JARAMOGI OGINGA ODINGA UNIVERSITY

OF SCIENCE & TECHNOLOGY

UNIVERSITY EXAMINATIONS 2012/2013

2ND YEAR 1ST SEMESTER EXAMINATION FOR THE DEGREE OF BACHELOR OF SCIENCE (COMPUTER SECURITY AND AUDIT)

(KISUMU L.CENTRE)

COURSE CODE: IIT 3212

COURSE TITLE: COMPUTER FORENSICS I

DATE: 12/8/2013 **TIME: 2.00-4.00 PM**

DURATION: 2 HOURS

INSTRUCTIONS

1. **This paper consists of 5 Questions.**
2. **Answer Question 1 (Compulsory) and any other 2 questions.**
3. **Write your answers on the answer booklet provided.**

QUESTION ONE [30 MARKS]

(a) "If you manage or administer information systems and networks, you should understand *computer forensics*"

(i) What do you understand by the term *computer forensics*? [2 Marks]

(ii) What is the difference between *computer forensics* and *forensic science*? [2 Marks]

(iii) Why is computer forensics important? [2 Marks]

(iv) Explain the 3As of computer forensics methodologies. [3 Marks]

(b) Distinguish between *Encipherment* and *Decipherment* as applies to cryptography. [2 Marks]

(c) Give the requirements for establishing a computer forensics laboratory. [3 Marks]

(d) In the 1980s, Clifford Stoll arguably became the first person to use forensic techniques to investigate computer misuse. Discuss any TWO techniques that he used and compare them with techniques that are currently being used. [4 Marks]

(e) When booting a suspect's computer, using boot media, such as forensic boot floppies or CDs, you must ensure that disk evidence isn't altered. Why is it so? [2 Marks]

(f) Data acquisition is important in digital evidence gathering. Name FOUR methods of data acquisitions that can be used in crime investigations process. [4 Marks]

(g) Prisca and Angela are both competitively vying for their company sales executive position. In order to outwit Angela, she circulated a damaging email to the company executives with an intention to water down her competitor's image. She opened and used a new email address to hide her identity. Which forensics tool is suitable for gathering digital evidence in this case? Identify THREE possible digital evidences that can be retrieved and used against Prisca. [4 Marks]

(h) Cybercrime is a word that is used but often listed in dictionaries. How do jurisdictional limitations affect how investigations into cybercrime are conducted? [2 Marks]

QUESTION TWO [20 MARKS]

(a) Using appropriate examples, define the following terms; [8 Marks]

(i) Incident Life Cycle,

(ii) Chain of Custody

(iii) Information Hiding Techniques

(iv) Expert Witness

(b) Imagine you are employed as an information security professional and are called to a crime scene in a company where there are a number of computers. There is strong suspicion that a crime has been committed using computers in the building. Describe ways in which you should capture data, and the order in which you should examine and catalogue machines in the affected area, including when and how they should be turned off and removed. [12 Marks]

QUESTION THREE [20 MARKS]

(a) Briefly discuss the legal complications of computer-based crime cases. [6 Marks]

(b) A woman accused her husband for being deeply involved in "wild hunting trips" where sexual encounters were arranged using computers. She presented her prayers infront of a jury where she opted for divorce and custody of their only daughter. In his defense to the accusation, the husband presented in court emails and attached pornographic images that made it appear the wife is the one who had been soliciting sex over the Internet. Custody of their 3 year old daughter was thus given to the husband and his mother (paternal grandmother). The wife denied she sent the emails and said it was not her in the photo. In preparation for divorce proceeding, the wife produced her husband's home computer Hard disk for forensic examination to locate financial records and child pornography. You have been hired to carryout forensic investigation in this case and file your report at the court registry for conclusion of litigation process. In your report, include investigation process, digital evidence, methods and forensics techniques used. [14 Marks]

QUESTION FOUR [20 MARKS]

(a) Using a suitable example, explain the difference between *computer forensics* and *network forensics*. [4 Marks]

(b) A "hack" can be often involving multiple techniques in order to circumvent various layers of security therefore, audits should encompass all types of security. Citing 5 practical examples, discuss the range of issues that the auditing process needs to consider if it is to achieve complete analysis of the organization's security framework. [10 Marks]

(c) Email is often used to distribute malware, turning machines into zombies on botnets. Access to these botnets can then be sold for nefarious purposes earning their masters huge cash. Describe how you can carry out forensics investigation into crime of this kind. [6 Marks]

QUESTION FIVE [20 MARKS]

(a) Name and describe one hardware and one software forensic tools that can be used in crime investigation. [4 Marks]

(b) "Acquisition of evidence is both a legal and technical problem. The approach to securing digital evidence is vital". Do you agree with this statement? Support your answer. [4 marks]

(c) What are the qualities of a good forensic investigator? [4 Marks]

(d) RFC 3227 lists the order of volatility in Windows-based system. How are volatile evidence handled in evidence gathering during a forensic investigation process? [2 Marks]

(e) How important are deleted files in digital evidence preparation? [2 Marks]

(f) What challenges might an investigator encounter when reviewing *utmp* and *wtmp* logs in UNIX systems? [4 Marks]

- END -