(Knowledge for Development)

KIBABII UNIVERSITY
(KIBU)

UNIVERSITY EXAMINATIONS
2022/2023 ACADEMIC YEAR

END OF SEMESTER EXAMINATIONS
YEAR 1 SEMESTER II

FOR THE DEGREE OF
MASTER OF DIGITAL FORENSICS

COURSE CODE: MDF 821

COURSE TITLE : DIGITAL FORENSIC INVESTIGATION

DATE: 10/02/2023 **TIME: 9.00 AM - 12.00 NOON**

INSTRUCTIONS

SECTION A IS COMPULSORY.

ANSWER ANY 2 QUESTIONS FROM SECTION B. EACH QUESTION IN THIS SECTION CONTAINS 20 MARKS.

SECTION A [COMPULSORY QUESTION]

QUESTION ONE [20 MARKS]

a. **i.** Whenever you are dealing with electronic evidence, there are general forensic and procedural principles that should be applied. Outline these principles. **[3 Marks]**

ii. Who can use the principles and guidelines in (i) above. **[4 Marks]**

b. i. Explain with examples what you understand by "***Electronic Evidence***" **[4 Marks]**

c. **i.**Precautions must be taken in the collection, preservation, and examination of electronic evidence. Explain how electronic evidence is handled at the Crime Scene. **[7 Marks]**

ii. Outline any two electronic devices from which we can collect electronic evidence. **[2 Marks]**

SECTION B

ANSWER ANY TWO (2) QUESTIONS FROM THIS SECTION

QUESTION TWO [20 MARKS]

a. Evidence is most commonly found in files that are stored on hard drives. User-created files may contain important evidence of criminal activity. Discuss any four (4) such files. **[4 Marks]**

b. **i.** A user of a computer system in your organization may hide evidence on the system h/she is using in a variety of forms. Explain briefly any four (4) ways the user may hide the data. **[8 Marks]**

ii. Outline any three components of files that may have evidentiary value to a forensic investigator. **[3 Marks]**

c. **i.** When using computers there are files that are generated by these devices. State any 3 computer generated files. **[3 Marks]**

ii. Outline any Two evidences one can get from a Voice answering machine **[2 Marks]**

QUESTION THREE [20 MARKS]

a. Outline any two investigative tools and equipment that can be used to collect electronic evidence. **[2 Marks]**

b. Discuss how you would secure and evaluate a crime scene in preparation for forensic investigation. **[18 Marks]**

QUESTION FOUR [20 MARKS]

a Outline the policy and principle that should be followed when documenting a crime scene. **[2 Marks]**

b When planning for digital forensic investigation in a house/ office, there is need for initial documentation of the physical crime scene. Discuss the contents of the initial physical documentation. **[10 Marks]**

c After securing the scene what would you do if the computer monitor is found to be "off" in order to avoid losing data. **[8 Marks]**

QUESTION FIVE [20 MARKS]

a. Computers are fragile electronic instruments that are sensitive to temperature, humidity, physical shock, static electricity, and magnetic sources. Therefore, special precautions should be taken when packaging, transporting, and storing electronic evidence. To maintain chain of custody of electronic evidence, its necessary to document its packaging, transportation, and storage. Discuss the recommended packaging, transportation and storage procedures to be followed. **[10 Marks]**

b. Securing and processing a crime scene where the computer systems are networked poses special problems, as improper shutdown may destroy data. This can result in loss of evidence and potential severe civil liability. When investigating criminal activity in a known business environment, the presence of a computer network should be planned for in advance. What are the indicators that a computer network may be present in this business environment? **[4 Marks]**

c. i. Outline any three evidences of 'computer intrusion'. **[3 Marks]**

ii. What is the importance of the Antistatic bags, Evidence bags and Evidence tape in digital forensic investigation. **[3 Marks]**