(*Knowledge for Development*)

KIBABII UNIVERSITY

UNIVERSITY EXAMINATIONS
2021/2022 ACADEMIC YEAR

END OF SEMESTER EXAMINATIONS
YEAR ONE SEMESTER ONE EXAMINATIONS

FOR THE DEGREE OF
MASTER DIGITAL FORENSICS

COURSE CODE : MDF 811

COURSE TITLE : FUNDAMENTALS OF DIGITAL FORENSICS

DATE: 01/10/2022 **TIME: 09.00 A.M – 12.00 A.M**

INSTRUCTIONS TO CANDIDATES

ANSWER QUESTIONS ONE AND ANY OTHER TWO.

QUESTION ONE (COMPULSORY) [20 MARKS]

a) Explain the following terms: **[8 marks]**

i) Digital forensic

ii) Computer crime

iii) Computer forensic

iv) Cyber security

b) Outline any two functions of a forensic specialist. **[2 marks]**

c) Computers and digital devices are prone misuse by people in and outside an organization. Explain some of the ways in which computers and digital devices can be used to commit crimes or may be misused. **[6 marks]**

d) Briefly explain how computer forensics is supporting the groups named below.

i) Criminals **[2 marks]**

ii) Governments **[2 marks]**

QUESTION TWO [20 MARKS]

a) Before digital evidence is analyzed, it must be secured, unmodified, and copied. Forensic data acquisition is the process of making an exact copy or image of digital media evidence. Which factors will an investigator consider when choosing the appropriate data acquisition method. **[4 marks]**

b) A computer crime happened in an organization two months ago. The management have reviewed the happenings and decided to engage the services of a computer forensic expert in order to un lock the mystery.

i) Data Acquisition is the process of imaging/ obtaining information from a digital device and it's peripheral equipment & media. Explain the types of data acquisition methods. **[4 marks]**

ii) Outline any two the tools that can be used to collect data from: disk to image and disk to disk. **[4 marks]**

iii) What will be the prime goal of the forensic expert in this case? **[2 marks]**

iii) Explain how the expert will about to in order to recover the evidence. **[6 marks]**

QUESTION THREE [20 MARKS]

a) Forensic evidence must be collected and analyzed in such a way that it is admissible in a court of law. Outline any FIVE qualities of good computer evidence. **[5 marks]**

b) Explain the formats used for data acquisition. **[6 marks]**

c) i. What do you understand by data de-duplication. **[2 marks]**

ii. Outline the advantages of data de-duplication. **[3 marks]**

iii. Discuss any two data de-duplication techniques. **[4 marks]**

QUESTION FOUR [20 MARKS]

a) Digital evidence differs from traditional evidence in multiple ways. Explain these differences. **[8 marks]**

b) Special consideration is necessary when establishing the authenticity, protecting integrity and maintaining the confidentiality of digital evidence (**CIA**). Outline any FIVE such special considerations during the forensic process. **[6 marks]**

c) Chain of Custody for digital evidence is the chronological documentation of its handling from the time of collection until its disposal. What elements should be documented in a chain of custody? **[6 marks]**

QUESTION FIVE [20 MARKS]

a) List the network file system (NTFS) analysis tools used in computer forensic. **[4 marks]**

b) A television's station's web-site was hacked by two teenagers who gained access to the web-site by accident with "hacker slogans"

i) Outline the lessons that the management learnt after the hacking. **[5 marks]**

ii) What preventive measures should the television station put in place to avoid a similar occurrence? **[4marks]**

iii) Digital evidence examination must be conducted in a professional way. Explain how you would successfully conduct digital evidence examination for Kibabii University. **[7 marks]**