UNIVERSITY COLLEGE TATI

UNIVERSITY COLLEGE TATI (UC TATI)

FINAL EXAMINATION QUESTION BOOKLET	
COURSE CODE	: BNS 4253
COURSE	: COMPUTER FORENSICS
SEMESTER/SESSION	: 2 - 2024/2025
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 you in doubt, raise your hands and ask the invigilator.

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

THIS BOOKLET CONTAINS 4 PRINTED PAGES INCLUDING COVER PAGE

QUESTION 1

a) Give **TWO (2)** examples of the most common forensics tools for data acquisition. (2 marks)

b) What is the top priority to be considered in performing data acquisition? (2 marks)

c) Explain why mobile device attached to a PC via a cable or cradle/docking station should be disconnected from the PC immediately. (2 marks)

d) Briefly explain **FOUR (4)** methods of data acquisition. (8 marks)

e) Clarify **TWO (2)** reasons why we need to validate data acquisition. (4 marks)

f) Identify **TWO (2)** examples of data acquisition validation. (2 marks)

QUESTION 2

a) How to determine that a computer-generated records are considered authentic? (2 marks)

b) Clarify the top most concern when dealing with digital evidence. (2 marks)

c) Suggest **FOUR (4)** steps could be taken if you discover evidence of a crime during a company policy investigation. (8 marks)

d) Classify **EIGHT (8)** basic steps for preparing a search. (8 marks)

QUESTION 3

a) Identify and briefly explain **TWO (2)** examples of software that could be used to repair/recover image files. (4 marks)

b) Suggest **TWO (2)** techniques of password recovery. (4 marks)

c) Explain **TWO (2)** scenario that required remote data acquisition. (4 marks)

d) Suggest **THREE (3)** factors involve in examining and analyzing digital evidence. (6 marks)

e) Why we need to always validate our data acquisition process? (2 marks)

QUESTION 4

a) Identify **FOUR (4)** tools that could be used to capture the Random Access Memory (RAM). (4 marks)

b) Distinguish between computer forensics and network forensics. (4 marks)

c) Briefly describe **TWO (2)** skills an investigator needs when working with Virtual Machines. (4 marks)

d) Compare **TWO (2)** differences between Static Acquisition and Live Acquisition. (4 marks)

e) Briefly explain how to isolate the device from incoming signals when conducting mobile device investigations. (4 marks)

QUESTION 5

a) Identify **TWO (2)** types of common Operating System for smart phone. (4 marks)

b) Explain **THREE (3)** reasons why we need to isolate device from incoming signals. (6 marks)

c) Suggest **FIVE (5)** evidences that could be obtained from a suspect's cell phone to be presented in a murder case. (10 marks)

----------End of Question----------