JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL OF INFORMATICS AND INNOVATION SYSTEMS

UNIVERSITY EXAMINATION FOR THE DEGREE OF BACHELOR OF SCIENCE

COMPUTER SECURITY AND FORENSIC

2ND YEAR 2ND SEMESTER 2013/2014 ACADEMIC YEAR

MAIN

COURSE CODE: IIT 3224

COURSE TITLE: CRIMINALISTICS/FORENSIC SCIENCE LAB

EXAM VENUE: CL I **STREAM: (BSc. Computer Security and Forensic)**

DATE: 15/04/14 **EXAM SESSION: 2.00 – 4.00 PM**

TIME: 2.00 HOURS

Instructions:

1. **Answer question 1 (Compulsory) and ANY other 2 questions**
2. **Candidates are advised not to write on the question paper.**
3. **Candidates must hand in their answer booklets to the invigilator while in the examination room.**

Question 1 30marks

a.) Briefly describe the chain of custody. (5 marks)

b.) According to the practice guide for computer based electronic evidence explain what are the 4 principals of computer based evidence. (8 marks)

c) Write brief explanation to the following

i. D. N.A - (2 marks)

ii. Serology - (2 marks)

iii. Ballistic expert - (2 marks)

iv. Evidence control - (2 marks)

v. What is evidence beg - (2 marks)

vi. Forensic toxicology - (2 marks)

d) Briefly describe the difference between public computer forensic investigation and private computer forensic investigation. (5 marks)

Question 2. 20 marks

a) As a forensic investigator you are called to a crime scene and find a windows 2000 computer turned ON what are the steps you should take when seizing the equipment . (10 marks)

b) Most computer forensic tools Run on MS – Dos and Not MS – Dos shell . explain why giving example of two such tools . (6 marks)

c) Explain why its necessary to create a bootable floppy in computer forensic workstation . . (4 marks)

Question 3 20marks

a) Explain with example why an employee can be

b) Held liable for email harassment (5 marks)

c) Reports are to communicate the results of computer forensic investigations . Explain what a formal report is and where it would be presented . (5 marks)

d) When case go for trial , you as the forensic expert can either be a technical witness or an expert witness with example. Explain the two roles (10 marks)

Question 4. 20 marks

a) Explain how imaging techniques are applied in:

b) Forensic imaging , give example to support your answers. (5 marks)

c) Small Computer System Interface (SCSI) connects are used for a variety of periphery devices. What are the challenges they offer to a computer forensic investigator . (5marks)

d) Explain the precaution observed during the collection of digital evidence. (10marks)

QUESTION 5 20 marks.

a) Data mining applications usually employ neural networks in retrieving data which are not

b) Linearly related . Explain the benefits divided for using a neural networks application inrecovery data as part of evidence collection. (7 marks)

c) Describe two applications each for ultra violet and infra red lights inevidence collections . . (8marks)

d) Explain the following

- BIOS (1 mark)
- CACHE (1 mark)
- ENCRIPTION (1mark)
- MACRO – VIRUS (1 mark)
- MODEM (1mark)