3

(Knowledge for Development)

KIBABII UNIVERSITY
(KIBU)

UNIVERSITY EXAMINATIONS

2021/2022 ACADEMIC YEAR

END OF SEMESTER EXAMINATIONS
YEAR FOUR SEMESTER TWO EXAMINATIONS

FOR THE DEGREE OF
(COMPUTER SCIENCE)

COURSE CODE: **CSC 458E**

COURSE TITLE: COMPUTER FORENSICS

DATE: 20 ~~5~~/08 ~~09~~/2022 **TIME:** 2.00 P.M - 4.00 P.M

INSTRUCTIONS TO CANDIDATES:

ANSWER QUESTIONS ONE AND ANY OTHER TWO.

QUESTION ONE (COMPULSORY) [30 MARKS]

a) Define the following: **[7 marks]**

i) Digital forensic

ii) Swap space

iii) Computer crime

iv) Computer forensic

v) Cyber security

vi) Malicious code

vii) Digital evidence

b) Outline the functions of a forensic specialist. **[7 marks]**

c) Differentiate between traditional forensic and computer forensic. **[2 marks]**

d) State and briefly explain any five computer crimes and misuses. **[10 marks]**

e) Briefly explain how computer forensics is supporting the groups named below.

i) Criminals **[2 marks]**

ii) Governments **[2 marks]**

QUESTION TWO [20 MARKS]

a) State the goals of Incident Response. **[8 marks]**

b) A computer crime happened in an organization two months ago. The management have engaged the services of a computer forensic expert in order to un lock the mystery.

i) What will be the prime goal of the forensic team in this case? **[2 marks]**

iii) State and briefly explain the phases the experts will go through to recover the evidence. **[6 marks]**

c) Explain the benefits of computer forensics on the following user groups. **[4 marks]**

i) Criminal prosecutors

ii) Civil litigation

iii) Insurance companies

iv) Law enforcement

QUESTION THREE [20 MARKS]

a) Outline any twelve qualities of good computer evidence. **[12 marks]**

b) Computer forensic analysis is not done directly on the suspect's computer but on a copy instead.

   i) State how this is done and explain why it is done. **[2 marks]**

   ii) Explain the precaution undertaken before copying data on the hard drive **[2 marks]**

   iii) Why must the hard drive be copied bit by bit (bit – stream backup)? **[2 marks]**

   iv) Name the commonly used tools for imaging of hard drives. **[2 marks]**

QUESTION FOUR [20 MARKS]

a) Outline any ten steps followed in performing computer forensic analysis in an attempt to find evidence. **[10 marks]**

b) An employee at Embu Agro Chemical Company claims that she is being harassed and discriminated by his senior, a fact that he is denying.
Outline the three evidentiary evidence that the investigator may look for during this exercise. **[3 marks]**

c) Data preservation is very critical in computer forensics. How can this be achieved for data collected to valid and acceptable for admissibility? **[2 marks]**

d) MAC times are used as prove that a suspect had knowledge of files and its contents under investigation. What important information are contained in this kind of forensic audit and how is it helpful to the investigator. **[4 marks]**

e) What could be the use of such evidence in the court of law? **[1 mark]**

QUESTION FIVE [20 MARKS]

a) List the network file system (NTFS) analysis tools used in computer forensic. **[4 marks]**

b) A television's station's web-site was hacked by two teenagers who gained access to the web-site by accident with "hacker slogans"

   i) Outline the lessons that the management learnt after the hacking. **[5 marks]**

ii) What preventive measures should the television station put in place to avoid a similar occurrence? **[4marks]**

iii) Outline with examples, how to manage the incident successfully. **[7 marks]**