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

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

CCF 3457: NETWORK FORENSICS INVESTIGATION TECHNIQUES

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

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

QUESTION ONE (30 MARKS)

a) Explain the role of a network forensic investigator and outline four tasks (4 Marks)
b) Describe the steps within the network forensic investigation methodology (4 Marks)
c) Discuss four common criminalities within mobile networks (4 Marks)
d) List four tools which network forensic investigators use for inspecting traffic (4 Marks)
e) If you strip a live Ethernet cable and attach an oscilloscope, illustrate the expected voltage patterns and explain the encoding standard used (4 Marks)
f) Explain the header information within an Ethernet frame and explain each filed using a diagram (4 Marks)
g) Distinguish between network surveillance verses network accountability (4 Marks)
h) What is file carving (2 Marks)

QUESTION TWO (20 Marks)

a) Using a diagram, explain the nature of addressing information processed during frame forwarding (4 Marks)

b) Distinguish between physical addresses verses logical address and explain how they can be used in an investigation (4 Marks)

c) After conducting a packet analyst using Wireshark, explain four indicators which can determine the presence of malicious code activities (4 Marks)

d) Identify and explain any four fields which are analyzed from a p-cap using Wireshark (4 Marks)

e) Distinguish between connection oriented verses connectionless protocols (4 Marks)

QUESTION THREE (20 MARKS)

a) Explain the outcome of applying the following packet analysis filters (4 Marks)

   i. tcp.port eq 25 or icmp

   ii. ip.src==192.168.0.0/16 and ip.dst==192.168.0.0/16

b) Distinguish between point-to-point verses broadcast networks and give an example of each (4 Marks)

c) List four network security threats and recommend solutions (4 Marks)

d) Describe the hardware and software necessary for a CCTV installation with intrusion detection and surveillance features (4 Marks)

e) Discuss two signal modulation techniques (4 Marks)

QUESTION FOUR (20 MARKS)

a) Illustrate the distinguishing between IPv4 verses IPv6 headers (4 Marks)

b) Distinguish between locally defined mac addresses verses OUI (4 Marks)

c) Discuss the techniques used in the protection of intellectual properties for multimedia content (4 Marks)

d) Explain how fingerprint multicast transmission works (4 Marks)

e) What is cyber attribution? (4 Marks)

QUESTION FIVE (20 MARKS)

a) Describe the trackback mechanism within ip based networks (4 Marks)

b) Discuss the ethical considerations when giving court testimony (4 Marks)

c) What is steganography? (4 Marks)

d) Explain the metadata within a jpeg file (4 Marks)

e) Illustrate the components of a cellular network and explain how they achieve data transmission (4 Marks)