II. Attachments sent with the e-mail message
    III. Unique message identifier
    IV. Contents of the e-mail message
    V. date and time the message was sent
    A. I, II, III
    B. I, II, IV, V
    C. I, III, IV, V
    D. II, IV, V

16. A company's web server became unresponsive due to a suspected Denial of Service (DoS) attack. What is the primary indicator of a DoS attack that the investigator should look for in network logs?
    A. Multiple failed login attempts
    B. High volume of incoming traffic from a single IP
    C. Unauthorized file access attempts
    D. Sudden drop in outbound traffic

17. An organization detected unauthorized access to its internal network via a compromised Wi-Fi access point. What is the first step the forensic investigator should take to identify the unauthorized device?
    A. Perform a site survey to detect rogue devices
    B. Change the Wi-Fi network's SSID and password
    C. Disable the compromised access point
    D. Review DHCP logs for unknown MAC addresses

18. A company's network monitoring system detected unusual outbound traffic during non-business hours. The security team suspects data exfiltration. Which initial step should the forensic investigator take to analyze the suspicious traffic?

A. Examine firewall logs for outbound connections
B. Analyze employee emails for sensitive information
C. Review physical security camera footage
D. Conduct employee interviews

19. A company's CEO reports receiving an email from a trusted partner, but the email contained unusual content and a suspicious attachment. The CEO did not open the attachment. As an investigator, you are asked to determine whether the email was spoofed. Which email header field should you examine to verify the authenticity of the sender's email address?

A. To:
B. CC:
C. Return-Path:
D. Date:

20. What analysis can help determine if the email's sender address was forged?

A. Comparing the 'From' address with the 'Return-Path' address.
B. Checking the email's subject line for anomalies.
C. Reviewing the email's body content for spelling errors.
D. Scanning the attachment for malware.

21. In the FAT file system, what is the most likely consequence when the root directory becomes corrupted due to improper formatting or tampering?

A. The entire file system becomes unreadable, preventing all data access.
B. Only the file names and directories in the root directory are affected, and data in other directories remains intact.
C. The FAT table becomes unresponsive, leading to complete data loss.
D. The FAT table and all associated data blocks are unaffected, allowing full data recovery.

22. A forensic investigator is analyzing a FAT file system for deleted files. During the analysis, they encounter "unallocated clusters" within the file system. The investigator uses file carving techniques to recover deleted files, but some of the recovered files appear corrupted or incomplete.

Which of the following factors is most likely to explain why the recovered files are incomplete?

A. The deleted files' data is overwritten by new data, leading to partial recovery.
B. The forensic tool failed to identify the correct cluster chain, resulting in incomplete file reconstruction.
C. The FAT file system doesn't store the file size, making carving impossible.
D. The FAT file system stores all data sequentially, which prevents carving from being effective.

23. A phishing email urges the recipient to act immediately by claiming their account will be suspended within 24 hours. Why is this tactic significant in phishing analysis?

A. It improves email delivery speed
B. It exploits urgency to reduce rational decision-making by the victim
C. It allows attackers to bypass spam filters
D. It ensures the email cannot be traced back to the sender

24. During a phishing investigation, an analyst notices that the "From" email address appears legitimate, but the "Received" headers show multiple unfamiliar mail servers. What is the most reasonable conclusion the investigator should draw?

A. The email is legitimate because the sender address matches a trusted domain
B. The email was likely spoofed and routed through unauthorized servers
C. The email was encrypted to protect user privacy
D. The email was delayed due to network congestion

25. During a cyber forensic investigation, an employee claims they unknowingly disclosed login credentials after receiving an urgent email from "IT Support." The email used the correct company logo, internal language, and a spoofed sender address.

Which factor would **MOST** strongly support the conclusion that this was a targeted social engineering attack rather than a generic phishing attempt?

A. The email requested the employee to click on a hyperlink
B. The attacker used technical terminology related to IT systems
C. The email content was customized using internal organizational details
D. The email bypassed the organization's spam filtering system

26. A forensic analyst finds that multiple employees fell for the same phishing email despite security training. Which factor BEST explains this outcome from a social engineering analysis perspective?
A. Weak encryption algorithms used by the organization
B. Attackers exploited psychological triggers such as authority and urgency
C. Lack of antivirus software on employee devices
D. Poor network firewall configuration

27. Which digital evidence would be **MOST** useful for analyzing whether a WhatsApp message was part of a social engineering attack?
A. Device IMEI number only
B. Message content, timestamps, and sender profile information
C. Battery usage logs of the mobile phone
D. Operating system version of the device

28. When analyzing a packet capture (PCAP) file, which combination of packet information is **MOST** useful for identifying suspicious network behavior?
A. Packet color coding and capture file size
B. Source IP, destination IP, protocol, and timestamps
C. Network adapter type and operating system version
D. Packet checksum values only

29. During network forensic analysis, what does a source IP address in a packet generally represent?
A. The device that received the packet
B. The network firewall address
C. The device that sent the packet
D. The internet service provider location

30. During a forensic examination, an investigator finds that a suspect's browser history is empty, but cached files and cookies related to multiple websites are still present. What is the **MOST** logical explanation based on browser analysis?

A. The websites were accessed through private browsing mode, which stores cache but not cookies

B. The browser history was selectively deleted while other browser artifacts remained intact

C. The cache files were automatically generated without user interaction

D. The browser was never used, and the artifacts are system-generated

SECTION B (Total: 50 marks)

INSTRUCTION: Answer ALL questions.
Please use the answer booklet provided.

Question 1 (20 marks)

A suspected domestic terrorist code named "Ramlee" was observed purchasing explosive materials and investigators believe that he is involved in planning an attack in Kampung Duyong. You have been asked to perform a forensic analysis of his laptop to determine the target of the attack and information that may lead to the identification of others involved in the terrorist plot. This is purely a fictional case scenario developed for academic purposes.

i. If you received the laptop which was switched off, describe how you will proceed to have a forensics copy of the data from the HDD of the laptop, ensuring that the evidence is not damaged or altered in any way.

(12 marks)

ii. Name a tool that can be used to make a forensic copy of the HDD.

(1 marks)

iii. Please suggest options other than logical acquisition that forensic analysts can take into consideration.

(1 marks)

iv. Based on the answer in (iii), state **ONE (1)** difference between these techniques with logical acquisition.

(2 marks)

v. Why a forensically tool should be used to make the copy of the HDD instead of using a backup tool? State **TWO (2)** reasons.

(4 marks)

Question 2 (20 marks)

You were assigned with a case where a teenager had run away from home. During the interrogation with his friend, you find out that the boy mostly spent a lot of time on the Internet.

i. Suggest **TWO (2)** area that you will investigate in internet browser to find his interest. Your elaboration should include the technique of investigation and characteristics of that investigation area.

(6 marks)

ii. Before the boy went missing, he had received an email from someone that was not from his ordinary contact. Identify **FOUR (4)** information that you can retrieve from the email header of the sender.

(4 marks)

iii. Suggest another **TWO (2)** areas related to the email that you will investigate to find clues of the sender.

(4 marks)

iv. While searching for other information in the device, you also found, files that were password protected. Elaborate **TWO (2)** common technique used to crack the password.

(6 marks)

Question 3 (10 marks)

During a digital forensic investigation, an examiner recovered the following executable files from a suspect's computer:

File Name	File Size
update.exe	2.5 MB
gamepatch.exe	3.1 MB
invoice_viewer.exe	2.5 MB

The investigator suspects that one or more of these files may be malware. To verify the files, the investigator generates cryptographic hash values (e.g., SHA-256) and compares them with entries in known malware databases. As a digital forensic investigator:

(a) Explain the purpose of generating cryptographic hash values during a malware investigation.

(3 marks)

(b) Describe how hash values can be used to identify whether a recovered executable file is known malware.

(3 marks)

(c) Analyze **TWO (2)** advantages of using hashing techniques to support digital forensic and malware investigations.

(4 marks)

END OF EXAMINATION PAPER