UNIVERSITY EXAMINATIONS
2022/2023 ACADEMIC YEAR

END OF SEMESTER EXAMINATIONS
YEAR ONE SEMESTER TWO EXAMINATIONS

FOR THE DEGREE OF
MASTER OF SCIENCE IN DIGITAL FORENSICS

COURSE CODE : MDF 822

COURSE TITLE : OPERATING SYSTEM INVESTIGATION

DATE: 10/02/2023 **TIME: 2:00 P.M – 05:00 P.M.**

INSTRUCTIONS TO CANDIDATES

ANSWER QUESTIONS ONE AND ANY OTHER TWO.

QUESTION ONE [20 MARKS]

Windows 8 Digital Forensic investigation follows the current Forensic process models that are available. A successful investigation will rely on the resources available, the objectives of the investigation, the policies of the organization and the circumstances involved in the investigation. Mainly the Digital Crime Scene Investigation comprises of six phases: Preservation, Survey, Documentation, Search & collection, Reconstruction, and Preservation. Other authors have described the Forensic process where electronic evidence offers very special challenges for its admissibility in court. In order to meet the admissibility in court, proper Forensic procedures have to be followed.

i. Discuss the potential evidence found in Windows Operating System and the types of files focused by the highlighted evidences. [10 Marks]

ii. The computer Forensic tools testing handbook release by National Institute of Standards and Technology provides reports on the selection of the tool to determine the tools performance on the core Forensic such as imaging drives. Discuss the tools reviewed for Windows 8 Digital Forensic investigation today. [10 Marks]

QUESTION TWO [20 MARKS]

a) Email is one of the most common methods of communications today. What are some of the ways that email can be investigated and used as evidence? [5 Marks]

b) Discuss the various laws that have been enacted for email investigations. [5 Marks]

c) The Windows Operating system is the most common operating system on the planet. Discuss some of the tools and files that are routinely examined and used in a Windows Operating System investigation. [10 Marks]

QUESTION THREE [20 MARKS]

a) Suppose you are an investigator and you have been given an assignment from an investigating firm, in which you have been given a Virtual image of a compromised system. The first thing you need to do is to setup an environment to mount the image. As a result, you need to choose an OS, what should you choose, and why? [10 Marks]

b) In the investigation field, there a proposition that one should never make assumptions about a tool and its "memory footprint" when run on a system. Without thorough examination and testing, you'll never know the kind of footprint an executable has on a system or the kinds of artifacts it leaves behind following its use. Justify this statement. [10 Marks]

QUESTION FOUR [20 MARKS]

a) Often, users hide or protect files to prevent them from being found or accessed. There are a variety of techniques to hide files. Discuss some of the most common methods used to achieve this objective. [6 Marks]

b) A user might also seek to protect files using steganography or encryption. Discuss the reasons why you would prefer one over the other. [5 Marks]

c) The Windows registry is a central database that stores settings and configurations for the operating system and most applications installed on the system. The system and its users, applications, and hardware make use of the registry to store configuration details and for reference while operating the system. Discuss each of the following hives as used in windows registry.

i. HKEY_CLASSES_ROOT (HKCR) [3 Marks]

ii. HKEY_CURRENT_USER (HKCU) [3 Marks]

iii. HKEY_LOCAL_MACHINE (HKLM) [3 Marks]

QUESTION FIVE [20 MARKS]

a) Differentiate between Digital Forensics and Digital Investigations [4 Marks]

b) Within the digital forensics field, there are several different types of special experts. Discuss each of the following.

i. Operating and file system experts [1 Mark]

ii. Data recovery experts [1 Mark]

iii. Forensic accounting experts [1 Mark]

iv. Recording and archival extraction experts [1 Mark]

v. Intrusion and malicious code experts [1 Mark]

vi. Cloud-computing experts [1 Mark]

QUESTION FIVE [20 MARKS]

(a) You have been alerted that the computer you are using has a polymorphic virus.

(i) What are polymorphic viruses? **[2 Marks]**

(ii) Describe TWO approaches that hackers use to devise such viruses. **[2 Marks]**

(iii) List TWO controls that can be used against polymorphic viruses. **[2 Marks]**

(b) Consider the following pseudocode in an authentication program:

```
1.username = read_username();
2 password = read_password();
3 if username == "?133t h4ck0r?" then
4 return ALLOW_LOGIN;
5 endif
6 if username and password are valid then
7 return ALLOW_LOGIN;
8 else
9 return DENY_LOGIN;
10 endif
```

(i) Explain the type of malicious code this one is. **[1 Mark]**

(ii) Briefly describe this type of malicious code AND suggest a control against it. **4 Marks]**

(c) Considering the access control matrix shown below for some components of an IT system, write the access control list for "File-2" and "Process-1" **[4 Marks]**

	File-1	File-2	Process-1	Process-2
User-A	r	orwx	-	orwx
User-B	r	orw	r	rw
Process-1	orw	-	rw	r
Process-2	-	w	orwx	r

(d) Describe the role of a firewall within an IT system, and give examples of TWO simple security policies that firewalls can implement. **[5 Marks]**

c) A file system is "a method for storing and organizing computer files and the data they contain, to make it easy to find and access them." It provides a method to access specific data, which is stored on a disk in files. A file is a named collection of related data that is used for organizing secondary memory. Discus the correlation between File System and Master File Table. [6 Marks]

d) Discuss two major file systems used to organize data in Windows operating system. [4 Marks]