NAMIBIA UNIVERSITY
OF SCIENCE AND TECHNOLOGY

FACULTY OF COMPUTING AND INFORMATICS
DEPARTMENT OF CYBER SECURITY

QUALIFICATION : BACHELOR OF COMPUTER SCIENCE HONOURS (DIGITAL FORENSICS)	
QUALIFICATION CODE: 08BHDF	**LEVEL:** 8
COURSE: DIGITAL FORENSICS MANAGEMENT	**COURSE CODE**: DFM 811S
DATE: JUNE 2023	**PAPER:** THEORY
DURATION: 3H	**MARKS:** 100

FIRST OPPORTUNITY EXAMINATION QUESTION PAPER	
EXAMINER(S)	MR. JULIUS SILAA
MODERATOR:	DR. AMELIA PHILLIPS

THIS QUESTION PAPER CONSISTS OF 2 PAGES
(Excluding this front page)

INSTRUCTIONS

1. Answer ALL the questions on the answer scripts.
2. Write clearly and neatly.
3. Number the answers clearly.

PERMISSIBLE MATERIALS

1. Calculator.

Question 1

Digital forensics is the application of **computer science** and **investigative procedures** for a legal purpose involving the **analysis** of **digital evidence** after proper **search authority, chain of custody, validation with mathematics**, use of **validated tools, repeatability, reporting**, and possible **expert presentation**.

Discuss each of one of the twelve underlined key component of digital forensics in the definition above. (12 marks)

Question 2

a) Explain the difference between "live acquisition" and "post-mortem acquisition"(4 marks)

b) What are the advantages and disadvantages of live and post-mortem acquisition? (4 marks)

c) Give an example when "live digital forensics acquisition" is necessary (3 marks)

Question 3

a)Outline in detail any five anti-forensics techniques and highlight how each can be countered. (10 marks)

b) Digital forensics tools can fall into many different categories and many tools fulfill more than one function simultaneously, and a significant trend in digital forensics tools are "wrappers"—one that packages hundreds of specific technologies with different functionalities into one overarching toolkit.

Complete the table below by recommending at least three (3) sub functions per each category of function which investigator should ensure the tool possess. (12 marks)

#	***Functionality***	***Sub functions***
1	*Acquisition*	
2	*Validation and verification*	
3	*Extraction*	
4	*Reconstruction*	
5	*Reporting*	
6	*Automation and other features*	

Question 4

a)One important step in E-discovery is to capture as much evidence as possible before litigation. List any 4 possible sources of e- discovery evidence. (4 marks)

b)*Vindicator* legal practitioner law firm has hired you as their expert witness pending any litigation that may requires a lot of digital artefacts and evidence extracted from various internet sources. Discuss how time and cost consideration affect what tools *Vindicator* would select for discovery and ESI retention. (6 marks)

Question 5

Digital forensics experts need to be well versed in the collection, examination, preservation, and presentation of digital evidence. Experts must be thorough, treating every investigation like it's going to court, so their methods and documentation need to be incredibly detailed. Discuss any five (5) best and standard practises digital forensics experts must follow to ensure that their investigation is thorough and the evidence they present is credible.

(15 marks)

Question 6

Write a well-structured one-page essay about IoT Forensics.
Your essay should among other things provide a short background to this emerging technology, contrast digital forensics from IoT forensics, discuss IoT architecture, summarize the key challenges associated with IoT Forensics, and describe any other interesting trends and facts surrounding IoT forensics. (30 marks)

*******END OF PAPER*******