



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

DATE:9/1/25

EXAM SESSION:9-11.00 AM

COURSE CODE: IIT 1407 TIME:2 HRS

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) Briefly explain what you understand by the following using suitable examples as applies to cybercrime investigation: (10 Marks)

Expert Witness

Authority of Seizure

Cyber crime

Forensic investigator

Forensic readiness

- b) What do you understand by the expression “digital evidence”? (2 marks)
- c) State three sources of digital evidence (6 marks)
- d) Define the term cyber stalking as applied to cybercrime (2 marks)
- e) Discuss the two types/modes of cybercrime attacks. (4 Marks)
- f) Discuss the rules that a cybercrime investigator must uphold during investigation.

(6 Marks)

QUESTION TWO

[20 MARKS]

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

a. Authentic

b. Accurate

c. Whole

d. Acceptable

e. Admissible

- b) Write down the three components of digital evidence that is admissible (4 Marks)
- c) Discuss the rules that a cybercrime investigator must uphold during investigation. (6 Marks)

QUESTION THREE

[20 MARKS]

- a) Discuss how log files and IP addresses can be used to track the unauthorized computer user (12 Marks)
- b) Maintaining a chain of custody is critical in cybercrime investigation process. Discuss. (4 Marks)
- c) Cybercrime investigators perform general tests on the evidence after collection to determine authenticity and reliability of the evidence. Discuss (4 Marks)

QUESTION FOUR

[20 MARKS]

- a) Define the term hacking (2 marks)
- b) Discuss how cybercrime relates to hacking (10 marks)
- c) Explain the meaning of the term “hate speech” (4 marks)
- d) Log file provide records of events taking place in an operating system. Provide four types of log files that you know. (4 marks)

QUESTION FIVE

[20 MARKS]

- a) What do you understand by the expression “digital evidence”? (2 marks)
- b) With the help of examples provide a detailed explanation why “cyber stalking” is considered a crime under the Kenyan legal system (8 marks)
- c) An incident happened years ago where Dr. Lubanga Moeba, a KEMRI researcher, was suspected of mailing anthrax-contaminated letters causing ten deaths and injury to dozens of more people. It is said that Dr. Moeba used disposable e-mail accounts with false names during the time of the anthrax attacks. Although Dr Moeba eventually died in a road accident before being charged, he was the primary suspect in these anthrax attacks. Before he died, a case was in a court after the bereaved families sought legal redress with a view of claiming compensations. Consider yourself having been engaged as an expert to assist in this case. Explain in details how you would conduct your investigation and effectively assist the jury in solving this case. (8 Marks)
- d) State two reasons why there is need for standard operating procedures for investigation of cybercrime. (2 Marks)

This is the last printed page

- END -