University Examinations 2023/2024

FOURTH YEAR SECOND SEMESTER EXAMINATION FOR THE DEGREE OF
BACHELOR OF COMPUTER SECURITY AND FORENSICS

CCF 3456: COMPUTER CRIME AND DIGITAL EVIDENCE

DATE: APRIL 2024   **TIME: 2 HOURS**

INSTRUCTIONS: *Answer question **one** and any other **two** questions*

QUESTION ONE (30 MARKS)

a) State any five rules of digital evidence that can be used in computer crime adjudication

(5 Marks)

b) Explain the following terms in relation for computer crime investigation   (5 Marks)

    i.   Affidavit

    ii.   Plain view doctrine

    iii.   Search warrant

    iv.   Chain of custody

    v.   Cyclic Redundancy Check

c) List three data hiding techniques that investigators may encounter during digital evidence
analysis   (3 Marks)

d) Distinguish between Computer Crime and Digital Evidence   (2 Marks)

e) Describe the general guidelines for writing investigation reports after a computer crime investigation process (5 Marks)

f) Outline five tools in an initial response field kit used by computer crime investigators (5 Marks)

g) Describe what is intellectual property and state four ways that can be used to protecting against issues relating to Infringement of Intellectual Property rights (5 Marks)

QUESTION TWO (20 MARKS)

a) Discuss the ethical considerations and challenges associated with the use of digital evidence in investigations (6 Marks)

b) Law enforcement officer may search for and seize criminal evidence only with probable cause. Using an example briefly explain what is meant by probable cause in relation to computer crime investigations (4 Marks)

c) Describe the overall computer crime investigation process by citing the key steps that are involved in conducting a successful investigation (6 Marks)

d) State any four characteristics of digital evidence (4 Marks)

QUESTION THREE (20 MARKS)

a) Highlight the standard details captured in digital evidence collection form (5 Marks)

b) Discuss any three types of cybercrimes that can be exploited by cyber criminals (6 Marks)

c) In the protection of computer crime the companies should ensure three of the security measures are put in place. State and briefly explain these three main measures (6 Marks)

d) Briefly describe the role of metadata in digital evidence analysis (3 Marks)

QUESTION FOUR (20 MARKS)

a) Discuss any four tools and techniques used to commit computer crime (8 Marks)

b) Describe three principles that investigators should adhere to when handling digital evidence (6 Marks)

c) Outline the process of collecting digital evidence   (6 Marks)

QUESTION FIVE (20 MARKS)

a) Computer crime investigation is conducted following step by step procedures and involving various investigation tools and techniques. Discuss three barriers in computer crime investigation   (6 Marks)

b) When collecting digital evidence from a live computer one needs to perform some basic activities in order to handle a running computer. Describe any of these five activities of handling a running computer   (5 Marks)

c) In cases of a computer crime the forensic team must collect evidences. State four source of digital evidences   (4 Marks)

d) Describe who is a technical advisor in the computer crime investigation process and outline any four responsibilities of a technical advisor   (5 Marks)