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: July 2022	**SESSION:** 2
DURATION: 3 hours	**MARKS:** 100

SECOND OPPORTUNITY/SUPPLEMENTARY EXAMINATION QUESTION PAPER	
EXAMINER(S)	**MR. ISAAC NHAMU**
MODERATOR:	**DR. AMELIA PHILLIPS**

THIS EXAM QUESTION PAPER CONSISTS OF 3 PAGES
(Excluding this front page)

INSTRUCTIONS

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. Non-programmable calculator.

Question 1

a. What are the four methods of preserving a crime scene? [4]

b. Discuss two issues on privacy that may affect digital forensic investigations. [6]

Question 2

Identify five advantages and five disadvantages of using Open-source tools during a digital forensics investigations. [10]

Question 3

Identify and discuss five challenges to the digital forensics investigation process that are specifically related to cloud computing. [10]

Question 4

Evidence integrity is essential in order for digital evidence to be admissible in court and to carry weight as evidence.

a. What is CoC (Chain of Custody) and why is it important for evidence integrity? [3]

b. What is OOV (order of volatility), and how does it influence decisions regarding which evidence should be preserved first? [2]

c. List various data storage media as a function of their OOV. [5]

Question 5

You are presented with a case where a suspect attempted to hide picture files about child pornography on his computer system. Your initial investigation points to the fact that the suspect hid the malicious picture files under an NTFS Windows system.

a. Draw a plan describing the steps you would take in carrying out this investigation. [10]

b. Describe the places where you would search for these files and describe how you would recover the files. [10]

Question 6

Justina (not her real name), an employee of PWD cc a local catering company is suspected of stealing the company's receipt; of preparing snack with a Namibian twist. It is suspected that she is communicating with an employee from a competing company via emails and instant messaging while at the company premises. You have been approached to investigate this case and you have been instructed to handle the investigation in a proper manner.

a. Detail how you would initiate the acquisition of evidence for the investigation. [4]

b. Draft a plan as to where and how you might get email evidence for this case. [10]

c. Detail how Agnes can cover up the trails of email and how you can still recover the emails if possible. [6]

Question 7

a. With regards to Digital Forensics Incident Response (DFIR), what is the meaning of the following terms:

   i. Event
   ii. Incident
   iii. Attribution
   iv. Artifact [4]

b. State any two goals for a DFIR team. [2]

c. You are given the two following methodologies for implementing DFIR in stages. Compare and contrast these methodologies by stating what happens at each stage or otherwise. [14]

DFIR Methodology #1	DFIR Methodology #2
Preparation	Preparation
Identification	Detection and Analysis
Containment	Containment, Eradication, and Recovery
Investigation	Post incident activity
Eradication	
Recovery	
Follow-up	

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