UNIVERSITY COLLEGE TATI (UC TATI)

FINAL EXAMINATION QUESTION BOOKLET	
COURSE CODE	: BNS 4253
COURSE	: COMPUTER FORENSICS
SEMESTER/SESSION	: 2-2023/2024
DURATION	: 3 HOURS

Instructions:

1. This booklet contains 5 questions. Answer **ALL** questions.
2. All answers should be written in answer booklet.
3. Write legibly and draw sketches wherever required.
4. If in doubt, raise your hands and ask the invigilator.

DO NOT OPEN THIS BOOKLET UNTIL YOU ARE TOLD TO DO SO

THIS BOOKLET CONTAINS 5 PRINTED PAGES INCLUDING COVER PAGE

QUESTION 1

Data acquisition process usually consist of creating a bit-perfect COPY of the digital media evidence. The aim of working on a copy of the evidence is to leave the original media intact, which allows for any evidence to be verified (proven accurate) at a later date.

a) Define the following term:

i) Computer Forensics (2 marks)

ii) Disaster Recovery (2 marks)

b) Consider the following situation from infamous hacker, Kevin Mitnick:

"I would sit across the street from McDonald's and I would take their order and tell them they were the 50th customer so your order is free. Please drive through your order is free," Mitnick reminisced. "People would drive up to the window and I would say, 'our weight detection system detected your car is a little heavy so we recommend the salad instead of the Big Mac."

i) From the statement above, explain in detail the types of attack that been used by Kevin Mitnick. (6 marks)

ii) Provide **TWO (2)** examples with detail explanations of countermeasure techniques to overcome that security attacks. (4 marks)

iii) State **THREE (3)** tools to discover the neighbor network area. (3 marks)

c) Explain the **THREE (3)** ways to determine the best data acquisition method. (6 marks)

d) Discuss which method is more efficient to acquire the data of cybercrime such as Wannacry. (4 marks)

e) Forensic investigator can remotely connect to a suspect computer via a network connection and acquire data from it. Discuss the difficulty of using remote acquisition to acquire data of Wannacry computers. (4 marks)

f) Give **THREE (3)** types of RAID level. (3 marks)

QUESTION 2

In a Network Security Lab, one student uses his smart phone to intercept network traffic and launch a Man-in-the-Middle attacks against UC TATI server. Since Man-in-the-Middle attack is launched through the computer network, the forensic investigator of this attack should deal with volatile and dynamic information.

a) Explain **FOUR (4)** types of network based evidence that may be gathered from the UC TATI network regarding this attack. (8 marks)

b) Discuss the **TWO (2)** challenges of collecting evidence from the student's mobile device. (4 marks)

c) State **THREE (3)** types of information that investigator may retrieve from the mobile device. (3 marks)

QUESTION 3

An important aspect of the forensic analysis process is to salvage all data from storage media and convert unreadable data into a readable form. Data can be hidden on a drive in many ways and it is not feasible to look for all of them in all cases, examiners should be able to identify the major sources of data or at least be able to recognize large amounts of missing data.

a) As a Forensic Analyst, state **FOUR (4)** main areas on media where useful data may be found. (4 marks)

b) Data hiding involves changing or manipulating a file to conceal information. Give **THREE (3)** examples of data hiding techniques. (3 marks)

c) Outline **FIVE (5)** standard procedures of Network Forensics. (5 marks)

d) What is the purpose of Tcmpdump tool? (2 marks)

QUESTION 4

a) As a forensic investigator, you are investigating a suspect drive that contains several password-protected files and other files with headers that do not match the extension. Describe **FIVE (5)** procedures you need to follow to retrieve the evidence.

(10 marks)

b) Handling of electronic evidence must follow three C's of evidence: care, control and chain of custody. Discuss **FOUR (4)** procedures that help maintain the chain of custody.

(8 marks)

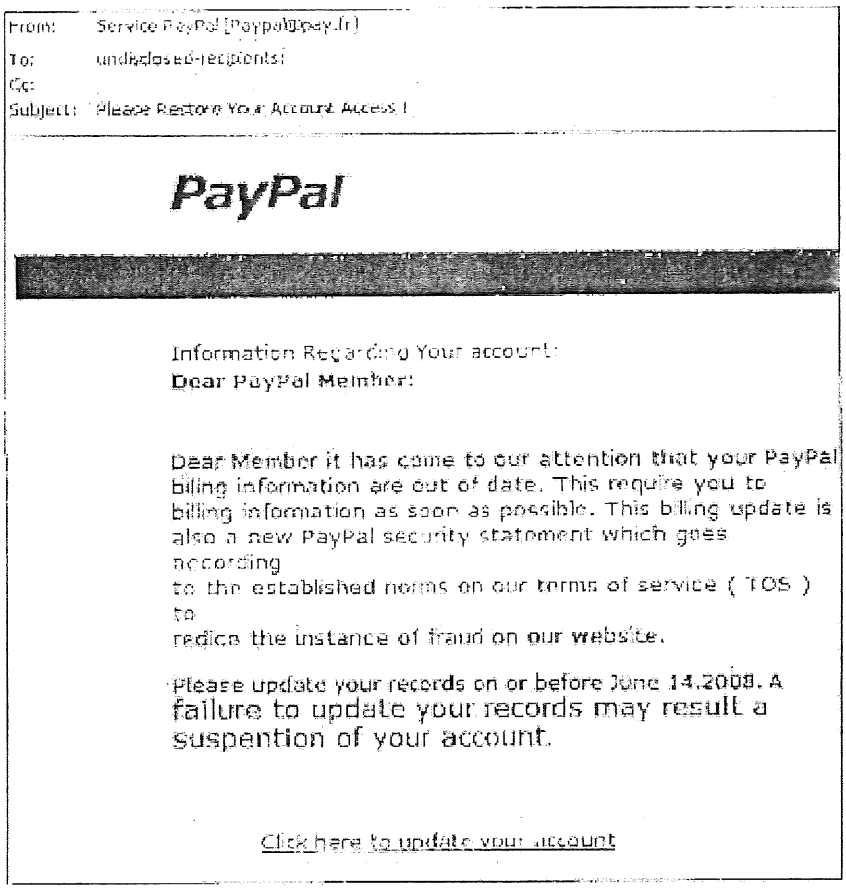
c) Give **FIVE (5)** information that should have in Chain of Custody form.

(5 marks)

d) Collecting evidence from a large drive can take several hours. Discuss the **TWO (2)** differences between logical and sparse acquisition. (4 marks)

QUESTION 5

Assume that you received the email shown in Figure 1.


From: Service PayPal [Paypal@pay.fr]
To: undisclosed-recipients:
Cc:
Subject: Please Restore Your Account Access !

PayPal

Information Regarding Your account:
Dear PayPal Member:

Dear Member it has come to our attention that your PayPal billing information are out of date. This require you to billing information as soon as possible. This billing update is also a new PayPal security statement which goes according
to the established norms on our terms of service (TOS) to
redice the instance of fraud on our website.

Please update your records on or before June 14,2008. A failure to update your records may result a suspention of your account.

Click here to update your account

Figure 1

(a) Explain on how to verify whether the email is normal or spoofed email. (4 marks)

(b) E-mail spoofing is the forgery of an e-mail header so that the message appears to have originated from someone or somewhere other than the actual source. Distributors of spam often use spoofing in an attempt to get recipients to open, and possibly even respond to, their solicitations. In terms of concerns and challenges, outline **SIX (6)** methods on how the email investigation process in digital forensics. (6 marks)

----------End of question----------