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 2024/2025

FOURTH YEAR FIRST SEMESTER FOR THE DEGREE OF BACHELOR OF SCIENCE IN COMPUTER SECURITY AND FORENSICS

CCF 3406: DIGITAL FORENSICS ANALYSIS AND INVESTIGATION TECHNIQUES

DATE: JANUARY 2025 **TIME: 2 HOURS**

INSTRUCTIONS: *Answer question **ONE** (Compulsory) and any other **TWO** questions*

QUESTION ONE (30 MARKS)

a) Explain the historical development of digital forensics and its relevance to modern investigations. (5 marks)

b) Discuss the role of certifications in building a business case for a digital forensics lab. (5 marks)

c) Describe the key steps involved in acquiring data from RAID systems. (5 marks)

d) Outline the procedures for seizing digital evidence at a crime scene. (3 marks)

e) Explain how file systems handle deleted and slack space during forensic analysis. (3 marks)

f) Discuss the strengths and weaknesses of current digital forensics hardware tools. (4 marks)

g) Explain the role of virtual machine forensics in investigating network-based crimes. (5 marks)

QUESTION TWO (20 MARKS)

a) Describe how to use hashing techniques to verify the integrity of collected digital evidence. (5 marks)

b) Explain the challenges involved in acquiring data from mobile devices in forensics investigations. (5 marks)

c) Discuss the role of cloud forensics in the modern investigative environment. (5 marks)

d) Evaluate the importance of report writing in high-tech digital forensic investigations. (5 marks)

QUESTION THREE (20 MARKS)

a) What are the legal and technical challenges of conducting forensics on social media platforms? (5 marks)

b) Explain the relevance of understanding file systems in Linux-based forensic investigations. (5 marks)

c) Discuss the importance of ethics for digital forensic expert witnesses in court proceedings. (5 marks)

d) Describe the process of recovering compressed graphic files and the challenges associated with it. (5 marks)

QUESTION FOUR (20 MARKS)

a) Explain the concept of live acquisition in network forensics and its importance. (5 marks)

b) Discuss the use of e-mail forensics tools to investigate e-mail-based crimes. (5 marks)

c) Describe the role of virtual machines in digital forensics investigations. (5 marks)

d) What are the challenges of conducting digital forensic investigations on encrypted devices? (5 marks)

QUESTION FIVE (20 MARKS)

a) Explain the role of data-hiding techniques in cybercrime and how forensics experts uncover hidden data. (5 marks)

b) Discuss the importance of understanding the file system structure in Macintosh-based forensic investigations. (5 marks)

c) What are the key factors to consider when acquiring evidence from Internet of Anything (IoT) devices? (5 marks)

d) Explain the importance of preparing a thorough curriculum vitae (CV) as a digital forensics expert witness. (5 marks)