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 2015/16 ACADEMIC YEAR

MAIN CAMPUS

COURSE CODE: IIT 3414

COURSE TITLE: CYBERCRIME INVESTIGATION

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

DATE: Dec 2016 **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

a) What do you understand by the expression "unauthorized access"? **(2 marks)**

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

c) Outline the documents that have to be included in an investigative report for a crime **(6 marks)**

d) Below is an extract from the Kenya Cybercrime law, read and provide an explanation why the law is providing an exemption stated in bold in the last paragraph.

> (1) *A person who, intentionally without lawful excuse or justification— (a) intentionally initiates the transmission of multiple electronic mail messages from or through such computer system; (b) uses a protected computer system to relay or retransmit multiple electronic mail messages, with the intent to deceive or mislead users, or any electronic mail or Internet service provider, as to the origin of such messages, or (c) materially falsifies header information in multiple electronic mail messages and intentionally initiates the transmission of such messages, commits an offence is liable upon conviction to an imprisonment term for a period not exceeding three years, or to a fine not exceeding five hundred thousand shillings or to both.*
>
> ***This section shall not apply to the transmission of multiple electronic messages within customer or business relationships.***

(8 marks)

e) i) Explain the term network probing **(4 marks)**

ii) Suggest two ways in which the *network scanning* can be used to counteract cybercrime. **(6 marks)**

Question 2

a) Define the term cyber stalking as applied to cybercrime **(2 marks)**
b) With the help of examples provide a detailed explanation why "cyber stalking" is considered a crime under the Kenyan legal system **(18 marks)**

Question 3

Describe how digital evidence is gathered in a cybercrime scene **(20 marks)**

Question 4

An authorized user has just forced his way into university network system and caused changes to the ERP system,

Discuss how logfiles and IP addresses can be used to track the unauthorized user.

(20 marks)

Question 5

a) What do you understand by the term cybercrime? **(2 marks)**

b) Describe the processes involved in preserving digital evidence in a cybercrime scene **(18 marks)**