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 2023	**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 5 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.

Section A (Structured Questions) [65 marks]

Question 1

The **mobile device forensics tool classification system** was created by Sam Brothers to give investigators an overview of available tools, from least complicated to most complex, for the purpose of gathering mobile evidence. The classification or levels are frequently illustrated as a triangle with five layers as in Figure 1.

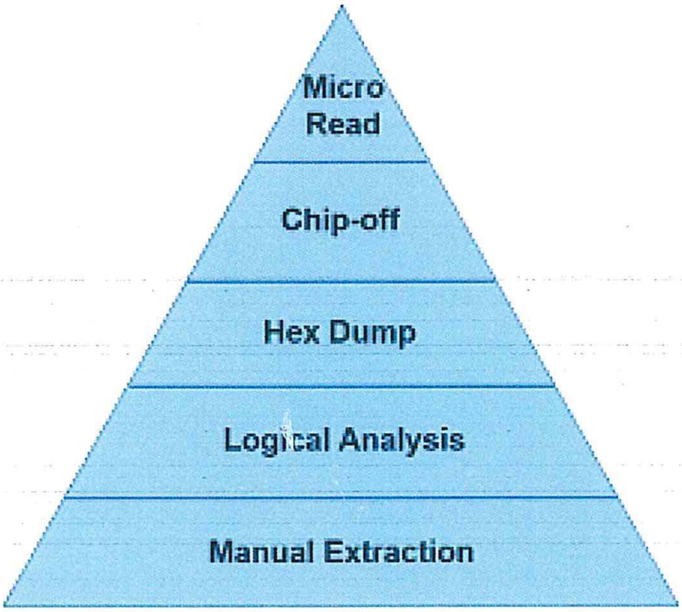

Figure 1: Sam Brothers tool levelling pyramid

Explain/describe a technique used to acquire digital evidence from a mobile device at each level, and give a scenario when each can be used. [10]

Question 2

a. Compare digital evidence to physical evidence. In your comparison, give at least three advantages of digital evidence over physical evidence and at least two advantages of physical evidence over digital evidence. [10]

a. List five digital forensics artifacts that can retrieved from a mobile phone. [5]

Question 3

a. What is cell site analysis? How is it useful to mobile forensics. [3]

b. Expand the abbreviations, GSM and CDMA. [1]

c. Outline two main differences that make digital forensic investigations unique for GSM phones and CDMA phones. [4]

d. Figure 2 shows the architecture of a GSM cellular network. Expand the abbreviations and state what information of forensic value can be obtained from:

   i. BTS

   ii. BSC

   iii. HLR

   iv. VLR

   v. EIR

   vi. AuC [12]

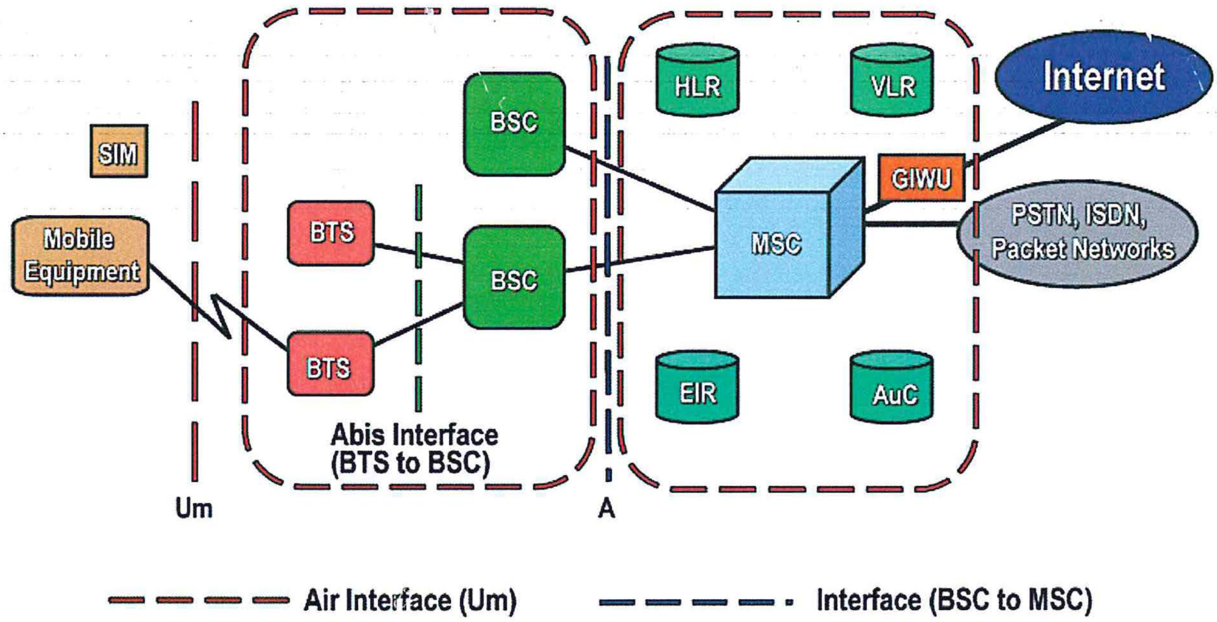

Figure 2: Architecture of a GSM mobile network

Question 4

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 3 below shows Type 1 and Type 2 deployment of Hypervisors.

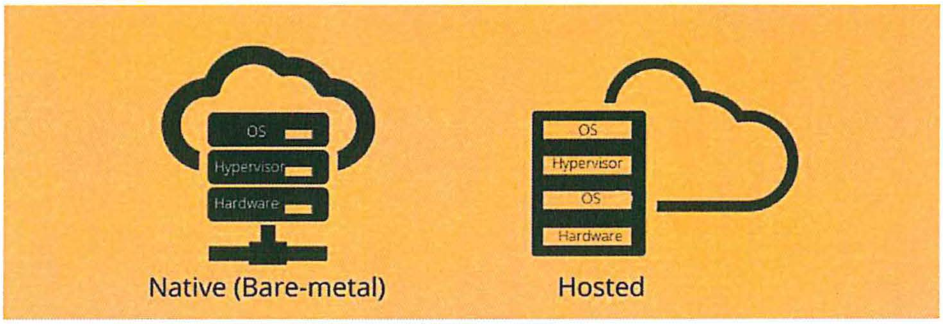

Figure 3: Type 1 (left) and Type 2 (right) Hypervisors

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 5

Figure 4 below shows the security architecture diagram for iOS.

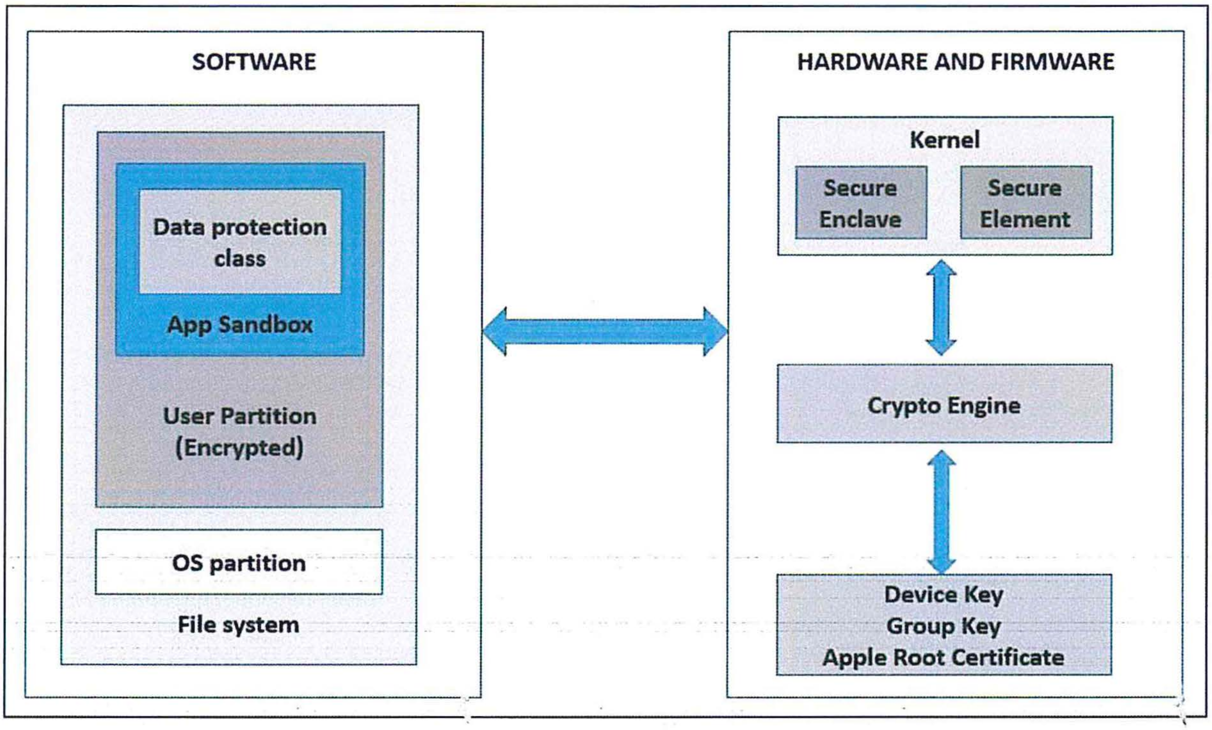

Figure 4: Security architecture diagram for iOS

a. What file system does iOS use? [1]

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

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

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

e. What are some of the pitfalls of this technique in the context of digital forensics. Give two. [2]

Section B (Scenarios and Practice) **[35 marks]**

Question 7

You are given that a crime was committed and in the commission of the crime an iOS device was recovered. Given the following different scenarios, state what action can be taken to preserve information on the device in each case:

a. Device turned on and unlocked,

b. Device turned on and locked,

c. Device turned off and without passcode,

d. Device turned off and with passcode. [20]

Question 8

Reverse Engineering is important in mobile forensics and might be the only way evidence on a phone may be accessible. However, it does affect the digital forensics investigative process.

a. Besides rooting and starting the device in recovery mode, explain three ways passcodes in Android phones can be circumvented. [6]

b. How can each of the methods you identified in a. be prevented. [3]

c. Rooting a phone is one way of circumventing passcodes,

i. Explain three ways of rooting an Android phone. [3]

ii. List three potential dangers of rooting a phone. [3]

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