JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS

UNIVERSITY EXAMINATION FOR THE DEGREE OF BACHELOR SCIENCE IN SECURITY AND FORENICS

2nd YEAR 1st SEMESTER 2021/2022 ACADEMIC YEAR

MAIN CAMPUS

COURSE CODE: ICB 1201

COURSE TITLE: Computer Forensic 1

EXAM VENUE: STREAM: BSc Computer Forensics

DATE: August 2022 EXAM SESSION:

TIME: 2.00 HOURS

INSTRUCTIONS:

1. **Answer Question 1 (Compulsory) and ANY other TWO questions**
2. **Candidates are advised not to write on the question paper**
3. **Candidates must hand in their answer booklets to the invigilator while in the examination room**

Question 1

a) Explain the meaning of the term physical environment in forensic science? **(2 marks**)

b) Give two reasons why a Closed Circuit Television (CCTV) is important as a source of evidence in computer forensics.
(4 marks)

c) Explain how Privacy Analyzer in useful to a Computer Forensics expert?
(4 marks)

d) List three examples of computer forensic tools **(3 marks)**

e) Distinguish between digital evidence and physical evidence? **(3 marks)**

f) Provide an explanation why Evidence preservation is considered important in conducting computer forensic investigation. **(5 marks)**
g) State one major reasons why Computer Security Incidence Response Team (CSIRT) in an organization could be referred to as forensic team **(3 marks)**

h) List three aspects of an email that can be used to identify the sender. **(3 marks)**

i) "A browser history is very important to a computer forensics". Give one reason to support the statement. **(3 marks)**

Question 2

a) Distinguish between *Domain Name* and *IP addresses* **(4 marks)**

b) You have been provided with an IP address of a computer server that sent an email with a pornographic attachment.

Describe how that information can be used to trace the pornographer using one of the Forensic Tools **(16 marks)**

Question 3

a) Identify four specific areas in a computer where digital evidence can be obtained.
(4 marks)

b) An intruder has just broken into the university computer system and erased the files from the department of finance. As an expert you are now tasked with the responsibility of carrying out a forensic analysis to determine the identity of the culprit.

Briefly describe the nature of digital evidence related to the crime that you would be searching for. **(16 marks)**

Question 5

a) Distinguish between a computer forensic expert witness and a fact witness **(4 marks)**

b) Outline four key factors that are considered for a digital evidence to be *admissible* in a court of law **(16 marks)**

Question 4

a) Use Lockard's Principle to explain the statement, "Modification increases evidence authenticity." (10 marks)

b) Describe the two conditions that have to be fulfilled for digital evidence to be admissible in a Court of Law (10 marks)