(*University of Choice*)

MASINDE MULIRO UNIVERSITY OF SCIENCE AND TECHNOLOGY (MMUST)

MAIN CAMPUS

UNIVERSITY EXAMINATIONS
2023/2024 ACADEMIC YEAR
FOURTH YEAR EXAMINATIONS

FOR THE DEGREE

IN

COMPUTER SCIENCE

COURSE CODE: BCS 471

COURSE TITLE: COMPUTER FORENSICS

DATE: 07/12/2023 **TIME:** 3:00 – 5:00 PM

INSTRUCTIONS TO CANDIDATES

- Answer **Questions ONE** and **ANY OTHER TWO**.

TIME: 2 Hours

MMUST observes ZERO tolerance to examination cheating

This Paper Consists of 3 Printed Pages. Please Turn Over.

Question 1 COMPULSORY (30 MARKS)

a) The two types of computer crime investigations are computer-based crime and computer-facilitated crime. Briefly explain what they mean giving one example of each. **(8 marks)**

b) Many cyber incidents can be handled more efficiently and effectively if forensics considerations are incorporated into the information system life cycle. Name and explain and four such considerations. **(8 marks)**

c) Highlight and explain five examples of corporate computer crimes **(5 marks)**

d) Briefly explain the differences between them digital evidence and physical evidence **(4 marks)**

e) Explain what chain of custody means and why it is important to maintain chain of custody and how you would maintain it. **(5 marks)**

Question 2 (20 MARKS)

a) Name and explain any three types of data acquisition techniques that you know of highlighting cases in which they will be used **(10 marks)**

b) As a DF expert, explain which data acquisition technique you will use in each of the following cases highlighting your reasons for your choice:

- RAID configuration for servers
- Email investigation
- Lack of a password for logging in to the OS
- Bitlocker protected disks.
- Computer seized during police raid. **(10 marks)**

Question 3 (20 MARKS)

a) Discuss the differences between volatile and non-volatile data in the context of computer forensics. Provide examples of each. **(3 marks)**

b) A suspect's computer has been seized as part of a criminal investigation. You suspect that there could be some virtual machines running on the computer. Highlight any three ways you can use to confirm this. **(6 marks)**

c) Explain five major task categories a DFT (Digital Forensic Tool) is expected to perform. **(5 marks)**

d) A suspect's computer has been seized as part of a criminal investigation. You are tasked with preserving the integrity of evidence on the suspect's computer. Describe any three best practices you would use for this. **(6 marks)**

Question 4 (20 MARKS)

a) Headers contain useful information when conducting e-mail forensics. Describe any four items an email header will provide to you. **(4 marks)**

b) The university wants to setup a Digital Forensic Workstation. Highlight any four recommendations you would give them to set up a Digital Forensic Workstation. **(8 marks)**

c) You have been hired to conduct Network Forensics. Explain what Network Forensics is the main purpose of Network Forensics? **(4 marks)**

d) Briefly explain the difference between Digital Evidence First Responder (DEFR) and a Digital Evidence Specialist (DES). **(4 marks)**

Question 5 (20 MARKS)

a) In a case involving an employee suspected of data theft, outline the steps you would take to investigate and prove or disprove the allegations. Include details about the forensic tools and techniques you would use for each step. **(20 marks)**