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

4th YEAR 1st SEMESTER 2018/19 ACADEMIC YEAR

MAIN CAMPUS

COURSE CODE: IIT 3414

COURSE TITLE: CYBERCRIME INVESTIGATION

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

DATE: December 2018 **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 1 30 MARKS

a) Define the following terms:

i) Cybersquatting **(2 marks)**

ii) Data diddling **(2 marks)**

iii) Denial of Service(dos) attack **(2 marks)**

b) Explain how you would track on line child offenders **(4 marks)**

c) Evidence integrity is essential in order for digital evidence to be admissible in court and to carry weight as evidence.

i) What is Chain of Custody (CoC) **(2 marks)**

ii) Why is CoC important for evidence integrity **(2 marks)**

d) A police officer has come to search your premise for suspected cybercrime.How will you know that the search warrant he has is valid **(8 marks)**

e) Discuss how logfiles and IP addresses can be used to track unauthorized users **(8 marks)**

QUESTION 2 20 MARKS

a) What is OOV (order of volatility) and how does it influence decisions regarding which evidence should be preserved first **(4 marks)**

b) List 6 data storage media as a function of their OOV **(6 marks)**

c) Discuss 5 tools that hackers use to hack systems **(10 marks)**

QUESTION 3 20 MARKS

i. What is digital evidence **(2 marks)**
ii. Explain different types of digital evidence **(8 Marks)**
iii. Describe how digital evidence is gathered in a cybercrime scene **(10 marks)**

QUESTION 4 20 MARKS

b)What is the importance of cyberlaws in Kenya **(4 marks)**

b) Explain 5 types of cybercrime that are done frequently in digital world **(10 marks)**

c) Digital evidence is a rich and often unexplored source of information.These evidences can be used for crime reconstruction.Describe the 3 types of analyses that can be performed as part of cybercrime reconstruction **(6 marks)**

QUESTION 5 20 MARKS

a) What are the practical and technological issues that can arise during analysis of digital evidence **(10 marks)**

b) Describe the processes involved in preserving digital evidence in a cybercrime scene **(10 marks)**