NAMIBIA UNIVERSITY
OF SCIENCE AND TECHNOLOGY

FACULTY OF COMPUTING AND INFORMATICS
DEPARTMENT OF CYBER SECURITY

QUALIFICATION : BACHELOR OF COMPUTER SCIENCE HONOURS IN DIGITAL FORENSICS	
QUALIFICATION CODE: 08BHDF	**LEVEL:** 8
COURSE: MOBILE AND CLOUD FORENSICS	**COURSE CODE:** MCF811S
DATE: JULY 2025	**PAPER:** THEORY
DURATION: 2H	**MARKS:** 100

SECOND OPPORTUNITY /SUPPLEMENTARY EXAMINATION QUESTION PAPER	
EXAMINER(S)	MR. JULIUS SILAA
MODERATOR:	DR. NKOSINATHI MPOFU

THIS QUESTION PAPER CONSISTS OF 4 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 **[5 marks]**

Match each cloud forensics concept or challenge in Column A with its corresponding description or action in Column B by writing the correct letter (A–E)

Column A: Concept/Challenge	Answer	Column B: Description/Action
1. Establish legal and contractual clarity	____	**A.** Capture memory dumps (volatile) and disk images (non-volatile) to retain critical data.
2. Understand Cloud Service Models and Deployment Types	____	**B.** Ensure agreements define data access, ownership, and forensic responsibilities before investigation.
3. Collaborate with Cloud Service Providers	____	**C.** Recognize SaaS, PaaS, IaaS, and public, private, or hybrid clouds to guide investigation scope.
4. Collect volatile and non-volatile data	____	**D.** Work with providers to access logs, backups, or virtual machine snapshots.
5. Preserve evidence with minimal alteration	____	**E.** Use hashing (e.g., MD5, SHA-1) and write-blockers to avoid modifying original data.

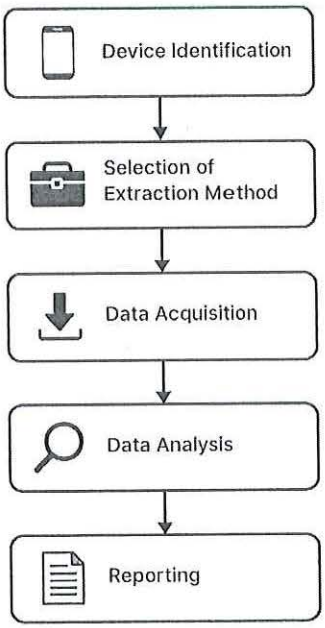
Question 2 **[15 marks]**

Understanding Android data acquisition techniques and their interaction with the system's security and file structure is essential for effective mobile forensic investigations.

Briefly explain the difference between logical extraction, physical extraction, and file system extraction in the context of Android data acquisition. Provide one practical example of when each technique might be used.

Question 3 **[15marks]**

Examine the following Android forensic data extraction workflow diagram which consists of Device identification, Selection of extraction method, Data acquisition, Data analysis, and Reporting. Select and explain any stage from the provided workflow where data integrity could be compromised if proper procedures are not followed. (15)



Question 4 **[15 marks]**

a) Expand and provide a brief description of the following acronyms associated with Apple File System (APFS) encryption:

i. AES
ii. XTS
iii. CBC (5)

b) Contrast AES-XTS or AES-CBC encryption in the Apple File System (APFS) from their predecessor Hierarchical File System (HFS), focusing on the following aspects:

i. HFS encryption limitations
ii. Modern Algorithms AES-XTS and AES-CBC features and their significancy
iii. Three Modes of AES-XTS and AES-CBC encryption (10)

Question 5 **[25 marks]**

Describe the following features in the Apple File System (APFS) and why they are significant for modern data management: (25)

i. Clones
ii. Snapshots: Point-in-Time (PIT)
iii. Crash protection: Copy On Write (COW) metadata scheme
iv. Sparse files
v. Space sharing

Question 6 **[15 marks]**

Understanding techniques for bypassing Android passcodes and rooting devices, along with their prevention and risks, is essential for assessing mobile security and forensic implications.

a) Besides rooting or using recovery mode, describe three methods to bypass passcodes on Android devices. (6)

b) Explain how each method identified in (a) can be prevented. (3)

c) Describe three methods to root an Android device and list three potential risks of rooting. (6)

Question 7 **[10 marks]**

a) This semester, you completed a class group project focused on cloud forensics. In your class group project, you worked with a cloud computing platform (such as AWS or Google Cloud) and now need to preserve its data for future analysis. Identify one specific step you could take to save a copy of the cloud instance and explain why this action would be beneficial. (3)

b) After doing activities on a cloud computer, the project asks you to bring files like memory dumps or snapshots to your own computer for closer inspection—what is one reason you might download files like a memory dump or snapshot to your own computer? (3)

c)The project involves making a pretend suspicious file called malware.txt on a cloud computer to see how it behaves when you use it—describe one thing you could do with a file like malware.txt to make sure it leaves a trail in the cloud instance. (4)

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