JARAMOGI OGINGA ODINGA UNIVERSITY OF SCENCE AND TECHNOLOGY

SCHOOL OF INFRMATICS AND INNOVATIVE SYSTEMS

COURSE CODE: IIT 3224

COURSE TITLE: CRIMINALISTICS/ FORENSIC SCIENCE LAB

KISUMU LEARNING CENTRE

DECEMBER 2013 TIME 2HRS

INSTRUCTIONS:

i. **This paper contains five (5) questions.**
ii. **Question ONE is Compulsory and any other TWO questions**
iii. **Answer the questions on the booklet provided**

QUESTION ONE (30) COMPULSORY

a) Briefly describe the five standard steps for computer investigations [10 Marks]
b) Explain what is involved in planning an investigation [8 Marks]
c) Write brief explanations for the following:
   i) What is evidence bag? [2 Marks]
   ii) Why should your evidence be "write protected"? [2 Marks]
   iii) What should be on an evidence control from? [2 Marks]
   iv) Forensic toxicology [2 Marks]
   v) Finger – Print technology [2 Marks]
   vi) Forensic Psychology [2 Marks]

QUESTION TWO (20)

a) Briefly explain the strengths and weaknesses of the following information retrieval commands for displaying host names and network information. [10 Marks]
   i) Nslookup
   ii) Ifconfig
   iii) Rwho
   iv) Ruptine
   v) Trace route

b) Explain at least two challenges you encounter for recovering data from hard disk which is oddly partitioned [5 Marks]
c) Supposing you have FAT (File Allocation Table) of a hard disk logically intact and the rest of the tracks destroyed, will it be possible to recover data? Provide reasons if yes or no [5 Marks]

QUESTION THREE (20)

a) Explain with examples why an employer can be held liable for e-mail harassment [5 Marks]
b) Reports are to communicate the results of computer forensic investigations. Explain what a formal report is and where it would be presented [5 Marks]
c) When cases go for trial, you as the forensics expert can either be a technical witness or an expert witness. With examples, explain the two roles. [10 Marks]

QUESTION FOUR (20)

a) Explain the chain custody [5 Marks]
b) According to the practice guide for computer based electronic evidence, explain what are the four principles of computer based evidence [8 Marks]
c) Explain the following terms [7 Marks]
   i) Cracker
   ii) CACHE
   iii) MD5 Hash
   iv) Slack space
   v) Trojan Horse
   vi) Imaging
   vii) Dongle

QUESTION FIVE (20)

a) Data mining applications usually employ neural networks in retrieving data which are not linearly related. Explain the benefits derived for using a neural networks application in recovering data as part of evidence collection. [7 Marks]

b) Explain how imaging techniques are applied in forensic imaging. Give examples to support your answers. [5 Marks]

c) Discuss two applications each for ultra violet and infra red lights in evidence collections. [8 Marks]