UNIVERSITY EXAMINATIONS
2021/2022 ACADEMIC YEAR

YEAR FOUR SEMESTER TWO EXAMINATIONS

FOR THE DEGREE OF BACHELOR OF SCIENCE COMPUTER SCIENCE

COURSE CODE : CSC 458E

COURSE TITLE : COMPUTER FORENSICS

DATE: 21/11/2022 **TIME: 08:00 A.M – 10:00 A.M**

INSTRUCTIONS TO CANDIDATES

ANSWER QUESTIONS ONE AND ANY OTHER TWO.

QUESTION ONE [COMPULSORY] [30 MARKS]

a) What do you understand by the following as applied in computer forensics:
   i) File manipulation [2mks]
   ii) Disk manipulation [2mks]
   iii) Encryption [2mks]

b) Define the following terms: [3mks]
   i) Define stenography
   ii) Watermarking
   iii) Slack

c) An incident occurred in an organization and a forensic expert was called in to try and recover the information to an earth the details and inform the decision making by the organization. The expert experienced some difficulties in accessing the password used. State three ways the expert could use to gain access to the password for the machine in question. [4mks]

d) Describe any five good qualities of good evidence. [10marks]

e) An organizations website was hacked into and the management would like to find out the details. Describe how a forensic auditor could assist in this exercise. [4mks]

f) Keystroke loggers can be employed by a network administrator to try and safe guard organization resources. Briefly explain why method may be affecting the organization resources. [3mks]

QUESTION TWO [20 MARKS]

a) Explain the three main methods followed in computer forensics. [8mks]

b) Name the commonly used tools in imaging hard disk drives/disks. [2mks]

c) Explain any five computer crimes. [10mks]

QUESTION THREE [20 MARKS]

a) What is the importance of looking into the system logs after an incidence? [5mks]

b) A part from the system logs, which other logs can a system admin exam to try and find the activities of an intruder? [2mks]

c) Which are the most common files that hackers replace most when they gain entry to a system [3mks]

d) Briefly explain the goals of an incident response. [8mks]

e) What is the prime of any forensic expert? [2mks]

QUESTION FOUR [20 MARKS]

a) Outline the differences between an examination report and verbal report in forensics. [8mks]

b) What do you understand by Spoliation? [1mk]

c) Briefly explain the structure of a forensics report. [8mks]

d) Why is authenticating evidence usually difficult in computer forensics? [3mks]

QUESTION FIVE [20 MARKS]

a) Outline the various techniques that intruders use to hide data. [9mks]

b) With examples, differentiate between traditional forensics and computer forensics. [2mks]

c) Briefly explain the type of data acquisition in computer forensics. [4mks]

d) Acquisition tools have been developed for different operating systems including Windows, Linux, Mac .Outline the acquisition methods that can be used in forensics. [5mks]