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 COMPUTER FORENSICS

2ND YEAR SEMESTER 1 2018/2019 ACADEMIC YEAR

MAIN CAMPUS

COURSE CODE: IIT 3212

COURSE TITLE: COMPUTER FORENSIC I

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) Give brief explanation to the following terminologies

(i) Cracker (2 marks)

(ii) Cache (2 marks)

(iii) MD5 Hash (2 Marks)

(iv) Slack space (2 marks)

(v) Trojan horse (2 marks)

(vi) Imaging (2 Marks)

(vii) Dongle (2 Marks)

(viii) Steganography (2 Marks)

(ix) Asymmetric encryption. (2 Marks)

(x) Symmetric encryption. (2 Marks)

(b) Explain what is chain custody (4 Marks)

(c) What is evidence bag (4 Marks)

(d) What is the difference between FAT16 and FAT32 (2marks)

QUESTION TWO 20 marks

(a) Briefly describe five standard steps for computer investigation . (10 Marks)

(b) Explain what is involved in planning a computer forensic investigation (8 Marks)

(c) Explain Finger print technology. (2 Marks)

QUESTION THREE 20 MARKS

(a) Explain with examples why an employer can be held 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 a case goes for trial, you as the forensic expert can either be a technical witness or an expert witness. Explain the two roles. (10 Marks)

.

QUESTION FOUR 20 MARKS

(a) List four computer forensic tools with brief explanation you would use while conducting an investigation. (8 marks)

(b) What is Digital evidence? Give examples of four storage devices where such evidence could be found. (6 marks)

(c) List and briefly explain three common types of digital crimes. (6 marks)

QUESTION FIVE 20 MARKS

(a) Why is new technology file system (NTFS) more versatile. (5 Marks)

(b) New technology file system uses Unicode to store information. Briefly explain what is Unicord. (5 Marks)

(c) Small Computer System Interface(SCSI) connectors are used for variety of peripheral devices. Describe the challenges it gives a forensic investigator. (5 Marks)

(d) Explain inodes in Linux file system. (5 Marks)