JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS

DEPARTMENT OF COMPUTER SCIENCE & SOFTWARE ENGINEERING

UNIVERSITY EXAMINATION FOR THE DEGREE OF BACHELOR OF SCIENCE INFORMATION SECURITY AND COMPUTER FORENSICS

3RD YEAR SEMESTER 1 2018/2019 ACADEMIC YEAR

MAIN CAMPUS

COURSE CODE: IIT 3311

COURSE TITLE: COMPUTER FORENSIC II

EXAM VENUE:MAIN CAMPUS **STREAM IIT**

DATE: **EXAM SESSION:**

TIME:

INSTRUCTIONS

1. **Answer Question 1 (Compulsory) and ANY other TWO 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) (i) What is an image file (2 Marks)
(ii) Why is forensics copy of your evidence disk write protected? (2 Marks)
(iii) What is Drive Slack? (4 Marks)
(iv) Explain what AUTOEXEC.BAT is (2 Marks)
(v) Explain what is Meta Data and Data as used in Unix/Linux file structure(4 Marks)
(vi) LILO is a Linux/Unix utility program explain its use (2marks)
(vii) Why is it necessary to mitigate security risks in forensic and computer system? (3 Marks)
(viii) What is Digital Evidence? (2 Marks)
(ix) Identify three forensic tools available to system administrators (3Marks)

(b) Describe four tasks an investigator performs when working with digital evidence. (4 Marks)

(c) what does it take to be a successful computer forensic investigator. (2 marks)

QUESTION TWO. 20 MARKS

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

(b) Explain at least two challenges you encounter while 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 MARKS

(a) Data mining applications usually employ neural networks in retrieving data which are not linearly related. Explain the benefits derived for using a neural network application in recovering data as part of evidence collection. (10 Marks)

(b) Explain how imaging techniques are applied in forensic imaging. Give an example to support your answer (5 Marks)

(c) Outline the processes involved in the investigation of electronic crime (5 marks)

QUESTION FOUR 20 MARKS

(a) Describe two types of works protected under copyright. (6 marks)
(b) What is intellectual property? (2 Marks)
(c) What is Patent? Give two examples of patents with respect to computers. (6 marks)
(d) Ex plain the requirements needed by the federal court when presenting yourself as expert witness (6 marks)

QUESTION FIVE 20 MARKS

(a) Explain what is conflict out. (4 marks)
(b) Describe the three facts and issues you should know before giving testimony . (6 Marks)
(c) Explain the following
    (i) Deposition (2 marks)
    (ii) Discovery deposition (2 marks)
    (iii) Testimony preservation deposition (2 marks)
(d) When you go to collect evidence and you find the suspects computer turned on explain at least four precautionary steps you would take. (4 Marks)