NATIONAL UNIVERSITY OF SCIENCE AND TECHNOLOGY

FACULTY OF APPLIED SCIENCES

DEPARTMENT OF INFORMATICS AND ANALYTICS

DIGITAL FORENSICS

SCI 4201

Examination Paper
Second Semester, 2025

This examination paper consists of 3 pages

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

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 answer any TWO (2) 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 with possible evidence. Outline the steps you will take as a forensic examiner in this scenario. You should note how to properly document and handle these devices based on guidelines for law enforcement. As part of your outline, describe the tools you would use. [25]

QUESTION TWO

a) Outline how the Cyber and Data Protection Act of 2021 affects an investigation and how it should be conducted. [8]

b) Discuss the Daubert Standard, showing how it relates to the activities done by forensic investigators. [8]

c) Evaluate the investigative triad, illustrating it with a detailed diagram. [9]

- SECTION B -

QUESTION THREE

a) Explain the importance of chain-of-custody in digital forensics. [1]

b) Evaluate **three** challenges that are faced by forensic investigators. [6]

c) Identify the factors you would consider when deciding which acquisition method to use for an investigation. [9]

d) Explain the benefits and drawbacks of each storage format for digital evidence.

[9]

QUESTION FOUR

a) GUI and command line tools can be used for forensic processes. Identify two commands used to acquire data using command prompt. [5]

b) Distinguish between private and public investigations in forensics. [8]

c) Using a business case, justify the need for a forensics lab within a large company. Outline the type of workstation, tools, and staff that should be included. [12]

QUESTION FIVE

a) In the context of digital forensics, explain the following terms:

i) Cross-Validation
ii) File Carving
iii) Imaging
iv) Metadata
v) Steganography [5]

b) Computer forensics examiners are required to create different types of reports. Describe the main guidelines for writing forensic reports. [8]

c) Ethics are very important and influence the way an investigation is done. Discuss four ethical codes of conduct you must follow as an investigator. [12]

END OF QUESTION PAPER