UNIVERSITI KUALA LUMPUR
MALAYSIAN INSTITUTE OF INFORMATION TECHNOLOGY

FINAL TEST
MARCH 2026 SEMESTER

COURSE CODE	:	IKB42503
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. Faris is trying to locate where an email administrator stores the email system's .db files. He uses .log as his search criteria in a third-party tool. What log files, related to email, will Faris find?

   I. Logged events for attachments received
   II. Logged events for messages
   III. Logged events for messages rejected
   IV. Logged events for accounts accessing email

   A. I and II
   B. II and IV
   C. I, II and III
   D. III and IV

2. Faris is a forensics examiner specializing in email forensics. He does not like it when an email administrator uses log rotation instead of logging. Why does Faris dislike log rotation?

   A. Log rotation makes it harder to recover logs over time.
   B. Log rotation removes email header information, so it is impossible to see who wrote an email.
   C. Log rotation overwrites the log file after a certain size or time. After the log is overwritten, the log cannot be recovered except if it has been backed up.
   D. Log rotation triples the amount of work Faris must do to recover log files because, depending upon the number of days that the logs are kept, that will determine the number of log files Faris must review to find the right files.

3. Faris is investigating a case involving online threats toward a poll worker during the last election cycle. The poll worker was receiving increasingly disturbing emails from an individual. Eventually, Faris was able to catch the individual by searching the email messages he sent to the poll worker. How did Faris use the sent email to find the suspect?

A. Faris examined the Enhanced/Extended Simple Mail Transfer Protocol (E/SMTP) ID and noticed it was identical to other email coming from the same email address, so he was able to pinpoint the suspect's location.

B. Faris examined the headers and encoding at the beginning and ending of the suspect's emails to trace the route the emails took through servers. That information allowed Faris to pinpoint the sender's location.

C. Through forensic linguistics, Faris was able to ascertain that the suspect was the same person sending the email messages because they had the same tone and style. He then searched a known database of suspects who are guilty of email threats and found the suspect.

D. The suspect signed his name to the message, and Faris was able to track him that way.

4. While investigating a suspect's home, Faris discovers a SIM card. SIM cards carry copious amounts of information that can be used to determine what the suspect has been doing. What is some of the information that can be found on a SIM card?

I. Message information
II. Attachments
III. Call data
IV. Location information

A. I and II
B. I and III
C. I, III and IV
D. II, III and IV

5. Faris must recover information from a mobile device that was just seized from a suspect's home. Out of all the methods of recovering information from a mobile device, which is the best way to recover it?

A. Acquire a forensic image
B. Use a USB port with a USB write-blocker and connect it to a Windows computer
C. Take pictures manually of each phone screen
D. Static acquisition

6. During an investigation at a suspect's home, Faris discovers a mobile device attached by USB to a laptop. When he sees this setup, he must disconnect the mobile device from the laptop immediately. Why is that important?

A. The laptop can be programmed to erase data on both devices simultaneously.
B. The mobile device can inject malware into the laptop directing the laptop to overwrite its hard drive rendering the laptop useless.
C. Disconnecting the devices immediately helps prevent synchronization that might occur automatically on a preset schedule and overwrite data on the device.
D. If left connected, timestamps and other important metadata could be lost, making it difficult to determine if or when a crime was committed.

7. Faris is a network administrator and strong believer in using defense in depth for protecting his company's network. What makes defense an important tool for network administrators?
A. Defense in depth is inexpensive to use.
B. Defense in depth is easy to use.
C. Defense in depth has multiple modes that can be chosen from, not all of them need to be used.
D. If one mode of protection fails, the others can be used to thwart an attack.

8. Faris works in digital forensics and is comparing notes with her friend Karim, who works in network forensics. They find there is a difference between the two, what is it?
A. In network forensics, you can work from the image to find most of the deleted or hidden files and partitions. Sometimes, you restore the image to a physical drive so that you can run programs on the drive. In digital forensics, you must restore the drive to see how malware that attackers have installed on the system works.
B. In digital forensics, you can see how malware that attackers have installed on the system works.
C. In digital forensics, you cannot work from the image to find hidden or deleted files, but you can with the tools in network forensics.
D. In digital forensics, you can work from the image to find most of the deleted or hidden files and partitions. Sometimes, you restore the image to a physical drive so that you can run programs on the drive. In network forensics, you must restore the drive to see how malware that attackers have installed on the system works.

9. Maryam's company is experiencing an attack whereby the company server is having trouble keeping up with the number of established connections. Requests come in to establish connections, but then no connection is established. What type of attack is this?

A. Ping of death
B. DoS flood
C. SYN flood
D. Trojan

10 Shida notices that her servers are acting strangely. She also notices that the Internet traffic that the servers are receiving are 100 times greater than normal. What does this usually mean?

A. SYN flood attack
B. DDoS attack
C. Ping of death attack
D. Ransomware attack

11. The _____ allow the user to save web pages they find interesting and may give insight into the user's activity.

A. Cache
B. Bookmark
C. Freespace
D. Link

12. The Google Chrome history file will NOT contain one of the following.

A. Only the URL of the first visit
B. Start time of the downloaded file
C. Path of the downloaded file
D. URLs typed into the address bar

13. Julia was using a Hex editor and discovered a JFIF file. What file format is JFIF, and what is the corresponding beginning hexadecimal value and offset?

A. JPEG at Hex value FFD9 starting at offset 1
B. JPEG at Hex value FFE0 starting at offset 2
C. Exif JPEG at Hex value FFE1 starting at offset 2
D. Exif JPEG at Hex value FFE1 starting at offset 1

14. Rahim is examining photos from a suspect's drive that were downloaded from a smartphone. The issue is that when the suspect downloaded the photos, he changed the format from jpeg to tif. As a forensics examiner, why should Rahim consider this to be a problem for his investigation?

A. The format change may have changed the image.

B. The metadata may not be reliable due to the format change from the original file type when transferred.

C. The format change may have corrupted the image.

D. The suspect erased the metadata before changing formats.

15. Isa finds a jpeg file on a hard drive and discovers that the image quality is bad. Although camera quality can affect image quality, what other issue can cause image quality with a jpeg to degrade?

A. JPEG files use lossy compression and saving it multiple times with different names removes bits of data that reduces image quality.

B. JPEG files use lossy compression and saving it multiple times with the same name reduces image quality.

C. JPEG files require high-quality hardware in order to be viewed and printed properly.

D. JPEG data loss is not significant for the average user to ever notice. It takes special tools to tell there has been a degradation of quality.

16. Edward is examining the disk space on a hard drive for evidence. He notices that there is a 10 MB gap between two partitions, but there is no assigned drive letter for that 10 MB. What could be the reason for there being no drive letter assigned?

A. The drive letter has been removed intentionally to hide data in that 10 MB of space.

B. The 10 MB space between the two partitions is normal.

C. The 10 MB space between the two partitions carries computer startup data.

D. The 10 MB of space is fragmented data and will be removed once the disk is defragmented.

17. Audrey is examining a computer hard drive that uses the FAT file system. As she examines file clusters, she notices there are several bad clusters among the good ones. Are bad clusters important to Audrey in her forensic examination of the hard drive?

A. Bad clusters are eliminated as usable disk space. So, Audrey must only look in good clusters for evidence since only they can carry data.

B. Bad clusters can determine how many read/writes the disk has had in its lifetime.

C. Good clusters can be marked as bad to hide evidence of a crime.

D. All hard drives have bad clusters; it's a normal part of the manufacturing process.

18. Darla has scoured social media for information on a suspect so that she can try and crack his computer password. How does examining social media help Darla with her attempt to crack a suspect's password?

A. Darla can use names of people, pets, and other data gathered from social media and add those to a brute force attack database.

B. Darla can use names of people, pets, and other data gathered from social media to guess the password or passphrase.

C. Darla can use names of people, pets, and other data gathered from social media to create a rainbow table.

D. Darla can use names of people, pets, and other data gathered from social media and add those to a dictionary (hybrid) attack database.

19. Kyle is searching for image files on a suspect's drive that contains child pornography. He wants to make his job as simple as possible and automatically filter known good files from view. This list contains the hash values of illegal files. What is this database called?

A. Illegal File Filter

B. Known File Filter

C. File Database Filter

D. Illicit Data Filter

20. Lucia is taking her first test in computer forensics at Seminole College. The first question is regarding how a file system works. How does Lucia answer this question?

A. A file system provides an operating system with a road map to data on a disk.
B. A file system only holds the data on a disk.
C. A file system only holds the operating system.
D. A file system only holds the registry files.

21. Shira is trying to examine a drive partition, but she can't. Encryption is blocking access to the partition. What must Shira do to decrypt the partition and allow her to examine it?
A. Reset the BIOS
B. Decrypt the whole drive
C. Decrypt the drive's boot sector
D. Move the hard drive to another computer

22. Haida has been asked to examine the suspect's computer registry for information that might be useful in her company's latest investigation. Why is examining the registry important to Haida's examination?
A. It's a database containing system and user information.
B. It's a database where data files are kept.
C. It's a database where only user information is kept.
D. It's a database where only system information is kept.

23. Joaquim is examining the registry in a recent Windows 10 acquisition and is looking for stored information for the current logged-on user. Which key should Joaquim examine?
A. HKEY_LOCAL_MACHINE
B. HKEY_CURRENT_CONFIG
C. HKEY_USERS
D. HKEY_CLASSES_ROOT

24. Kenneth is testing the accuracy of his compressed file (lossless). Once he checks the before and after compression hash values, he finds they do not match. What could be the reason for this error?
I. Software error
II. Hardware error
III. System crash
IV. The file itself

A. I and II
B. I and III
C. II and IV
D. III and IV

25. Bella is about to decrypt a hard drive. The best thing about decryption is that allocated data and unallocated data are not altered when the drive is decrypted. However, Bella does have a big concern about whole disk encryption. What is Bella concerned about?

I. Cracking the password or passcode
II. Recovering the decryption key
III. Automating the decryption process
IV. Making sure there is enough drive space

A. I and II
B. I and III
C. II and IV
D. III and IV

26. Colin is examining an x86 computer with a disk drive that uses a Master Boot Record (MBR). What firmware program does Colin need to be familiar with when examining this boot process?

A. EFI
B. UEFI
C. BIOS
D. CMOS

27. Jeremiah is looking for where the system configuration, date, and time information is stored when the power to the system is off. He's new to the field of Computer Forensics, so he needs some help. Where will Jeremiah find the information he's looking for?

A. BIOS
B. CMOS
C. GUID
D. UEFI

28. What are the main differences between public-sector investigations and private-sector investigations?

I. Private-sector investigations involve government agencies responsible for criminal investigations and prosecution. Public-sector investigations focus more on policy violations.

II. Private-sector investigations can become criminal investigations and public-sector investigations can become civil investigation depending upon the circumstances.

III. Public-sector investigations involve government agencies responsible for criminal investigations and prosecution. Private-sector investigations focus more on policy violations.

IV. The private sector can ignore criminal investigations, and the public sector can ignore civil investigations.

A. I and II
B. II and III
C. I and IV
D. III and IV

29. When conducting a computer investigation for potential criminal violations of the law, the legal processes you follow depend on local customs, legislative standards, and rules of evidence. In general, however, a criminal case follows three stages. What are those three stages?

A. Complaint, the investigation, and the prosecution
B. Complaint, discovery, and the trial
C. Complaint, service of process, and motions
D. Complaint, answer, discovery, and trial

30. Tyson is examining network logs. He discovers that a pattern has emerged regarding a single IP address assigned to one employee. It appears that this particular employee spends time on the Internet often. What is Tyson's next step?

A. Investigate the IP address and see where it leads
B. Investigate the employee and see what they are doing
C. Investigate the computer and see if it is infected with malware
D. Investigate the computer logs and see if anyone else is using that computer

SECTION B (Total: 50 marks)

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

Question 1 (25 marks)

A digital forensics laboratory received a removable storage media related to an old unresolved data theft case from several years ago. During the investigation, the forensic examiner discovered the following:

- Several files had been deleted from the storage media.
- The storage media used the FAT12 file system.
- Investigators must ensure that all evidence is legally admissible in court.

(a) Explain at least **FOUR (4)** important steps that should be performed by a forensic investigator from the moment the suspect computer is seized until evidence is presented in court.

(8 marks)

(b) The investigator plans to acquire data from the suspect's storage media. Discuss in **TWO (2)** differences between static acquisition and live acquisition.

(4 Marks)

(c) Explain the function of the following FAT12 components

(4 marks)

i. Boot Sector
ii. FAT Area
iii. Root Directory
iv. Data Area

(d) Explain how a deleted file can still be recovered from a FAT12 storage device.

(4 marks)

(e) Explain the process of file carving used to recover graphic file from unallocated space.

(5 marks)

Question 2 (25 marks)

A multinational technology company discovered that confidential research documents were leaked to competitors before the launch of a new product. Preliminary investigation suggests that the suspect used web browsers, encrypted messaging applications, social media platforms, and corporate email to conduct the exfiltration activities. As the lead forensic investigator, analyze the following scenarios.

(a) During analysis of the suspect's workstation, investigators discovered that the suspect attempted to clear browser history before the computer was seized.

(i) Explain **THREE (3)** browser artifacts that may still contain useful evidence even after browser history deletion.

(6 marks)

(ii) The suspect accessed a cloud storage platform using private/incognito mode. Critically evaluate whether private browsing completely prevents forensic recovery of browsing activities.

(5 marks)

(b) Investigators captured suspicious outbound traffic from the company network. The packet capture (PCAP) showed repeated encrypted connections from an internal host to an unknown external IP address during midnight hours.

(i) Explain **TWO (2)** forensic techniques that can be used to analyze suspicious network traffic in this scenario.

(4 marks)

(ii) Based on forensic principles, justify why encrypted traffic should still be considered valuable evidence even if the payload content cannot be decrypted.

(3 marks)

(c) The suspect allegedly sent confidential project details using a personal email account and later coordinated with external parties through social media direct messages.

(i) Explain how email header analysis can assist investigators in identifying the origin of suspicious emails.

(4 marks)

(ii) Critically discuss **TWO (2)** challenges faced during social media forensic investigations.

(3 marks)

END OF EXAMINATION PAPER