NAMIBIA UNIVERSITY
OF SCIENCE AND TECHNOLOGY
FACULTY OF COMPUTING AND INFORMATICS

DEPARTMENT OF COMPUTER SCIENCE

QUALIFICATION: BACHELOR OF COMPUTER SCIENCE (HONS DIGITAL FORENSICS)	
QUALIFICATION CODE: 08 BHDF	**LEVEL: 8**
COURSE: MOBILE AND CLOUD FORENSICS	**COURSE CODE:** MCF811S
DATE: JUNE 2022	**SESSION:** THEORY
DURATION: 1 HOUR 30 MINUTES	**MARKS: 50**

FIRST OPPORTUNITY EXAMINATION QUESTION PAPER	
EXAMINER(S)	DR ATTLEE M. GAMUNDANI
MODERATOR:	MR PICKY S. KAUMUNIKA

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

INSTRUCTIONS

1. Answer ALL the questions.
2. Write clearly and neatly.
3. In answering questions, be guided by the allocated marks.
4. Number your answers clearly following the numbering used in this question paper.

PERMISSIBLE MATERIALS

1. None

Section A: 24 Marks [CASE STUDY]

The Last Argument

She was married just a few months before her death. Her husband took her life and then his own. Her phone was triaged through a forensic tool commonly used by law enforcement. The initial investigation located two short recordings that documented arguments they had been having. She had recorded them without his knowledge, just days prior to their bodies being discovered. After the phone was triaged, the case agent reviewed the case report (media disk). He called the examiner back a few days later. "I believe there's another large file on her phone that recorded the events that took place at her death. Can you try to get it to play?" The file had initially been "looked over" and dismissed as a corrupt, unplayable sound file. Per the request of the case agent, the file was viewed with additional scrutiny. Using a hex editor, it was found that the file header and footer were missing, but the case agent may be correct; based on the size of the file, and the time and date of its creation, she probably did record her own death.

Question 1

If we define Mobile Forensics as the process of **(a) recovering** mobile-related **(b) data** through a forensic examination using **(c) validated** means. Considering the highlighted and underlined keywords in this definition (**a**), (**b**) and (**c**),

(a) Explain with reference to the given study what (i) recovering and (ii) data entails. ***[4 marks]***

(b) Explain the four ways in which data that is acquired off mobile devices from the case study, will be validated. ***[8 marks]***

Question 2

In the context of the given case study, (a) Give and explain any strengths and (b) any two weaknesses for the two types of data available for this case? ***[12 Marks]***

Section B: 26 Marks

Question 1

(a) Base stations are key components in Mobile Forensics. Explain why that is the case, giving an example where necessary. ***[3 Marks]***

(b) What would you say is the primary function of a SIM card? ***[2 Marks]***

(c) In addition to a SIM, most cellphones have a (n)? (for unique identification) ***[1 Mark]***

Question 2

(a) Those involved in system administration should know about Mobile Forensics. Give and explain any three reasons. ***[6 Marks]***

(b) The general rules of evidence apply across board when considering Mobile and Cloud Forensics. Identify any three such rules and explain each of them in brief. ***[6 Marks]***

Question 3

(a) Mobile Forensics is filled with challenges, which are yet to be addressed for full solution provision. Identify and explain any such challenges. ***[2 Marks]***

(b) *Penda an IT equipment supplier based in Katutura gets an order for 5000 Laptop hard drives from Ndapa* via WhatsApp. Ndapa is an ex-girlfriend to Penda. The whole transaction was processed and agreed via WhatsApp. When the order was ready, Ndapa says she did not place the order. John retrieves the WhatsApp messages sent by Ndapa. Ndapa still insists she did not send the request. You have been tasked to investigate this case, as it happens to be a case of money laundering scheme by a South African Drug Cartel. Penda's bank raised a flag when they saw a huge deposit into his bank account following the order. **Outline the proper chain of custody you are going to follow.** ***[6 marks]***

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