20

(The University of Choice)

MASINDE MULIRO UNIVERSITY OF SCIENCE AND TECHNOLOGY (MMUST)

MAIN CAMPUS

UNIVERSITY EXAMINATIONS

2021/2022 ACADEMIC YEAR

FOURTH YEAR SPECIAL/SUPPLEMENTARY EXAMINATIONS

FOR THE DEGREE
OF
BACHELOR OF SCIENCE IN COMPUTER SCIENCE

COURSE CODE: **BCS 473E**

COURSE TITLE: **COMPUTER FORENSICS**

DATE: TUESDAY 02-08-2022 **TIME:** 12:00NOON-4:00P.M

INSTRUCTIONS TO CANDIDATES

Answer questions ONE and any other TWO questions.

TIME: 2 Hours

MMUST observes ZERO tolerance to examination cheating

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

QUESTION ONE 30 MARKS (COMPULSORY)

a. Once the evidence is gathered, it can be used to reconstruct the crime to produce a clearer picture of the crime and identify the missing links in the picture. Identify and briefly explain the three fundamentals of reconstruction for investigating a crime. 6 Marks

b. Briefly explain why you think it is difficult or easy to reconstruct evidence for a network investigation. Justify your choice. 6 Marks

c. Explain the following terms as they apply in the field of forensics. 8 Marks

   i. Chain of custody

   ii. Encapsulation

   iii. Buffer overflow attack

   iv. DriveSpy

d. Identify FIVE different types of volatile and nonvolatile information an investigator can collect from a Windows system. 5 Marks

e. What are the strategies to secure Web applications? 5 Marks

QUESTION TWO 20 MARKS

a. Data can be hidden on the storage devices of the computer. To detect and recover such information that is hidden, data-hiding analysis contributes to revealing the knowledge, ownership, or intent contained therein. Briefly explain how an investigator would achieve Data-hiding analysis. 6 Marks

b. How would you investigate Web attacks in Windows-based servers? 5 Marks

c. Several registry values and settings could impact the follow-on forensic analysis and investigation. Identify any two registry values that can greatly affect an investigation and briefly explain how they can impact an investigation. 6 Marks

d. Describe the functions of the Cain and Abel tools. 3 Marks

QUESTION THREE 20 MARKS

a. In situations where an individual is suspected of using a certain computer, time-frame analysis can contribute to associating the events that occurred on the computer with that individual. Identify and briefly explain any two Time-frame analysis methods. 6 Marks

b. What are the necessary components of a search warrant? 4 Marks

c. Describe the importance of network forensics. 3 Marks

d. Briefly explain Defense in depth (DiD) strategy and its three modes of protection 7 Marks

QUESTION FOUR 20 MARKS

a. Explain standard procedures for performing a live acquisition 9 Marks

b. Describe primary concerns in conducting forensic examinations of virtual machines 5 Marks

c. Explain the term Enumeration and highlight its key components. 6 Marks

QUESTION FOUR 20 MARKS

a. Explain standard procedures for network forensics 5 Marks

b. Identify any FOUR DoS attack and briefly explain how each is executed 8 Marks

c. Describe how a system administrator in an organizational setup, would provide a first line of defense against DNS attack. 3 Marks

d. Explain how the sequential change-point detection technique is achieved and what it entails. 4 Marks