JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS

DEPARTMENT OF COMPUTER SCIENCE AND SOFTWARE ENGINEERING

UNIVERSITY EXAMINATION FOR THE DEGREE OF MASTER OF INFORMATION TECHNOLOGY SECURITY AND AUDIT

2ND YEAR 1ST SEMESTER 2021/2022 ACADEMIC YEAR

KISUMU CAMPUS

COURSE CODE: IIT 5214

COURSE TITLE: COMPUTER DIGITAL FORENSICS

EXAM VENUE: **STREAM: Msc**

DATE: DECEMBER 2022 **EXAM SESSION:**

TIME: 3.00 HOURS

INSTRUCTIONS:

1. **Answer ANY three 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 **[20 MARKS]**

a) Consider a case where a commercial bank operating in Nairobi has hired you to investigate employee fraud. The bank uses four 20 TB machines on a LAN. You're permitted to talk to the network administrator, who is familiar with where the data is stored.
   i) Explain the strategies and acquisition method you shall use in this case. [4 Marks]
   ii) Briefly outline the problems you expect to encounter, explaining how to rectify them, and describing your solution. Be sure to address any customer privacy issues. [6 Marks]

b) Consider a case where your spouse works at a training college in Kisumu and reports rumors of a tutor, Mr. Zilch Otoyo, molesting some students and taking illicit pictures of them. Otoyo allegedly viewed these pictures in his office. Your spouse wants you to take a disk image of Otoyo's computer and find out whether the rumors are true.
   i) Briefly outline how you would guide your spouse and school administrators on how to proceed with this case. [6 Marks]
   ii) Explain why walking into Otoyo's office to acquire a disk image wouldn't preserve the integrity of the evidence. [4 Marks]

QUESTION TWO **[20 MARKS]**

a) Consider a case where John has desperately called you because he has accidentally deleted crucial files from his hard drive and can't retrieve them from the Recycle Bin.
   i) Explain what options you are likely to opt for while assisting John in this case. [4 Marks]
   ii) Provide a write-up explaining your capabilities and listing the questions you need to ask her about her system. [6 Marks]

b) Consider yourself as the digital forensics investigator for a law firm here in Kenya. The firm acquired a new client, a young woman who was fired from her job for inappropriate files discovered on her computer. She swears she never accessed the files.
   i) List the kind of questions you shall ask her and how you shall handle the case. [4 Marks]
   ii) Provide a report describing the computer the client used, who else had access to it, and any other relevant facts that should be investigated. [6 Marks]

QUESTION THREE **[20 MARKS]**

The CEO of Madawa Hospital Ltd have heard about forensics readiness and has expressed interest in adopting it within their enterprise network. Consider a case where she has contacted you to advise her on how her institution can incorporate it in their management of digital assets. Prepare an advisory document for her along the following lines:

a) Goals of forensics readiness for their institution [4 Marks]
b) Benefits of forensics readiness for their institution [3 Marks]
c) Relevant steps to be considered in forensic readiness planning for their institution. [10 Marks]
d) Challenges that are likely come with the forensic readiness. [3 Marks]

QUESTION FOUR **[20 MARKS]**

a) Consider a case where you have acquired a forensic image of a suspect's laptop. After doing an examination, you discovered that at least one Virtual Machine (VM) installed, and you are convinced more data can be found though you aren't sure. Suppose you decide to make a copy of the VM's files and mount the VM as an external drive. Describe the best procedure you shall use for this case. [6 Marks]

b) A cloud customer has asked you to do a forensics analysis of data stored on a Cloud Service Provider's server. The customer's lawyer explains that the Cloud Service Provider (CSP) offers little support for data acquisition and analysis but will help with data collection for a fee. The lawyer asks you to prepare a memo with detailed questions of what you need to know to perform this task. She plans to use this memo to negotiate for services you'll provide in collecting and analyzing evidence. In your memo, include the questions the lawyer shall ask the CSP. [7 Marks]

c) Your attention has been drawn into a case where a high school student, Wambui, claims she just received a Facebook message from another student who was threatening to commit suicide. She isn't sure where the student was when she sent the message. Describe how you shall proceed and enable obtaining evidence that can be used by law enforcement agencies to address this case. [7 Marks]

QUESTION FIVE **[20 MARKS]**

a) Consider yourself investigating a case involving an employee who's allegedly sending inappropriate photos via e-mail in attachments that have been compressed with a zip utility. As you examine the employee's hard disk, you find a file named xyz.zip, which you suspect is a graphics file. When you try to open the file in an image viewer, a message is displayed indicating that the file is corrupt. Briefly explain how you shall recover xyz.zip for further investigation. [4 Marks]

b) There is a case where several graphics files were transmitted via e-mail from an unknown source to a suspect in an ongoing investigation. The lead investigator gives you these graphics files and tells you that at least four messages should be embedded in them. Use your problem-solving and brainstorming skills to determine a procedure to follow in handling this case. [5 Marks]

c) In the case of a drive you're investigating, you have discovered that it contains several password-protected files and other files with headers that don't match the extension.

i) Describe the procedures you shall use to retrieve the evidence with some of the forensics tools and hexadecimal editors. [4 Marks]

ii) Explain how you shall identify the file headers and determine how their extensions are mismatched. [4 Marks]

iii) Discuss the techniques and tools you shall use for recovering passwords from the protected files. [3 Marks]

- END –