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: June 2025	**PAPER:** THEORY
DURATION: 2H	**MARKS:** 100

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

THIS QUESTION PAPER CONSISTS OF 3 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 **[10 Marks]**

a) Extracting data from a SIM card in a forensically sound manner requires following a specific sequence of steps to ensure data integrity and admissibility in investigations. Put the following steps in the correct order in accordance to the current best practice for extracting data from SIM card in forensically sound manner.

i. Extract data from the device

ii. Reserve the evidentiary SIM card in the evidence locker

iii. Extract data from the evidentiary SIM card

iv. Remove the evidentiary SIM card from the device

v. Place the cloned SIM card in the device

vi. Create a clone (network-isolated) SIM card (6)

b) The first step in a forensic examination of mobile device should be identifying the device model. Why is this important? (4)

Question 2 **[20 Marks]**

Exploring Android's development, architecture, and security mechanisms provides insight into its growth as a leading mobile operating system and its approach to user protection.

a) What are the key milestones that have defined Android's evolution from its inception to its current version? (4)

b) How do the core components of Android's architecture, such as the Linux Kernel, Android Runtime (ART), and Application Framework, work together? (8)

c) How does Android ensure user security through features like app permissions, encryption, and Google Play Protect? (8)

Question 3 **[15 Marks]**

Digital forensics in mobile and cloud environments is critical for uncovering evidence, with SIM cards and cloud systems presenting unique opportunities and obstacles for investigators.

a) List five digital forensics artifacts that can be retrieved from a mobile phone's SIM card. (5)

b) Describe any five challenges of acquiring evidence from the cloud. (5)

c) How does log data contribute to effective cloud forensics investigations? (5)

Question 4 **[20 Marks]**

a) In iOS backup, the **sms.db** file contains timestamp values, which could be in Unix Epoch or Cocoa Core Data format. Determining the correct format is crucial for accurate time-based analysis.

You are analysing an iOS backup and encounter a timestamp value of '672,345,890' in the **sms.db** file. Explain without performing the real calculations how you would determine whether this is a Unix Epoch or Cocoa Core Data timestamp. (4)

b) Mobile forensic extraction from iOS artifact sources like the **CallHistory.storedata** SQLite database, which holds call logs, requires selecting the right technique—logical, filesystem, or cloud—based on device access, security, and investigation needs for effective evidence collection.

Discuss when it is appropriate to perform mobile forensic data extraction from a typical artifact source such as **CallHistory.storedata** SQLite database on an iOS device using the following techniques: **(12)**

i. logical extraction (4)

ii. filesystem extraction, and **(4)**

iii. cloud extraction. (4)

Your response should emphasize when to use each method and why not the other two alternatives in those specific scenario

c) The SQLite Write-Ahead Log (WAL) in an iPhone's **sms.db** file may hold important artifacts

A forensic investigator needs to recover deleted text messages from an iPhone's ***sms.db file***. Explain the role of WAL in this process (4)

Question 5 **[20 marks]**

The following presents four different scenarios involving a recovered iOS device after a crime has been committed. For each scenario, the question asks for the actions that can be taken to preserve information on the device. The scenarios are:

a) Device turned on and unlocked (4)

b) Device turned on and locked (4)

c) Device turned off and without passcode (4)

d) Device turned off and with passcode (4)

Question 6 **[15 marks]**

a) This semester, you completed a class group project focused on cloud forensics. Reflecting on your class group project, you utilized a cloud computing platform (such as AWS or Google Cloud). Identify one step you could take to save a copy of a cloud instance and explain why this action could be beneficial. (5)

b) A memory dump is like a snapshot of what a cloud computer is thinking about at a certain moment, captured using a tool during this project—what is one type of evidence you could collect from a memory dump, and how might it help you understand what happened? (5)

c) In this class group project, you pretend to send messages over the internet from a cloud computer and save them in a file to look at later—mention one tool you could use to look at a network capture file and describe something you might find in it.(5)

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