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: www.must.ac.ke Email: info@mucst.ac.ke

University Examinations 2018/2019

THIRD YEAR SPECIAL/SUPPLEMENTARY EXAMINATIONS FOR DEGREE OF BACHELOR OF SCIENCE

CCF 3300: COMPUTER FORENSICS AND SECURITY I

DATE: SEPTEMBER 2019 **TIME: 2 HOURS**

INSTRUCTIONS: Answer Question ONE and any other TWO questions.

QUESTION ONE (30 MARKS)

a) Describe the role of a computer forensic investigator. (3marks)

b) List and explain any three tools used in capturing digital evidence. (3marks)

c) Explain the necessary steps undertaken when investigating cyber crime. (3marks)

d) Distinguish between the following terms:

i. Computer forensics Vs incidence response (4marks)

ii. Live data forensics Vs Network forensics (4marks)

e) Discuss the motivations behind cyber crime and give five examples (4marks)

f) Give a brief history of computer forensics and its importance in modern organizations. (3 marks)

g) Computer forensics is more of an "art" than "science". Support or discredit this notion with examples or scenarios. (3 marks)

h) Elaborate on the three tees which make up cyber security (3 marks)

QUESTION TWO (20 MARKS)

a) "The internet never forgets", give examples of forensic cases where this phrase can be applied. (4 marks)

b) Digital evidence can at times be inculpatory or exculpatory in some cases. Explain and give examples of such cases. (4 marks)

c) Define the term Computer forensics and distinguish it from the following disciplines:

i. Networks forensics (3 marks)

ii. Data Recovery (3 marks)

iii. Computer Security (3marks)

d) 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 aspects of Privileged communication and confidentiality as relates to this debate

(3 marks)

QUESTION THREE (20 MARKS)

a) Explain the various stages of forensic investigation when tracking computer crime

(4Mks)

b) Outline the necessary skills required by a forensics examiner (4Mks)

c) Use scenarios to elaborate on the "3 As" of computer forensic methodologies.

(4Mks)

d) Discuss the approaches used to formulate cyber laws. (4Mks)

e) Sometimes a computer security policy may not necessarily translate to a public law and sometimes it may. Identify possible scenarios when such happens. (4Mks)

QUESTION FOUR (20 MARKS)

a) Distinguish between an IDE and a SCSI hard drive. (4Mks)

b) You have booted up your forensic workstation and a SCSI hard drive connected to the external chain is not detected. How would you resolve this? (4Mks)

c) From the description of the file system layers, what would be the process for identifying unallocated space on a drive? (4Mks)

d) How would you identify slack space (RAM and file slack)? (4Mks)

e) 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? (4Mks)

QUESTION FIVE (20 MARKS)

a) You arrive at work a few minutes early one day. As you walk past a few of the open employee cubicles, you notice several of the IT staff viewing inappropriate images on their monitors. You also notice that an employee seems offended and upset about it.

(i) Identify the laws which forbid such acts (4Mks)

(ii) Explain how evidence can be capture in such an incident (4Mks)

b) What considerations would you make when choosing a storage device for your forensic tools ? (4Mks)

c) In order to determine if executable files are associated with listening ports, what solution would you apply ? (4Mks)

d) Why is it unnecessary to obtain application logs during live data forensics ? (4Mks)