JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS

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

2nd YEAR 1st SEMESTER 2020/2021 ACADEMIC YEAR

SPECIAL/RESIT

MAIN CAMPUS

COURSE CODE: IIT 3212

COURSE TITLE: COMPUTER FORENSIC 1

EXAM VENUE: **STREAM: BSc Computer Forensics**

DATE: **EXAM SESSION:**

TIME: 2.00 HOURS

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 do you understand by the term file recovery? **(2 marks**)

b) Describe how you would recover the following files;

i) Sent to the recycled bin from the desktop **(3 marks)**

ii) Deleted while formatting a disk **(6 marks)**

c) A stranger has just forcefully broken into your computer systems. List down five factors that you would consider carrying out in intrusion analysis after the incident **(10 marks)**

d) Explain what happens when a file is sent to the recycle bin in NFTS? **(5marks)**

e) List four key procedures undertaken in computer forensics **(4 marks)**

QUESTION TWO [20MARKS]

a) Explain the meaning of the term forensics as applied to computer science **(4 marks)**

b) An intruder has just broken into the university computer system and erased the files from the department of finance.

As an expert you are now task with the responsibility of carrying out a forensic analysis to determine the identity of the culprit.

Briefly describe the type of digital evidence you will be looking for and suggest how the evidence can be made readable. **(16 marks)**

QUESTION THREE [20MARKS]

Two students of University A broke the door to the computer Lab on a Sunday.

One of them opened a computer and embarked on developing a programme that is part of his term work assignment. In the process when the code was run it deleted all operating system, replicated and spread to other computers on the university network.

The other student concentrated on games until the computer stopped after the operating system n collapsed. Later in the day the university security personnel realized and apprehended the two.

a) Explain the meaning of term computer incident security.
b) Identify the incidences for the day
c) List down the possible incidence responses from the scenario
d) State four reasons why incident response is a necessity in computer forensic analysis
c) In your opinion, do you think the two students referred to in the scenario committed a computer crime? Provide reason(s) to support your answer.

(20 marks)

QUESTION FOUR [20 MARKS]

a) List down the major factors that are of significance in the efficient use of water marking as a technique for protecting copy right **(4 marks)**

b) Briefly explain the difference between steganography and cryptography as data hiding techniques **(16 marks)**

QUESTION 5 [20 MARKS]

a) Explain the meaning of the term digital evidence as applied to computer forensics **(4 marks)**

b) You have been assigned the task of recovering information hidden in a word document with encrypted password by a suspect. Describe how you go about the exercise of accessing the information in the document. **(16 marks)**