NATIONAL UNIVERSITY OF SCIENCE AND TECHNOLOGY

FACULTY OF APPLIED SCIENCES

DEPARTMENT OF INFORMATICS AND ANALYTICS

DIGITAL FORENSICS

SCI 4201

Examination Paper
2024

This examination paper consists of 3 pages

Time Allowed: 3 hours
Total Marks: 100%
Examiner's Name: Dr. P. Nyoni

INSTRUCTIONS

1. This paper consists of five (5) questions
2. Answer any four (4) questions
3. All questions carry equal marks.
4. There are Two (2) sections in this paper. Section A is COMPULSORY and must be answered. You may choose to answer any Three (3) of the remaining questions.

MARK ALLOCATION

QUESTION	MARKS
1.	**25**
2.	**25**
3.	**25**
4.	**25**
5.	**25**

- SECTION A -

QUESTION ONE

You have been called to the residence of a suspected cyber-criminal. At the residence, you are informed that there is a laptop computer and a mobile device. **Outline** the steps you will take in the possible onsite examination of these devices. You should note how to properly **document** and handle these devices based on guidelines for law enforcement. As part of your outline, write about the type of **equipment** (hardware or software) the investigator should bring to the suspect's residence.

[25]

- SECTION B -

QUESTION TWO

a) Describe the fundamental principle for volatile data collection. **[3]**

b) What are the conditions under which volatile data should be collected? **[4]**

c) Describe five kinds of data you could find residing in memory and how they would be useful as evidence. **[12]**

d) What computer forensics tools can be used to image RAM memory? Are there any issues with using RAM as a source of evidence in an investigation? **[6]**

QUESTION THREE

a) Distinguish between private and public investigations. What are the main differences between the two? **[10]**

b) There are many challenges modern forensic investigators face in the profession. Describe any three challenges to forensics. **[6]**

c) Discuss the digital artifacts that can be found on a client computer relating to a user's network activity. **[6]**

d) Why are RAM captures necessary in some investigations? **[3]**

QUESTION FOUR

a) How do you ensure that a mobile phone is isolated from incoming signals after you have acquired it in an investigation? **[6]**

b) Performing cloud forensics is one of the more challenging tasks for forensic investigators. Identify three (3) issues you know and how you might overcome them. **[9]**

c) Differentiate between a bitstream copy and a regular copy in forensics? **[4]**

d) There are many ways a suspect can attempt to hide or destroy potential evidence on a hard disk. Identify three (3) the different ways data can be hidden from an investigator. **[6]**

QUESTION FIVE

a) Discuss each of the different storage formats that forensic tools can read. In your discussion the benefits and drawbacks of each format. **[10]**

b) GUI and command line tools can be used for forensic processes. Explain some of the commands used to acquire data from different operating systems. **[6]**

c) Describe methods for validating and testing computer forensics tools. **[5]**

d) Hashing is a technique often used by forensic investigators. What is hashing and why is it important? Give 2 examples of algorithms you know. **[4]**

END OF QUESTION PAPER