JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL OF INFORMATICS AND INNOVATION SYSTEMS

UNIVERSITY EXAMINATION FOR THE DEGREE OF BACHELOR OF SCIENCE INFORMATION AND COMMUNICATION TECHNOLOGY

2ND YEAR 1ST SEMESTER 2013/2014 ACADEMIC YEAR

REGULAR

COURSE CODE: IIT 3212

COURSE TITLE: COMPUTER FORENSICS I

EXAM VENUE: LR 3 **STREAM: (BSc. ICT)**

DATE: 17/04/14 **EXAM SESSION: 11.30 – 1.30 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 ONE 30 MARKS

a) Define computer forensics?

b) What are the goals of forensics?

c) Who uses computer forensics

d) Compare and contrast between **Forensics vs. Incident Handling**

e) When you receive a workstation anti-virus alert, where do you expect to find log data

f) What can we learn from: i) Email logs, ii) Web server logs

g) Outline and describe the processes involved in computer forensics

(2+6+2+6+2+6+6Marks)

QUESTION TWO 20 MARKS

a) The following technologies are used in computer forensics:

   a. Slack space

   b. Host Protected Area (HPA)

   c. Device Configuration Overlay (DCO)

   d. Disk imaging

   Describe each technology

b) Computer Forensics investigation requires collaboration of

   – Law enforcement

   – Attorneys

   – Computer specialists

   Explain the role of all the above players

(10+10 marks)

QUESTION THREE 20 MARKS

a) State the ten guidelines in privacy protection during computer forensics

b) Outline some of the procedures used during imaging to ensure that evidence collected is clearly identified and preserved.

c) State some of the naming convention used when manually tagging all evidence items with an assigned case number.

(10+5+5 marks)

QUESTION FOUR 20 MARKS

a) What is case law and explain its importance?

b) Many legal issues facing technology and computer forensics from start of investigation through court testimony face complexities and adaptability of technology also potentially create a myriad of issues. Discuss

c) Explain the basic methodology consisting of the 3 As for computer forensics

d) Describe the general types of digital forensics

(5+5+5+5 marks)

QUESTION FIVE 20 MARKS

a) Outline the general forensic principles

b) State and explain the five rules of evidence

c) Compare and contrast between Bitstream vs. Backups

d) Computer related crime and violations include a range of activities including, outline them

e) Outline some of the methods used for hiding data

(4+4+4+4+4 marks)