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 FORENSICS	**COURSE CODE:** MBF821S
DATE: NOVEMBER 2019	**SESSION:** THEORY
DURATION: 2 HOURS	**MARKS:** 70

FIRST OPPORTUNITY EXAMINATION QUESTION PAPER	
EXAMINER:	DR. ATTLEE M. GAMUNDANI
MODERATOR:	DR. AMELIA PHILLIPS

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

INSTRUCTIONS

1. Answer ALL the questions.
2. Write clearly and neatly.
3. Begin each question on a new page.
4. Number the answers clearly as per the question paper numbering.
5. Marks/Scores per question paper are given in [].
6. NUST examination rules and regulations apply.

PERMISSIBLE MATERIALS

1. None

Question 1

(a) Mobile Forensics is a branch of digital Forensics. What therefore does mobile forensics entail which makes it different from digital forensics in general? ***[4 Marks].***

(b) Mobile phones are dynamic systems that present a lot of challenges to the examiner in extracting and analysis of digital evidence. Identify any four (4) such challenges and explain why they are a challenge towards extracting or analysing of digital evidence ***[12 Marks].***

(c) Give four (4) uses or purpose that the SIM card provides ***[4 Marks].***

Question 2

(a) Since there is no well-established standard process for mobile forensics evidence extraction, Figure 1 is an overview of process considerations for extraction of evidence from mobile devices. Explain briefly what takes place during: -

- **(i).** Identification ***[2 marks].***
- **(ii).** Isolation ***[2 marks].***
- **(iii).** Verification ***[2 marks].***
- **(iv).** presentation ***[2 marks].***

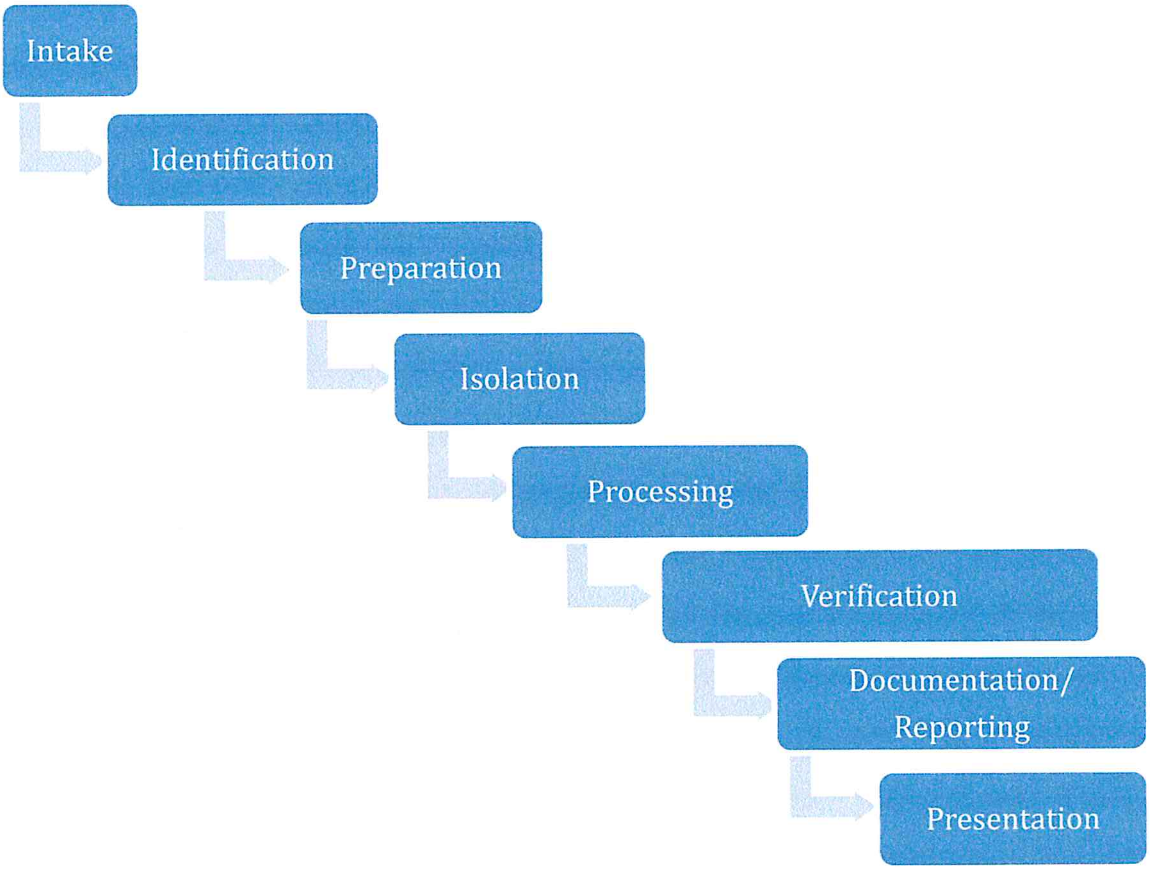

Figure 1: Evidence extraction process

(b) Explain briefly what each of the following data acquisition methods entails

- **(i).** Physical ***[4 marks].***
- **(ii).** Logical ***[4 marks].***
- **(iii).** Manual ***[4 marks].***

Question 3

(a) When identifying the appropriate tools for the forensic acquisition and analysis of mobile phones, a mobile device forensic tool classification system displayed in Figure 2 is very useful. Explain with some examples what happens at the following stages

- **(i).** Manual Extraction ***[3 marks].***
- **(ii).** Chip- off ***[4 marks].***
- **(iii).** Micro Read ***[3 marks].***

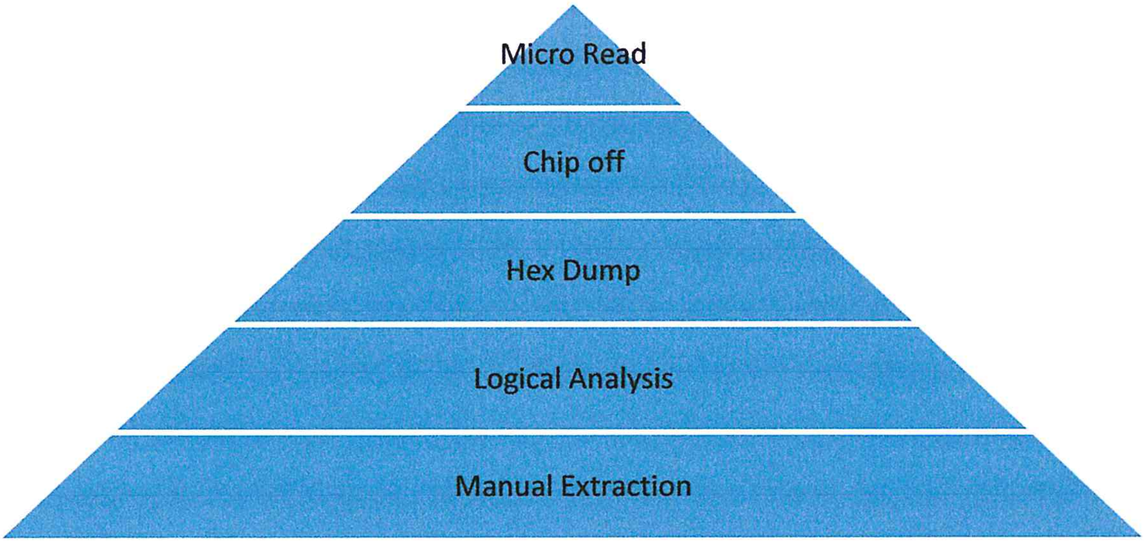

Figure 2: Cellular phone tool levelling pyramid (Sam Brothers, 2009)

(b) The five (5) rules of evidence namely: - **admissible, authentic, complete, reliable and believable** ensures that your digital evidence is useful in courtrooms. Expand on what **admissible, reliable** and **believable** features of evidence entail ***[6 Marks].***

(c) Besides the stated rules in **3 (b)**, which are some of the good forensic practices to apply to the collection and preservation of evidence to ensure that evidence will be accepted in court as being authentic and accurate? ***[4 Marks].***

Question 4

(a) Explain the concept of Jailbreaking in the context of IOS mobile devices ***[2 marks].***

(b) The first step in a forensic examination of an IOS device should be identifying the device model. Why is this important? ***[2 Marks].***

(c) Explain the function of the Linux Kernel on Android OS ***[4 marks].***

(d) What role does the Dalvik Virtual Machine play on an Android OS? ***[2 marks].***

*******End of Examination Paper*******