NAMIBIA UNIVERSITY
OF SCIENCE AND TECHNOLOGY
Faculty OF COMPUTING AND INFORMATICS

Department OF Computer Science

QUALIFICATION: BACHELOR OF COMPUTER SCIENCE HONOURS (DIGITAL FORENSICS)	
QUALIFICATION CODE: 08BHDF	**LEVEL:** 8
COURSE: Digital Forensics Management	**COURSE CODE:** DFM811S
DATE: June 2019	**SESSION:** 1
DURATION: 3 hours	**MARKS:** 100

FIRST OPPORTUNITY EXAMINATION QUESTION PAPER	
EXAMINER(S)	**MR. ISAAC NHAMU**
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. 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. Non programmable Scientific Calculator.

Question 1

a. Explain the following types of data as used in digital forensics.
   a. Active data
   b. Ambient data
   c. Transient data
   d. Archival data
   e. Residual data
   f. Metadata [12]

b. Describe in detail how digital evidence differs from physical evidence. [8]

Question 2

a. Define the term digital economy and describe any two criminal opportunities that have been presented by the adoption of the digital economy in Namibia. [5]

b. What technical terms in digital forensics are used to describe A, B and C in Figure 1.1. [3]

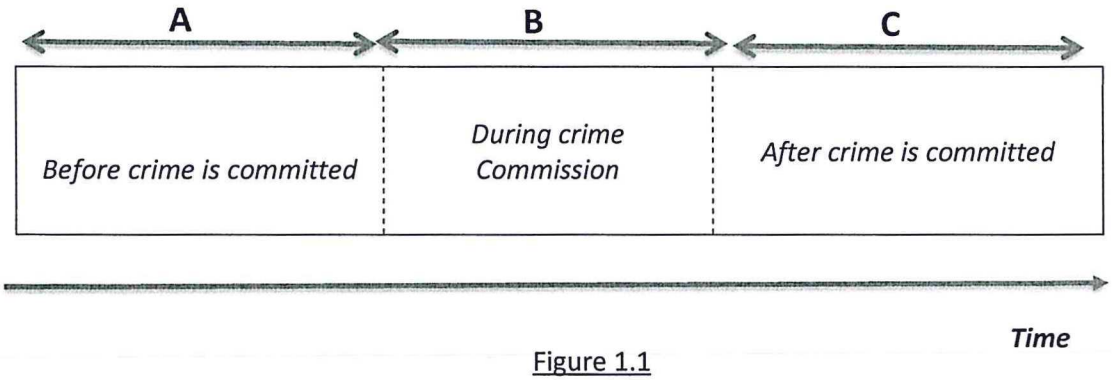

Figure 1.1

c. Describe two challenges that may be encountered at each of the stages A, B and C with respect to managing a digital forensics case. [12]

Question 3

a. State any two goals for a Digital Forensics Incident Response (DFIR) team. [2]

b. Describe the functions of any three named members of a DFIR team for a large corporate organization. [6]

c. Outline a six-step methodology for implementing DFIR in an organisation. [12]

Question 4

Pollitt (1984), proposed a methodology for dealing with digital evidence investigations called the Computer Forensics Investigative process. The process comprises of 4 distinct phases as shown in Figure 4.1 below.

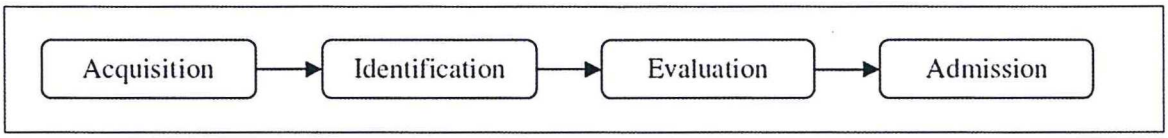

Figure 4.1

a. Describe what happens at each phase of the proposed methodology. [4]

b. Critique Pollitt's proposed methodology by mentioning its strengths and its shortcomings and how these would affect the investigation process. [10]

c. Propose a new methodology based on your critique in question 4b. that would address the concerns raised. [6]

Question 5

a. During the imaging process repeatability and reproducibility are important as standards for imaging tools. Differentiate between these two. [4]

b. What is the function of the Windows Registry? [2]

c. List 2 items of evidence that could be acquired from the Windows Registry. [2]

d. What would the following regedit queries display? [6]

i. `HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU`
ii. `HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU`
iii. `HKCU \Software\Microsoft\Search Assistant\ACMru`

e. State three methods that can be used to perform anti-forensics. [3]

f. How can the anti-forensics methods stated in e. be overcome? [3]

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