73

CONFIDENTIAL

UNIVERSITI KUALA LUMPUR

MALAYSIAN INSTITUTE OF INFORMATION TECHNOLOGY

FINAL EXAMINATION

JANUARY 2016 SEMESTER

COURSE CODE	:	IKB 31003
COURSE NAME	:	CYBER FORENSICS
PROGRAMME NAME	:	BIT (HONS) IN COMPUTER SYSTEM SECURITY
DATE	:	28 MAY 2016
TIME	:	2.00 pm – 4.30 pm
DURATION	:	2 HOURS 30 MINUTES

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. For Section B, answer ONE question ONLY
5. Please write your answers on the answer booklet provided.
6. Answer all questions in English language ONLY.

THERE ARE 5 PAGES OF QUESTIONS, EXCLUDING THIS PAGE.

SECTION A (Total: 75 marks)

INSTRUCTION: Answer ALL questions.

Please use the answer booklet given.

Question 1

(a) Describe your understanding about computer forensics.

(3 marks)

(b) What are the differences between computer forensics and network forensics?

(4 marks)

(c) To properly investigate an incident and possibly take action against the perpetrator, you'll need evidence that provides proof of the identity and actions of an attacker. From this statement:

i. Describe what computer evidence is.

(2 marks)

ii. Give **THREE (3)** elements that you can find in computer that categorized under computer evidence.

(3 marks)

(d) Briefly describe **FOUR (4)** main characteristics of private (corporate) investigations.

(4 marks)

(e) Describe **TWO (2)** of the most common types of corporate computer crime.

(2 marks)

(f) Briefly discuss **SEVEN (7)** points the use of Company Polices and Warning Banner which may help the corporate to address the crimes in corporate environment.

(7 marks)

Question 2

(a) When using computer forensic tool for an investigation, you will find **FIVE (5)** major function of forensics tool. Describe those functions.

(10 marks)

(b) At the forensic lab, you are required to do data acquisition. For the flexibility of analysis that will use different type of tools, create **TWO (2)** options of image copy.

(6 mark)

(c) What are the **TWO (2)** advantages and **TWO (2)** disadvantages of using Windows acquisition tools?

(4 marks)

(d) How can you prove that you made no changes to an original image during analysis?

(2 marks)

(e) Describe **THREE (3)** steps to update the Registry for Windows XP SP2 to enable write-protection with USB devices.

(3 marks)

Question 3

(a) Ali has been called upon to investigate a hacking incident reported by one of his clients. The company suspects the involvement of an insider accomplice in the attack. Upon reaching the incident scene, Ali secures the physical area, records the scene using visual media. He shuts the system down by pulling the power plug so that he does not disturb the system in any way. He labels all cables and connectors prior to disconnecting any. Critically explain **SEVEN (7)** steps what would be the next sequence of events until it is transported to forensic lab?

(7 marks)

(b) Evidence custody form is used to document the evidence. Explain how custody form will help in the investigation.

(3 marks)

(c) Majority of investigative work for termination cases involves employee abuse of corporate assets. Assume that you will investigate Internet abuse case. List **FOUR (4)** items that you require for an investigation involving e-mail abuse.

(8 marks)

(d) Although you were asked to do a thorough investigation of the case, you are afraid that this case will result in scope creep. Describe the effects of scope creep on an investigation in the corporate environment.

(3 marks)

(e) Forensics tools were being developed to help investigators in accomplishing forensics case. Explain the use of KFF ("Known File Filter") in a FTK tool to help investigator lessening the scoop creep issues.

(4 marks)

SECTION B (Total: 25 marks)

INSTRUCTION: Answer ONLY one question.

Please use the answer booklet given.

Question 4

Drive Size	Number of sectors per cluster
0-32 MB	1
33-64 MB	2
65-128 MB	4
129-255 MB	8
256-511 MB	16
512-1023 MB	32
1024-2047 MB	64
2048-4095 MB	128

(a) Table above describes the number of sectors assigned to a cluster on FAT 16 file system according to disk drive. Each sector is made up of 512 byte. Assume you want to save a 2000 byte file on 1.6 GB hard disk of FAT 16 file system. Answer the following questions:

i. Calculate the slack space in byte.

(4 marks)

ii. Use a diagram; show the allocation of space for the file.

(4 marks)

iii. How is saving a file ending up you create slack space in Windows.

(5 marks)

iv. Justify the importance of analyzing file slack in computer forensics.

(3 marks)

(b) Elaborate **THREE (3)** techniques of hiding data that commonly found during forensics analysis.

(9 marks)

Question 5

(a) You were assigned a task by your supervisor to find out a secret message sent via email by an employee to his partner. During the investigation, you found that the email was attached with file that has been compressed with a zip utility. As you examine, you found that the file was named Naluri.zip.

i. Write in detail explaining how to recover Naluri.zip for further investigation.

(4 marks)

ii. You were informed that the compressed file should contain graphic file. However, when you try to open the graphic file, the graphic editor prompt you with a message stating that the graphic file is corrupted. How will you recover back the graphic file?

(5 marks)

iii. The graphic file is now recovered. You suspected that the employee might hide secret message in the graphic file. What leads you to such conclusion?

(4 marks)

(b) You are assigned to investigate a case where a 12-years-old boy ran away from home. During the discussion with the parents, you were informed that the boy spent a lot of time surfing on the internet. This give you a clue that you need to analyze the boy's browsing history at his laptop. You will do data acquisition from the laptop and then you will analyze the artifacts created by the Internet Explorer in order to identify his whereabouts. Briefly describe **THREE (3)** files structure of interest that you might want to analyze.

(12 marks)

END OF EXAMINATION QUESTION