(60

(*University of Choice*)

MASINDE MULIRO UNIVERSITY OF SCIENCE AND TECHNOLOGY (MMUST)

MAIN CAMPUS

UNIVERSITY EXAMINATIONS

2022/2023 ACADEMIC YEAR

SPECIAL/SUPPLIMENTARY EXAMS

FOURTH YEAR EXAMINATIONS

FOR THE DEGREE

IN

INFORMATION TECHNOLOGY

COURSE CODE: BIT 416E

COURSE TITLE: INFORMATION FORENSICS AND AUDITING

DATE: 13/12/2022 **TIME:** 03:00-05:00PM

INSTRUCTIONS TO CANDIDATES

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

TIME: 3 Hours

Question 1 COMPULSORY (30 MARKS)

a) Briefly define the term Digital Forensics. **(3 marks)**

b) List and explain five characteristics that you need to be a successful digital forensics practitioner **(5 marks)**

c) Explain the difference between a physical drive, a logical drive, an image file and a VM file when conducting forensics. **(8 marks)**

d) Briefly explain what BYOD is and why it is difficult to perform forensics with BYOD. **(6 marks)**

e) Briefly explain the difference between Digital Evidence First Responder (DEFR) and a Digital Evidence Specialist (DES). **(5 marks)**

f) Explain what hashing means and why it is important in forensic investigations **(3 marks)**

Question 2 (20 MARKS)

a) Define the following concepts with respect to data acquisition for conducting forensics explaining situations where each is applicable:

- Static acquisition
- Live acquisition
- Logical acquisition and/or sparse acquisition

(9 marks)

b) Explain the steps required to perform a live acquisition. **(6 marks)**

c) Describe why data acquisition from clouds is difficult to carry out **(3 marks)**

d) Describe why whole disk encryption like BitLocker makes static acquisitions more difficult. **(2 marks)**

Question 3 (20 MARKS)

a) Describe what a packet sniffer is and what it does. (6 marks)

b) Describe the working structure of a hard disk drive **(4 marks)**

c) Describe the working structure of an SSD and explain why it is difficult to recover deleted files from an SSD. **(6 marks)**

d) You are conducting forensics on a computer and suspect that there are VMs running. Name two areas you might you look to determine if a VM exists on a host computer.
(4 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) E-mail fraudsters use phishing, pharming, and spoofing scam techniques. Explain what these three terms mean. **(6 marks)**

c) Three data storage formats for digital evidence. Name and explain these three formats? **(6 marks)**

d) List four sorts of forensic evidence can be collected through social media **(4 marks)**

Question 5 (20 MARKS)

a) Outline two advantages and two disadvantages of using GUI forensic tools. **(4 marks)**

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

c) As a digital forensics investigator, name and explain 4 different file / file system attributes that you may be interested (8 marks)

d) Explain why it is important to maintain more that one copy of the digital evidence and why you should never perform forensics on the original seized evidence. **(3 marks)**