JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL INFORMATICS AND INNOVATIVE SYSTEMS

UNIVERSITY EXAMINATION FOR THE DEGREE OF SCIENCE

COMPUTER SECURITY & FORENSICS

2ND YEAR 1ST SEMESTER 2013/2014 ACADEMIC YEAR

CENTRE: MAIN

COURSE CODE: IIT 3212

COURSE TITLE: COMPUTER FORENSICS I

EXAM VENUE: LR 6 **STREAM: BSc. Computer Security & Forensics**

DATE: 18/12/2013 **EXAM SESSION: 11.30 – 1.30 PM**

TIME: 2 HOURS

Instructions:

1. **Answer question 1 (Compulsory) and ANY other 2 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

(a) "*Computer forensics* is a relatively new discipline to the courts and many of the existing laws used to prosecute computer-related crimes"

(i) Do you agree with the above statement? Explain. [2 Marks]

(ii) Is computer forensics the same as digital forensics? Explain. [2 Marks]

(iii) Give TWO reasons why it is important to study computer forensics. [2 Marks]

(b) Define the following terms as applies to computer forensics [8 Marks]

(i) Digital evidence

(ii) Expert witness testimony

(iii) Chain of custody

(iv) Steganography

(c) Give TWO technical challenges that admissibility of digital evidence in a court of law faces. [2 Marks]

(d) Consider a case where an email is often used to distribute malware, turning machines into zombies on botnets. Access to these botnets is then sold for nefarious purposes earning their masters thousands of dollars. Describe how you can carry out forensic investigation in an event where crime of that nature occurs. [4 Marks]

(e) A local university is in the process of establishing a computer forensics laboratory for their teaching, research and outreach activities. They require an expert input and you have been approached to assist with advice on how to establish one. Provide a brief summary of your advice on the basic requirements of such a laboratory. [6 Marks]

(f) In computer forensics, data acquisition is more of retrieval of digital evidence from target storage device. Compare and contrast how data acquisition is carried out in Windows OS and Linux. [4 Marks]

QUESTION TWO

(a) Compare and contrast evolution of computer forensics with forensic science. [4 Marks]

(b) Cybercrime can be understood to mean any illegal act that involves a computer, its systems, or its applications.

(i) Name any TWO practical examples of cybercrime you know [2 Marks]

(ii) Identify respective motivations of mentioned examples in (i) above. [2 Marks]

(iii) Give the required stages of forensic investigation involved in tracking a cybercrime [4 Marks]

(c) Consider this case involving computer forensics in which the defendant accessed child pornography on a workplace computer. The company monitored employee Internet use and determined by tracing the IP address that the child-pornographic websites had been accessed from the computer in the defendant's office. Suppose you have been engaged as a forensic expert to conduct investigation and prepare a report to be used in a court of law for further litigation purposes. Include also in your report the type of forensics tools, methods and techniques applied in acquiring evidence here. [8 Marks]

QUESTION THREE

(a) "From a network forensic standpoint, it is important to note that a virtual machine can be used to attack another system or network".

(i) In your own words, use a practical example to support the above statement. [4 Marks]

(ii) Briefly explain how you would retrieve digital evidence from a virtual machine. [6 Marks]

(b) Why is it important to understand the disk structure of target computer system when conducting a forensic investigation? Use an example to support your answer. [4 Marks]

(c) A corruption case that almost got concluded took a new twist after the ex-girlfriend of the accused voluntarily provided two hard disks left in her house containing data that is crucial in the case. She also availed four flash drives and fifteen diskettes that requests for formatting whenever plugged into a PC. She also revealed that more evidence can be got from her old company's e-mail account where she worked as an intern as they used to share information. As a forensic expert, you are hired to carry out investigation and present admissible evidence in a court of law, for litigation purposes. [6 Marks]

QUESTION FOUR **[20 MARKS]**

(a) What are the qualities of a forensic investigator? [2 Marks]

(b) Identify TWO activities that are involved in each of the following stages of forensic investigation listed below. [8 Marks]

(i) Raiding the scene of crime

(ii) Processing scene of crime

(iii) Preservation of digital evidence

(iv) Examination of collected digital evidence

(c) Apply the stages of investigation mentioned in qn. 4(b) above in the following cases below. [10 Marks]

(i) Ann hacked into university's network servers and accessed examinations information.

(ii) Peter uses his computer to produce illegal copies of copyrighted software for sale.

QUESTION FIVE

(a) "Investigating cell phones and mobile devices is one of the most challenging tasks in digital forensics"

(i) Do you agree with the above statement? Support your answer. [4 Marks]

(ii) List any FOUR items stored in cell phones that can attract forensic investigation [4 Marks]

(iii) Name any TWO software tools that can be used to retrieve data stored in mobile devices. [2 Marks]

(iv) Identify any TWO legal challenges likely to be faced when retrieving digital evidence from a cell phone. [2 Marks]

(b) Provide forensics investigation guidelines that can be used for the following cases [8 Marks]

(i) A mobile phone is used to send inflammatory messages

(ii) A mobile device is used to distribute and receive child pornographic contents