MERU UNIVERSITY OF SCIENCE AND TECHNOLOGY
P.O. Box 972-60200 – Meru-Kenya
Tel: +254(0) 799 529 958, +254(0) 799 529 959, + 254 (0) 712 524 293,
Website: info@must.ac.ke Email: info@must.ac.ke

University Examinations 2023/2024

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

CCF 3353: COMPUTER FORENSIC AND SECURITY II

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

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

QUESTION ONE (30 MARKS)

a) List any three tools used in capturing digital evidence in a computer forensic lab (3 Marks)

b) Describe the purpose of a write block protection devices (3 Marks)

c) Identify four essential team members that you would need to build a forensic unit (4 Marks)

d) Explain the meaning of slack space and how it conceals digital evidence (5 Marks)

e) Describe the following terms as used in computer forensics (5 Marks)

i. Protocol Analyzer
ii. Digital evidence
iii. File slack
iv. Computer Forensics
v. Chain of custody

f) State and briefly explain the role of major components of a computer network in the context of forensic investigations (4 Marks)

g) dd is a tool that can be used for memory acquisition during live forensics. How do we use dd to dump the memory and what are the problems we face with this technique. (6 Marks)

QUESTION TWO (20 MARKS)

a) Describe any five of the constraints and dangers of live forensics (5 Marks)

b) Outline the legal and ethical considerations related to obtaining search warrants for network centers during forensic investigations process (4 Marks)

c) Discuss the following forensic tools (8 Marks)

   i. SANS SIFT

   ii. ProDiscover Basic

d) Describe the type of evidence that investigators normally try to find from e-mail logs (3 Marks)

QUESTION THREE (20 MARKS)

a) Outline the general guidelines that should be followed in the process of seizing evidence (7 Marks)

b) Discuss the main characteristics that differentiate public investigation and private investigation (6 Marks)

c) Describe the role of a computer forensic investigator (3 Marks)

d) Explain the following computer forensics technology (4 Marks)

   i. Remote monitoring of target computers

   ii. Theft recovery software for laptops and PCs.

QUESTION FOUR (20 MARKS)

a) You have been assigned the task of recovering information hidden in a word document with encrypted password by a suspect. Describe how you go about the exercise of accessing the information in the document (6 Marks)

b) Explain three general cryptanalysis techniques used to recover encrypted data (6 Marks)

c) Discuss the following forensic tools (8 Marks)

   i. Xplico

   ii. Oxygen forensic suite

QUESTION FIVE (20 MARKS)

a) Imagine that you compose a Word document and save it on your laptop with the filename Practical.doc. The process of saving a file on your hard disk involves three basic events. However, when you decide to delete Practical.doc, only two events happen. Considering the above statement, Required:

   i. Discuss the processes involved in storing a file in a hard disk drive and deleting it from the hard disk (6 Marks)

   ii. Explain also why deleting the file may not prevent forensic experts from getting the file (4 Marks)

b) Outline four types of non-volatile memory information that a computer forensic investigator might collect (4 Marks)

c) Explain two types of write blockers (6 Marks)