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: July 2019	**SESSION: 2**
DURATION: 3 hours	**MARKS:** 100

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

THIS QUESTION PAPER CONSISTS OF 3 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

a. Distinguish between the following? [4]

   i. Digital forensics and data recovery

   ii. Digital forensics and computer forensics

b. Outline five steps/phases that could be followed in a typical Digital/Computer forensics investigation process and briefly describe what happens at each step? [10]

c. Give an example of each of the following digital forensics investigation cases.

   i. Criminal case

   ii. Corporate case

   iii. Civil case [3]

d. With reference question 1 c. above describe a case that might involve at least two of the above cases. Give reasons why you think the case covers two areas. [3]

Question 2

Describe five types of ethical standards required of a digital forensic investigator. [10]

Question 3

a. State one GUI and one CLI computer forensics tool you know. [2]

b. State a subfunction for each of the five major categories of computer forensics tools. [5]

c. Give three examples of computer forensics hardware tools. [3]

Question 4

Nowadays HDDs are being slowly replaced by SSDs as storage media. With regards to computer forensics, answer the following questions.

a. Expand the abbreviations HDD and SSD. [2]

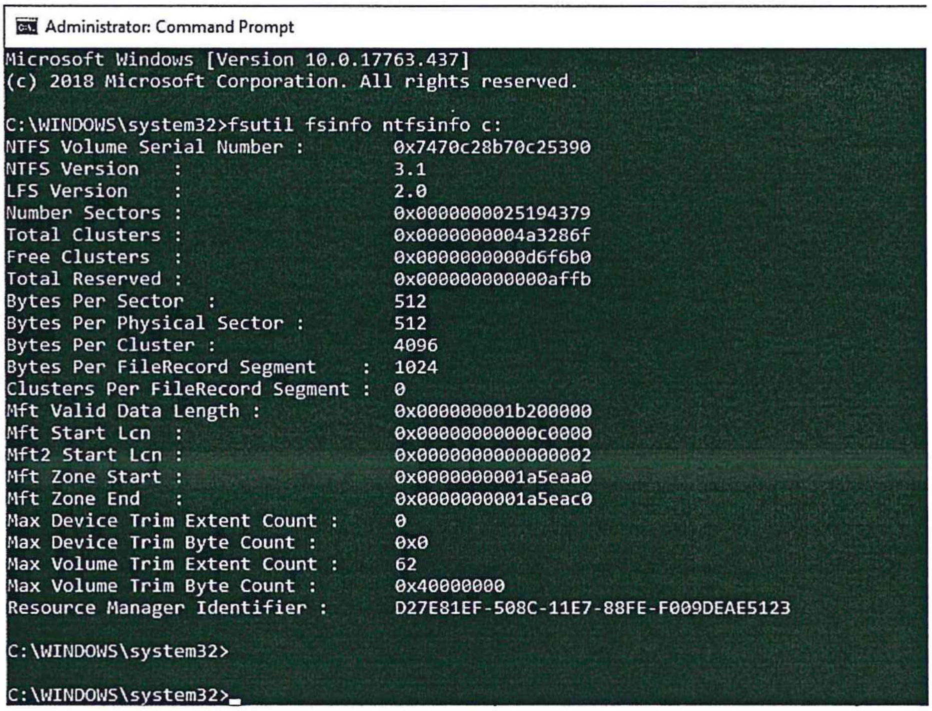
b. Outline what effect SSDs have on the computer forensics process as compared to HDDs. [8]

Question 5

a. Distinguish the following terms that relate to residual data. [6]

  i. Slack space
  ii. Free Space
  iii. Unallocated space

b. You are given a screenshot (Figure 5.1) of query that was executed on a Windows 10 machine.



Administrator: Command Prompt

```
Microsoft Windows [Version 10.0.17763.437]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>fsutil fsinfo ntfsinfo c:
NTFS Volume Serial Number :       0x7470c28b70c25390
NTFS Version   :                  3.1
LFS Version    :                  2.0
Number Sectors :                  0x0000000025194379
Total Clusters :                  0x000000004a3286f
Free Clusters  :                  0x00000000000d6f6b0
Total Reserved :                  0x000000000000affb
Bytes Per Sector  :               512
Bytes Per Physical Sector :       512
Bytes Per Cluster :               4096
Bytes Per FileRecord Segment    : 1024
Clusters Per FileRecord Segment : 0
Mft Valid Data Length :           0x000000001b200000
Mft Start Lcn  :                  0x00000000000c0000
Mft2 Start Lcn :                  0x0000000000000002
Mft Zone Start :                  0x0000000001a5eaa0
Mft Zone End   :                  0x0000000001a5eac0
Max Device Trim Extent Count :    0
Max Device Trim Byte Count :      0x0
Max Volume Trim Extent Count :    62
Max Volume Trim Byte Count :      0x40000000
Resource Manager Identifier :     D27E81EF-508C-11E7-88FE-F009DEAE5123

C:\WINDOWS\system32>

C:\WINDOWS\system32>_
```

Figure 5.1

  i. Using Figure 5.1 identify what the sector and cluster sizes are in Bytes as well as in KB. [2]

  ii. Given that a file of size 102.25KB is stored on this windows system. Find the size of File slack as well RAM slack that is created by storing such a file. [7]

Question 6

a. Distinguish between Bitmap and Vector images by stating two properties of each of these image types. [4]

b. What is a Raw File Format? [1]

c. Identify three things you would consider when choosing a computer forensics tool be it a hardware or software tool. [3]

d. Explain the difference between "live acquisition" and "post mortem acquisition". [2]

Question 7

a. Outline at least four features that distinguish computer forensics from other forensic science disciplines. [8]

b. With respect to computer forensics how do you authenticate the originality of digital evidence? [2]

Question 8

a. Give an example of each of the following formats used for data acquisition.

    a. Raw format

    b. Proprietary format

    c. Advanced Forensics Format [3]

b. Why would you choose to store acquired images as Raw Format? Give and explain two reasons. [4]

c. Why would you choose to store acquired images as Proprietary Format? Give and explain two reasons. [4]

d. Read the following scenario involving the company Global Digital Forensics (GDF) investigators and answer the questions below that deal with data acquisition concerning the case.

> A large accounting firm was hired to audit certain activities related to loans to individuals on the board of directors of a medium size, publicly traded bank (the "Bank"). During the audit, the auditors needed to examine several computer systems used by certain Bank employees, as well as by certain board members. GDF's digital forensic examiners were immediately dispatched and sent in to arrange for the forensic analysis of the computer systems and to search for corroborating evidence in support of the audit team's suspicions and findings. The systems GDF analysts forensically analyzed included laptop computers issued to managers in the loan origination department and desktop systems used by managers and board members. Email (Exchange) servers, as well as voicemail systems, were examined.

e. From the four digital investigation methods decide what type of method would be used in this scenario to acquire the data and give reasons for your choice of the method. [4]

<<<<<<<<<<<< **END** >>>>>>>>>>>