NAMIBIA UNIVERSITY
OF SCIENCE AND TECHNOLOGY

FACULTY OF COMPUTING AND INFORMATICS

DEPARTMENT OF CYBER SECURITY

QUALIFICATION : BACHELOR OF COMPUTER SCIENCE (HONOUR) IN DIGITAL FORENSICS	
QUALIFICATION CODE: 08BHDS	**LEVEL: 8**
COURSE: MOBILE AND CLOUD FORENSICS	**COURSE CODE: MCF811S**
DATE: JUNE 2024	**SESSION: 1 (THEORY)**
DURATION: 3 HOURS	**MARKS: 100**

FIRST OPPORTUNITY EXAMINATION QUESTION PAPER	
EXAMINER (S)	**MR. ISAAC NHAMU**
MODERATOR	**DR. NKOSINATHI MPOFU**

THIS EXAM 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.
4. When answering questions you should be guided by the allocation of marks in [ ]. Do not give too few or too many facts in your answers.

PERMISSIBLE MATERIALS

1. None.

Question 1

There is no well-established standard process for mobile forensics. However, Figure 1 below provides an overview of process considerations for the extraction of evidence from mobile devices.

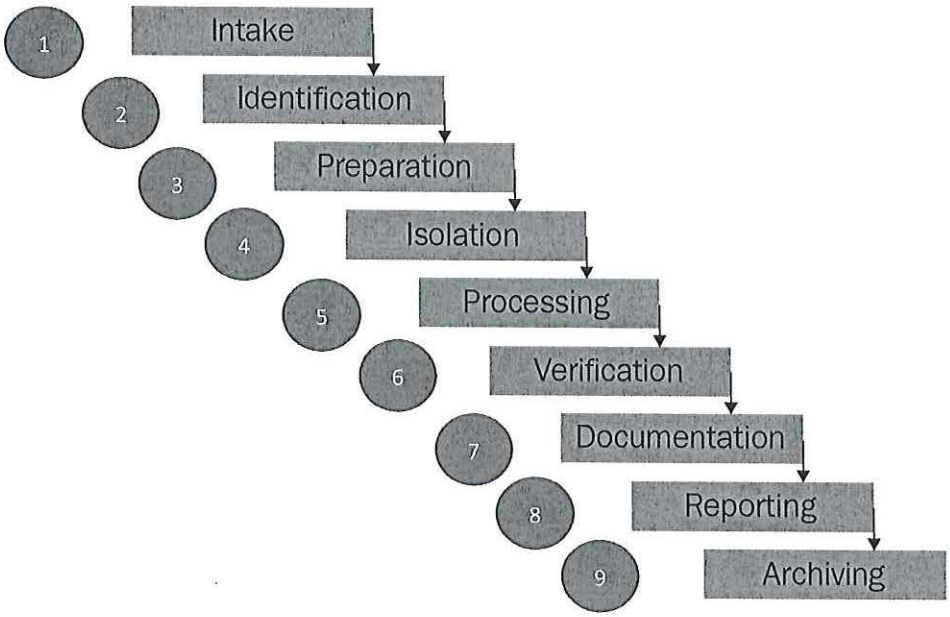

Figure 1: Mobile phone evidence extraction process

Explain what happens at steps/phase 1, 2, 3, 4 and 6. [10]

Question 2

a. List **five** digital forensics artifacts that can be retrieved from a mobile phone's SIM card. [5]

b. State any **five** challenges of acquiring evidence from the cloud. [5]

Question 3

Virtualization technology makes cloud computing possible. Cloud providers set up and maintain their own data centres. They create different virtual environments that use the underlying hardware resources. Figure 2 below shows Type 1 and Type 2 deployment of Hypervisors.

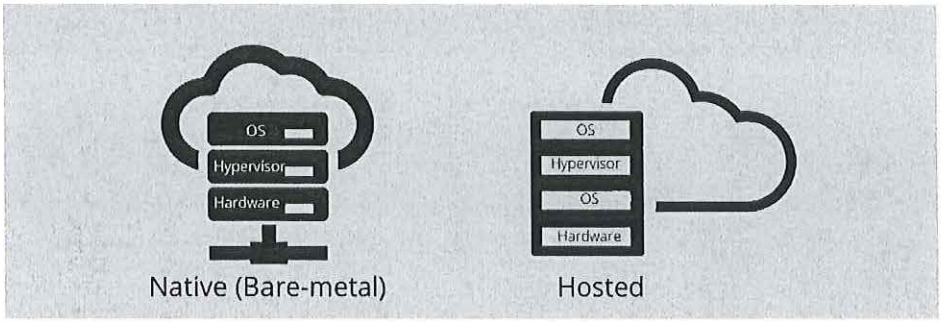

Figure 2: Type 1 (left) and Type 2 (right) Hypervisors

a. Describe the main difference between the two? [2]

b. Explain in detail, two advantages of acquiring evidence from a Type 1 over a Type 2 hypervisor system. [4]

c. Explain in detail, two advantages of acquiring evidence from a Type 2 over a Type 1 hypervisor system. [4]

Question 4

Before initiating a cloud investigation, you should review the SLA to identify restrictions that might limit the collection and analysing of data.

a. State **five** pieces of information that are normally included in an SLA for cloud customers. [5]

b. For each of the items stated in **a.** state how they could hinder or assist in mobile forensics. [5]

Question 5

Figure 3 below shows the security architecture diagram for iOS.

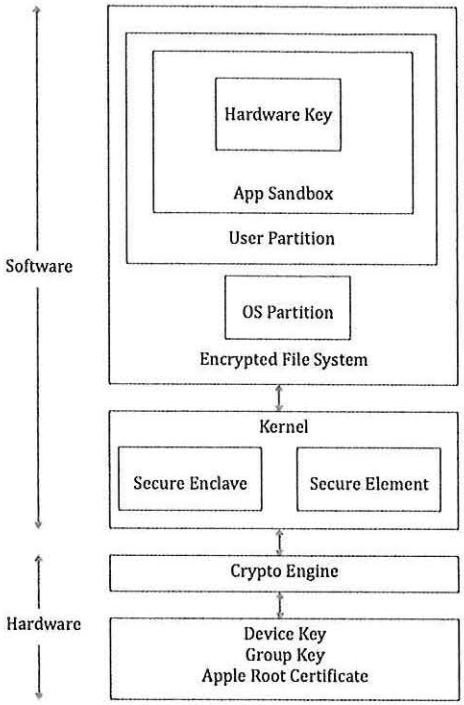

Figure 3: Security architecture diagram for iOS

a. What happens when you delete a file in an iOS device? [2]

b. With reference to iOS, what is sandboxing? [2]

c. Why is sandboxing important in digital forensics? [3]

d. What are some of the pitfalls of this technique in the context of digital forensics. Give two. [3]

Question 6

Describe the following methods of accessing a passcode protected phone and outline the risks each presents to the mobile forensics investigative process.

a. Jailbreaking

b. Rooting [10]

Question 7

The mobile industry in the world is divided between the three technologies **GSM, CDMA** and **iDen**. It is necessary for us to understand the basic differentiation of the three technologies as they may have an impact on the Forensic Investigative process.

i. Present the fundamental technical aspects of the three systems in your presentation describe briefly how each affects the mobile forensics investigative process. [15]

ii. Describe the **two** main challenges of 5G technologies on the mobile forensics investigative process. [5]

Question 8

While searching inside the house of a person under investigation, law enforcement agents found and seized, among other things, computers and a smartphone. After cataloguing and documenting everything, they put all the materials into boxes to bring them back to the laboratory. Once back in their laboratory, when acquiring the smart phone in order to proceed with the forensics analysis, they noticed that the smartphone was empty and it appeared to be brand new. The owner had wiped it remotely.

This therefore emphasises the importance of isolating the mobile device from all radio networks as a fundamental step in the process of preservation of evidence:

a. There are several ways to achieve this (isolating mobile phones), all with their own pros and cons. Outline five forensic methods of isolating mobile phone give at least one pro and one con of each. [15]

b. List any other **five** anti-forensics techniques that are used in an attempt to affect the mobile investigative process. [5]

<<<<<<<< END >>>>>>>>