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

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

CCF 3300: COMPUTER FORENSICS AND SECURITY I

DATE: DECEMBER 2024 **TIME: 2 HOURS**

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

QUESTION ONE (30 MARKS)

a) Discuss the two compelling arguments for encrypting your traffic when sending files from a target system (4 Marks)

b) Explain which volatile data to collect prior to forensic duplication (4 Marks)

c) Give the hardware and software tools needed for a forensics workstation (5 Marks)

d) Name four methods for hiding data on a hard drive, using the layers below the information classification layer only. How would you, as an examiner, detect these conditions? (4 Marks)

e) Outline the legal issues involved in seizure of computer equipment (4 Marks)

f) When reporting security breaches to law enforcement, identify the various categories of crimes which a forensic examiner would deal with (5 Marks)

g) Explain why it is helpful to know which services listen on which specific ports. (4 Marks)

QUESTION TWO (20 MARKS)

a) During the presidential debate in the run up to the 2016 US election, one of the candidates was accused of contravening government computer security polices and also breaking federal laws by transmitting personal emails over office email. Discuss the concept of Privileged communication and confidentiality as relates to this debate. (4 Marks)

b) In order to protect the integrity of the files you retrieve during the response; what steps should a forensic investigator take (4 Marks)

c) Discuss steps involved within the Computer Forensic Methodology (4 Marks)

d) Discuss the exploits of Kevin Mitnic and Robert Moriss (4 Marks)

e) Explain 4 qualities expected of a professional forensics examiner (4 Marks)

QUESTION THREE (20 MARKS)

a) With examples, give the difference between incident response and computer forensics. (4 Marks)

b) Your boss asks you to monitor a co-worker's email. What are factors which will influence your answer? (4 Marks)

c) When interviewing a source of information (witness) for an incident;

   i. Should you listen to his whole story first before taking any notes, or should you scribble down every remark when you first hear it? (4 Marks)

   ii. How does your interview of a manager differ from discussing incidents with a system administrator? (4 Marks)

d) What considerations wold you make when choosing a storage device for your forensic tools? (4 Marks)

QUESTION FOUR (20 MARKS)

a) Explain why is it unnecessary to obtain application logs during live response (4 Marks)

b) Outline reasons why remotely viewing event logs not considered a sound practice (4 Marks)

c) During initial response lsof and netstat are important tools which are very similar. In which cases would one apply each of these tools exclusively? (4 Marks)

d) Explain the techniques for risk-related modelling and calculations. (4 Marks)

e) Explain some of the benefits of having an organized incident response program (4 Marks)

QUESTION FIVE (20 MARKS)

a) Give a four scientific breakthroughs in the evolution of forensics in general (4 Marks)

b) Differentiate between the following terms: (6 Marks)

i. Computer forensics and data recovery

ii. Computer forensics and computer security

iii. Computer forensics and network forensics

c) give 3 security risk categories within a corporate network. (3 Marks)

d) During your initial response, discuss four options when retrieving information from a live system. (4 Marks)

e) Discuss the 3As of Computer Forensic Methodology (3 Marks)