NAMIBIA UNIVERSITY

OF SCIENCE AND TECHNOLOGY

FACULTY OF COMPUTING AND INFORMATICS

DEPARTMENT OF COMPUTER SCIENCE

QUALIFICATION: BACHELOR OF COMPUTER SCIENCE	
QUALIFICATION CODE: 07BACS	**LEVEL:** 7
COURSE: Computer Forensics	**COURSE CODE:** CFR712S
DATE: June 2019	**SESSION:** 1
DURATION: 3 hours	**MARKS:** 100

FIRST OPPORTUNITY EXAMINATION QUESTION PAPER	
EXAMINER(S)	**MR. ISAAC NHAMU**
MODERATOR:	**DR. AMELIA PHILLIPS**

THIS QUESTION PAPER CONSISTS OF 4 PAGES
(Excluding this front page)

INSTRUCTIONS

1. Answer ALL the questions.
2. Write clearly and neatly.
3. Number the answers clearly.
4. When answering questions you should be guided by the allocation of marks in [ ]. Do not give too few or too many facts in your answers.

PERMISSIBLE MATERIALS

1. Non programmable Scientific Calculator.

Question 1

Outline the functions of the following as they relate to digital forensics? [10]

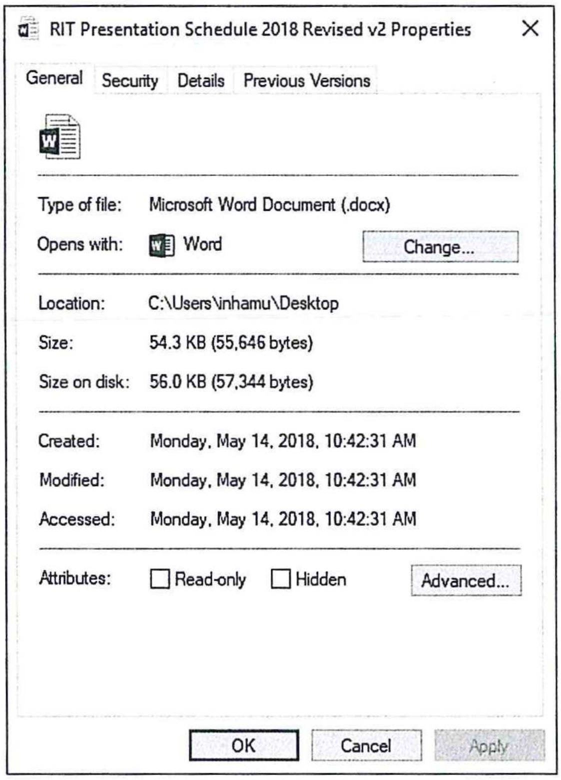
i. Hex editor
ii. Registry editor
iii. Steganalysis
iv. Wireshark
v. Data carving

Question 2

a. Identify which operating system is associated with each of the following file systems and outline one advantage each one brings to digital forensics.

   i. NTFS
   ii. Ext4
   iii. APFS [6]

b. Given the diagram below (Figure 2.1), explain the difference on the File size and the File size on disk. [2]



RIT Presentation Schedule 2018 Revised v2 Properties

Type of file: Microsoft Word Document (.docx)

Opens with: Word

Location: C:\Users\inhamu\Desktop

Size: 54.3 KB (55,646 bytes)

Size on disk: 56.0 KB (57,344 bytes)

Created: Monday, May 14, 2018, 10:42:31 AM

Modified: Monday, May 14, 2018, 10:42:31 AM

Accessed: Monday, May 14, 2018, 10:42:31 AM

Attributes: □ Read-only □ Hidden

Figure 2.1

c. What is the size of file slack space for the file shown in Figure 2.1 give your answer in KB? [2]

d. Outline how you would find the size of the sector for the Windows 10 machine in Figure 2.1 you can give your answer instructions in command line or GUI. [3]

e. Given that the size of the sectors in the file system shown in Figure 2.1 are 512 Bytes. Find the size of RAM slack created by the file. [4]

f. Why are RAM slack and file slack important to in Digital Forensics? [3]

Question 3

a. Explain what the "plain view doctrine" is when it comes to warrants and outline three criteria that must be met for it to hold. [5]

b. What is chain of custody? Why is it important in a digital forensic investigation? [2]

c. Give an example of each of the following types of digital forensics cases. For each example, state one source of digital evidence that could be obtained from such a case.

  i. Criminal case
  ii. Civil Case
  iii. Corporate case [3]

d. State five ways by which an investigator might conduct themselves unprofessionally while working on a case. [5]

Question 4

a. Give an example of a tool used in each of the following digital forensics tool categories. (Do not mention the same tool for every category. Each tool can only be mentioned once.)

  i. Acquisition
  ii. Validation and Verification
  iii. Extraction
  iv. Reconstruction
  v. Reporting [5]

b. State three advantages of using a GUI tool and two of using a command line tool when conduction a digital forensics investigation. [5]

Question 5

a. Compare Bitmap and metafile graphic images. [4]

b. What is the meaning of the following graphics terms?

   i. Pixel
   ii. Resolution [2]

c. What three factors determine the quality of raster images? [3]

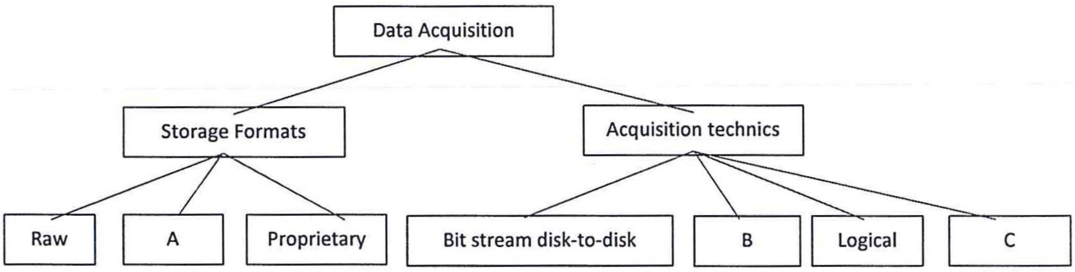
d. Give the full names for each of the following standard bitmap image formats.

   i. .png
   ii. .jpeg
   iii. .gif [3]

e. Outline three ways to detect steganography. [3]

Question 6

a. The diagram below describes some aspects of data acquisition. Identify the components marked A, B and C and point out one disadvantage of each of the identified components. [6]



b. With reference to Logical Acquisition and C; how do they differ? [2]

c. Differentiate between phishing and pharming. [2]

d. In Email investigations, what is an ESMTP? How does it help investigators? [2]

e. Outline three differences of POP3 and IMAP protocols with respect to digital forensics investigations? [3]

Question 7

A pharmaceutical company began receiving complaints from its representatives in certain geographical areas that sales of normally high volume drugs were slowing down considerably. The company's internal security department, as well as the security departments of its major distributors, began an investigation. The results of the investigations led the security professionals to believe a significant amount of the company's product was being diverted from foreign countries into the United States and sold through smaller distributors who specialized in sales to locally, privately owned pharmacies and dispensaries within nursing homes. The diversion activities were immediately reported to the local authorities in the regions, as well as to the FDA. An investigation was immediately launched and millions of dollars of diverted drugs and repackaging equipment was seized from several locations, including the warehouses of fully licensed pharmaceutical distributors. Along with the diverted product, the computers and other electronic equipment were also seized.

Adapted from https://evestigate.com/digital-forensics-case-studies/

Outline how you would carry out a forensically sound investigation of the case from start to end.

[15]

<<<<<<<<<<<< END >>>>>>>>>>>>>