JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS

UNIVERSITY EXAMINATION FOR THE DEGREE OF BACHELOR OF INFORMATION TECHNOLOGY

2ND YEAR 2ND SEMESTER 2023/2024 ACADEMIC YEAR

MAIN CAMPUS

COURSE CODE: ICB 1208

COURSE TITLE: CRIMINALISTICS AND FORENSIC LABS

DATE: 17/4/2025 EXAM SESSION:15.00-17.00 VENUE: CL: 3

TIME: 2 HOURS

Instructions:

1. Answer Question ONE and ANY other TWO questions.
2. Answers to Questions must be written in the spaces provided on the question paper.

QUESTION ONE (30 MARKS)

a) What is the difference between:
   i. forensic science and criminalistics? (2 marks)
   ii. Forensic pathology and Forensic anthropology (2 marks)

b) The services that a forensic science laboratory offers vary, depending on some factors. List any two of these factors. (2 marks)

c) What are the three types of explanation as the causes of criminal behavior? (3 marks)

d) What are the duties of a first responder at a crime scene? (2 marks)

e) List three common types of digital crime (3 marks)

f) What is meant by 'physical evidence' and why is it referred to as the 'silent witness' of a criminal act? (2 marks)

g) State any three methods of crime-scene recording. (3 marks)

h) What is the difference between private and public Forensic Science Laboratories? (2 marks)

i) What usually happens to a computer file once it is deleted by a user? (2 marks)

j) h) List the main functions of the forensic scientist. (2 marks)

k) define 'latent evidence'. In which areas would a computer forensic investigator look for latent data? (3 marks)

l) What is meant by 'Locard's exchange principle'? give any one instance of the occurrence of this principle (2 marks)

QUESTION TWO (20 MARKS)

a) What information must be included in any notes taken at the crime scene? (2 marks)

b) What is the first critical step in crime-scene investigation and why is it so important? (2 marks)

c) "The chain of custody is the backbone of forensic credibility." Discuss this statement in the context of physical and digital evidence, highlighting challenges in maintaining it across both domains. (8 marks)

d) explain any two types of forensic analysis (4 marks)

e) Scenario: A murder suspect's smartphone is recovered from a river. The device is water-damaged, and the forensic analyst attempts to power it on without proper drying or documentation.

   i. Which forensic principle was violated? Explain why. (2 marks)
   ii. Recommend a process to recover data while maintaining evidence integrity. (2 marks)

QUESTION THREE (20 MARKS)

a) Critically assess the challenges of maintaining evidence integrity in cloud-based environments. (6 marks)

b) How can forensic analysts ensure compliance with legal standards when acquiring data from third-party providers? (4 Marks)

c) a) Reports are to communicate the results of computer forensic investigations. Explain what a formal report is and where it would be presented (5 Marks)

b) When cases go for trial, you as the forensics expert can either be a technical witness or an expert witness. With examples, explain the two roles. (5 Marks)

QUESTION FOUR (20 MARKS)

a. What is Digital Forensics? (2 marks)

b. Describe the difference between live acquisition and static acquisition of digital evidence. (2 marks)

c. Explain the forensic process for analyzing a water-damaged laptop suspected of containing financial fraud data. Include steps for preservation, acquisition, and analysis while adhering to forensic best practices. (10 marks)

d. List three methods to preserve the integrity of digital evidence during acquisition. (3marks)

e. Give an example of each of the following digital forensics investigation cases.

i. Criminal case

ii. Corporate case

iii. Civil case (3 marks)

QUESTION FIVE (20 MARKS)

a) i. Distinguish between Bitmap and Vector images by stating two properties of each of these image types. (4 marks)

ii. What is a Raw File Format? (1 mark)

b) According to the practice guide for computer based electronic evidence, explain what are the four principles of computer based evidence (8 Marks)

c) Explain the following terms (7 Marks)

i) Cracker ii) CACHE iii) MD5 Hash iv) Slack space v) Trojan Horse vi) Imaging vii) Dongle