

**MERU UNIVERSITY OF SCIENCE AND TECHNOLOGY**

**P.O. Box 972-60200 – Meru-Kenya**

**Tel: 020-2069349, 061-2309217. 064-30320 Cell phone: +254 712524293, +254 789151411**

**Fax: 064-30321**

**Website:** [**www.must.ac.ke**](http://www.must.ac.ke) **Email:** [**info@must.ac.ke**](mailto:info@must.ac.ke)

**University Examinations 2016/2017**

THIRD YEAR FIRST SEMESTER EXAMINATION FOR THE DEGREE OF

BACHELOR OF SCIENCE IN COMPUTER SCIENCE AND FORENSICS

**CCF 3300: COMPUTER FORENSICS I**

**DATE: DECEMBER 2016 TIME: 2 HOURS**

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

**QUESTION ONE (30 MARKS)**

1. Define the term Computer Forensics and distinguish it from the following disciplines:
2. Networks forensics (2 marks)
3. Data Recovery (2 marks)
4. Computer Security (2 marks)
5. Digital evidence can at times be inculpatory or exculpatory in some cases. Explain and give examples of such cases (4 marks)
6. Give a brief history of computer forensics and justify its importance in modern organizations (3 marks)
7. Computer forensics is more of an “art” than “science”. Support or discredit this notion with examples or scenarios. (3 marks)
8. “The internet never forgets”, give examples of forensic cases where this phrase can be applied (4 marks)
9. Elaborate on the three tees which make up cyber security (6 marks)
10. Discuss the motivation behind cybercrime and the areas where cyber criminals usually target (4 marks)

**QUESTION TWO (20 MARKS)**

1. Explain the various stages of forensic investigation when tracking computer crime (4 marks)
2. Outline the necessary skills required by a forensics examiner (4 marks)
3. Use scenarios to elaborate on the “3 As” of computer forensic methodologies (4 marks)
4. Discuss the approaches used to formulate cyber laws (4 marks)
5. Sometimes a computer security policy may not necessarily translate to a public law and sometimes it may. Identify possible scenarios when such happens (4 marks)

**QUESTION THREE (20 MARKS)**

1. 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. (4 marks)
2. When reporti*ng* security breaches to law enforcement, identify the various categories of crimes which a forensic examiner would deal with (4 marks)
3. Discuss the significance of DOS based and Linux based tools when gathering digital evidence (4 marks)
4. Outline the legal issues involved in seizure of computer equipment (4 marks)
5. What are the international issues relation to computer forensics in a cybercrime investigation (4 marks)

**QUESTION FOUR (20 MARKS)**

1. With the use of a diagram, explain the various categories and examples of computer forensic tools (4 marks)
2. Discuss the nature of file systems you would expect when dealing with data created and stored using:
3. Windows OS (4 marks)
4. Linux OS (4 marks)
5. Mac OS (4 marks)
6. A partition on an ATA hard drive is not recognized on your forensic workstation, which is running Linux. Explain the order in which troubleshooting steps should be taken to resolve this problem (4 marks)

**QUESTION FIVE (20 MARKS)**

1. Distinguish between an IDE and a SCSI hard drive (4 marks)
2. 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? (4 marks)
3. From the description of the file system layers, what would be the process of identifying unallocated space on a drive (4 marks)
4. How would you identify slack space (RAM and file slack)? (4 marks)
5. Name four methods for hiding data on a hard drive, using the layers below and information classification layer only. How would you, as an examiner, detect these conditions (4 marks)