NAMIBIA UNIVERSITY
OF SCIENCE AND TECHNOLOGY

FACULTY OF COMPUTING AND INFORMATICS
DEPARTMENT OF CYBER SECURITY

QUALIFICATION : BACHELOR OF COMPUTER SCIENCE HONOURS (DIGITAL FORENSICS)	
QUALIFICATION CODE: 08BHDF	**LEVEL: 8**
COURSE: DIGITAL FORENSICS MANAGEMENT	**COURSE CODE: DFM811S**
DATE: JULY 2024	**PAPER: THEORY**
DURATION: 3HOURS	**MARKS: 100**

SECOND OPPORTUNITY/SUPPLEMENTARY EXAMINATION QUESTION PAPER	
EXAMINER(S)	**MR. JULIUS SILAA**
MODERATOR:	**PROF. AMELIA PHILLIPS**

THIS QUESTION PAPER CONSISTS OF 2 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.

PERMISSIBLE MATERIALS

1. Calculator.

Question 1

a) A banner is a piece of information displayed by a host that provides details about the service or system. List any two items that should appear on a warning banner. (4 marks)

b) A cyber forensic laboratory overall function is to identify, seize, acquire and analyze all electronic devices related to all cyber-enabled offences reported so as to collect digital evidence which is presented in a court of law for prosecution purposes.
Provide any 5 the mainstream key components of a cyber forensic lab. (5 marks)

Question 2

As part of the business planning for your forensic lab, you should determine which tools offer the most flexibility, reliability, and future expandability. List and briefly discuss what functions and subfunctions you think are necessary to determine which tools you should acquire for an investigation? (18 marks)

Question 3

a) After deleting a file from a FAT file system, what happens to the content of the file? (5 marks)

b) Pending an ongoing deformation of character investigation of Mr Cloete, a private forensic investigator has discovered that other than laptop and cell phones, NUST also provides an additional standard USB hard drive to each of their senior employees. The standard issued USB hard drive is not encrypted and the owners are responsible to protect the issued hard drive. NUST has not done an auditing on any of the issued hard drives, nor has it been keeping track of the issued hard drives on their corporate IT asset list. Nevertheless, based on NUST Information Security Policies, all senior employees are required to submit their hard drives to the IT department for back up at monthly basis. Describe what is the next course of action shall be taken by the investigator, and why. (15 marks)

Question 4

a) What volatile information which you will be collecting before switching off computer system? Also explain its role in digital forensic investigations. (5 marks)

b) Write short notes on evidence validation (3 marks)

c) Discuss the techniques of tracing an email message (5 marks)

Question 5

a) Briefly describe the main objective of meet and confer in e-Discovery. (5 marks)

b) Briefly discuss the relationship between volume and relevancy of ESI described in the EDRM. You may use a simple illustration (a complete EDRM is not necessary) to explain your answer. (5 marks)

Question 6

With virtual environments becoming more prevalent as an analysis tool in digital forensic investigations, it's becoming more important for digital forensic investigators to understand the limitation and strengths of virtual machines(VM).

Write short essay that provides a brief overview of digital forensic investigations and virtual environments. Your essay should among other things describe the fundamentals of a traditional forensic investigation and explain how virtualization affects this process. Finally, describe the common methods to find virtualization artifacts and identify virtual activities that affect the examination process. (30 marks)

*******END OF PAPER*******