JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS

DEPARTMENT OF COMPUTER SCIENCE AND SOFTWARE ENGINEERING

UNIVERSITY EXAMINATION FOR THE DEGREE OF

BACHELOR SCIENCE IN COMPUTER SECURITY AND FORENSICS

4ND YEAR 1ST SEMESTER 2024/2025 ACADEMIC YEAR

MAIN CAMPUS

COURSE CODE: IIT 1407

COURSE TITLE: CYBERCRIME INVESTIGATION

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**
4. **No mobile devices (e.g. laptops, phones. e.t.c.) are allowed into the Examination Room**

QUESTION ONE **[30 MARKS]**

a) Using appropriate examples, explain the following terms as used in cybercrime investigation: (10 Marks)

i) Expert Witness

ii) Authority of Seizure

iii) Chain of Custody

iv) E-evidence Admissibility

v) Unauthorized access

b) Discuss what do you understand by the term "*digital evidence*" (2 marks)

c) State THREE sources of digital evidence. (6 marks)

d) Explain the term *network probing* (4 marks)

e) Suggest TWO ways in which the *network scanning* can be used to counteract cybercrime. (6 marks)

f) Define the term *cyber stalking* as applied to cybercrime. (2 marks**)**

QUESTION TWO **[20 MARKS]**

a) Discuss the following attributes of evidence that cybercrime investigators must uphold for it to be admissible in a court of law. (10 Marks)

i) Authentic

ii) Accurate

iii) Whole

iv) Acceptable

v) Admissible

b) State TWO reasons why there is need for standard operating procedures during cybercrime investigations. (4 Marks)

c) Discuss the rules that a Cybercrime investigator must uphold during investigations. (6 Marks)

QUESTION THREE **[20 MARKS]**

a) Discuss any SIX examples of cybercrimes. (12 Marks)

b) Extensively discuss the rationale for maintaining a chain of custody during the Cybercrime investigation process. (4 Marks)

c) Cybercrime investigators perform general tests on the evidence after collection to determine authenticity and reliability of the evidence. Using relevant examples, discuss some of these tests. (4 Marks)

QUESTION FOUR **[20 MARKS]**

a) Discuss the rules that a cybercrime investigator must uphold during investigation. (10 Marks)

b) Discuss any five examples of cybercrimes. (10 Marks)

QUESTION FIVE **[20 MARKS]**

a) Computer forensics entails the preservation, identification, extraction, interpretation, and documentation of computer evidence. Using relevant examples, discuss these processes. (10 Marks)

b) Define the term cyber stalking as applied to cybercrime (2 marks)

c) With the help of relevant examples, provide a detailed explanation why "cyber stalking" is considered a crime under the Kenyan legal system. (8 marks)

This is the last printed page

- END -