(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 OF SCIENCE IN DIGITAL FORENSICS

COURSE CODE : MDF 813

COURSE TITLE : COMPUTER FORENSICS TECHNOLOGIES

DATE: 01/10/2022 **TIME: 02.00 P.M – 05.00 P.M**

INSTRUCTIONS TO CANDIDATES

ANSWER QUESTION ONE IN SECTION A AND ANY OTHER TWO QUESTIONS IN SECTION B

QUESTION ONE [30 MARKS]

a) Briefly describe the computer investigation model. [4 Marks]

b) What is digital evidence? What is its role in the investigation process? Give examples of some common digital evidences. [3 Marks]

c) Forensic practitioners must follow strict guidelines and maintain the highest standards of work ethics to achieve accuracy because emphasis must be on evidential integrity and security. A Computer Forensic investigation must follow a rigid set of methods to ensure that computer evidence is correctly obtained. These steps are Protect, Discover, Recover, Reveal, Access, Analyze, Report and Testimony. Describe the above steps with regard to application to computer forensic investigation. [4 Marks]

d) Assume that you are an employee of the Directorate of Criminal Investigation as an Investigation Officer. You have been presented with a case involving suspected murder to investigate and present a report to be relied on in court by a prosecutor. Joshua Zarkan found his girlfriend's dead body in her apartment and reported it. The first responding law enforcement officer seized a USB drive. A crime scene evidence technician skilled in data acquisition made an image of the USB drive with FTK Imager and named it C1Prj01.E01. Following the acquisition, the technician transported and secured the USB drive and placed it in a secure evidence locker at the police station. You have received the image file from the detective assigned to this case.

   i. Using the set of methods in c) above document the case. [4 Marks]

   ii. Examine/analyze it and identify any evidentiary artifacts that might relate to this case. [4 Marks]

e) Computer digital forensics utilize various tools (hardware and software) to collect and present credible evidence that can be used to justify a certain investigation course. Describe any such tools you are conversant with whether applied in computer systems, network analyzers or even mobile devices and the procedure of application. [7 Marks]

f) In the Kenyan context, describe the legal framework upon which computer digital forensics is established and operated on. [4 Marks]

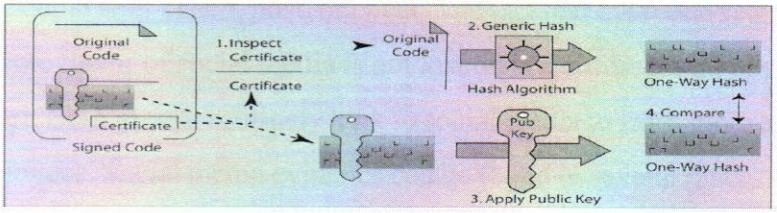
SECTION B

QUESTION TWO [15 MARKS]

i. You are the digital forensics investigator for a law firm. 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. What questions should you ask and how should you proceed? Write a one- to two-page report describing the computer the client used, who else had access to it, and any other relevant facts that should be investigated.

[6 Marks]

ii. Examine the following picture:



Describe what is happening and how it is fully applied in digital forensics? [9 Marks]

QUESTION THREE [15 MARKS]

Write a disaster backup and recovery plan of not more than two pages for a fictitious company's digital forensics lab. Include backup schedules, note the programs and OS installed on each machine, and list other information you would have to recover after a disaster. You should also note where the original disks and backups are located. [7 Marks]

A bank has hired your firm to investigate employee fraud. The bank uses four 20 TB machines on a LAN that has an internet connection. You're permitted to talk to the network administrator, who is familiar with where the data is stored. You are allowed to examine all network systems in your investigations among them the network and security equipment (IDS, IPS e.t.c) and computer systems. What diplomatic strategies should you use? Which acquisition method should you use? Write a two-page report outlining the problems you expect to encounter, explaining how to rectify them, and describing your solution. Be sure to address any customer privacy issues. [8 Marks]

QUESTION FOUR [15 MARKS]

i. Describe how the following internet technologies can provide a lot of forensic information when you are conducting an investigation. [9 Marks]

- Peer to peer applications
- Cache and temporary internet files
- Cookies
- Web browsers
- Indexed files

ii. E-mail and social media have at least one thing in common. There seems to be almost nothing that people won't send, post, or tweet. The fact that everyone seems to be on Facebook, Twitter, or some flavor of social media is not lost on law enforcement or prospective employers for that matter. Both groups routinely look to social media to learn more about suspects and prospective employees. Social media evidence can be found in several places. Assume that you are required to conduct an investigation involving a crime scene on these platforms, how would you go about while extracting evidence that would be used to bring the suspects to book? [6 Marks]

QUESTION FIVE [15 MARKS]

There are many different ways to hack and/or attack a network. These attacks change at something akin to "warp" speed, resulting in a constant strain on the security industry. Below are just some of the attacks in use today. Describe the underlisted attacks and how an investigator can extract critical information to be used to nab attackers. [15 Marks]

- Distributed Denial of Service (DDoS)
- Identity Spoofing
- Man-In-The-Middle-Attacks
- Social Engineering
- Footprinting or fingerprinting

QUESTION SIX [15 MARKS]

Describe the following terms/activities as used in digital forensics:

i. Types of Evidence: [7 Marks]

- The Rules of Evidence and General Procedure,
- Volatile Evidence,
- Collection and Archiving;

ii. Methods of evidence collection [8 Marks]

- Artifacts,
- Collection Steps,
- Controlling Contamination,
- Reconstructing the Attack.