JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS

DEPARTMENT OF COMPUTER SCIENCE & SOFTWARE ENGINEERING

UNIVERSITY EXAMINATION FOR THE DEGREE OF MASTERS IN INFORMATION TECHNOLOGY SECURITY AND AUDIT

2nd YEAR 1st SEMESTER 2023/2024 ACADEMIC YEAR

MAIN CAMPUS

COURSE CODE: **IIT 5214**

COURSE TITLE: **Computer Digital Forensics**

EXAM VENUE: **STREAM: Masters in IT security and Audit**

DATE: **EXAM SESSION:**

TIME: **3.00 HOURS**

INSTRUCTIONS:

Answer QUESTION ONE and ANY other TWO questions

QUESTION ONE (20 Marks)

a) A computer forensics professional does more than turn on a computer, make a directory listing, and search through files. The forensics professionals should be able to successfully perform complex evidence recovery procedures with the skill and expertise that lends credibility to a given case. Discuss any **FIVE** services that are offered by the computer forensics professionals. (5 mks)

b) Before you start collecting evidence, it is important to know the different types of evidence categories. Without taking these into consideration, you may find that the evidence you've spent several weeks and quite a bit of money collecting is useless. Real evidence is any evidence that speaks for itself without relying on anything else. Using relevant examples, describe the following as used in this respect.
   i) Testimonial Evidence (4 mks)
   ii) Hearsay (4 mks)

c) Computer evidence is fragile by its very nature, and the problem is compounded by the potential of destructive programs and hidden data. Even the normal operation of the computer can destroy computer evidence that might be lurking in unallocated space, file slack, or in the Windows swap file. Give some guidelines that should be followed during computer evidence processing. (7 mks)

QUESTION TWO (20 mks)

At the moment, many computer forensics workshops have been created to familiarize investigators and security personnel with the basic techniques and tools necessary for a successful investigation of Internet and computer-related crimes.

a) Discuss some of the forensic services available in the current forensics field. (10 mks)

b) Describe some of the computer forensics systems that can support the forensics services in (a) above. (10 mks)

QUESTION THREE (20 mks)

We live in a world that is driven by the exchange of information. Ownership of information is one of the most highly valued assets of any business striving to compete in today's global economy. Companies that can provide reliable and rapid access to their information are now the fastest growing organizations in the world. To remain competitive and succeed, they must protect their most valuable asset—data. Fortunately, there are specialized hardware and software companies that manufacture products for the centralized backup and recovery of business critical data. Hardware manufacturers offer automated tape libraries that can manage millions of megabytes of backed up information and eliminate the need for operators charged with mounting tape cartridges. Discuss how the following impede effectual backup services:

i) Backup window (5 mks)

ii) Network bandwidth (5 mks)
iii) System throughput (5 mks)
iv) Lack of resources (5 mks)

QUESTION FOUR (20 mks)

a) A chain of custody is a roadmap that shows how evidence was collected, analyzed, and preserved in order to be presented as evidence in court. Establishing a clear chain of custody is crucial because electronic evidence can be easily altered. A clear chain of custody demonstrates that electronic evidence is trustworthy. Explain how this trustworthiness can be achieved. (8 mks)

b) Discuss the following concepts as used in computer forensics:

i) Computer fraud (3 mks)
ii) Computer forgery (3 mks)
iii) Computer sabotage (3 mks)
iv) Unauthorized interception (3 mks)

QUESTION FIVE (20 mks)

a) Protection of digital evidence is critical. A knowledgeable computer forensics professional should ensure that a subject computer system is carefully handled. Discuss the main reasons for the proper handling of subject computer systems during forensics exercise. (10 mks)

b) Describe some of the problems encountered when dealing with computer forensic evidence.

(10 mks)