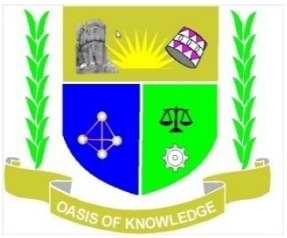

JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS

DEPARTMENT OF COMPUTER SCIENCE & SOFTWARE ENGINEERING

UNIVERSITY EXAMINATION FOR THE DEGREE OF BACHELOR OF SCIENCE IN SECURITY AND FORENSICS

2ND YEAR 1ST SEMESTER 2016/2017 ACADEMIC YEAR

KISUMU LEARNING CENTRE

COURSE CODE: IIT 3212

COURSE TITLE: COMPUTER FORENSICS 1

EXAM VENUE: **STREAM: COMPUTER SECURITY & FORENSICS**

DATE: **EXAM SESSION:**

TIME: 2HOURS

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) What is Computer Forensics? (3 marks)

b) What the difference between computer forensics and computer security? (3 marks)

c) State reasons why is cordoning off a crime scene important? (3 marks)

d) What is a file slack? Why should a forensic expert be concerned about file slack? 3 marks

e) Why is maintaining proper chain of custody of evidence important? (2 marks)

f) What is Steganalysis? (2 marks)

g) What Constitutes Digital Evidence? (2 marks)

h) What is the most common legal difficulty faced by organizations seeking to redress cybercrime in courts? (2 marks)

i) Why is keeping detailed log of ones actions is important during evidence gathering? (2 marks)

j) What best describes metadata? (2 marks)

i. Data that is important to the investigation
ii. Data about data
iii. Data that is hidden
iv. Operating system data

k) What type of encryption uses a different key to encrypt the message than it uses to decrypt the message? (2 marks)

i. private key
ii. asymmetric
iii. symmetric
iv. secure

l) If you copy a file between two folders on different partitions, what permissions with the file have after being copied? (2 marks)

i. The source folder
ii. Neither folder
iii. The destination folder
iv. The source partition

m) Most popular desktop PCs and notebook computers lack adequate security. This situation creates an ideal environment for electronic document discovery of the following, except: (2 marks)

i. Computer files
ii. File fragments
iii. Added files
iv. Data miming
v. Erased files

QUESTION TWO [20 MARKS]

a) What is a protocol analyzer (2 marks)
b) Who Uses Computer Forensics? (10 marks)
c) Identify and explain the four-step process in Computer Forensics (8 marks)

QUESTION THREE [20 MARKS]

a) Differentiate between active and passive attacks. Give two examples each (6 marks)
b) Proper handling information is a crucial activity done by computer forensic experts and more so volatile information. List and give example of volatile information (8 marks)
c) In order to maintain the integrity of evidence, the chain of custody procedures must be strictly observed. Describe Three of the chain of custody procedures (6 marks)

QUESTION FOUR [20 MARKS]

a) A digital fingerprint such as MD5 and SHA- 1 can be used to preserve evidence. List the two functions achieved by these digital finger prints on evidence. (2 marks)
b) Windows operating system does produce system data and artifacts that can be used as evidence. Briefly explain any Three types of system generated data and artifacts. (6 marks)

c) List and explain any three data hiding techniques (12 marks)

QUESTION FIVE [20 MARKS]

a) State various reasons For Evidence collection (4 marks)

b) An employee working with in the IT Department at ADC Corporation, Kisumu city is suspected to be selling the organization's bandwidth to deep webs to mine bit coins, against the company policy. He is also suspected to have been downloading and sharing child pornographic material. As independent consultant, you have been called by the head of IT to investigate the malpractice, misuse of company resources and prepare evidence to present the same in court of law as an expert witness.

Required:

i. Assume you and the Head of IT plan to ambush the suspect while s/he still using s/her workstation

ii. State any tools or software's you plan to use in the investigation.

iii. You are free to make any assumptions but do clearly state them if you do.

iv. Come up with a step by step procedure in processing the evidence (16 marks)