NAMIBIA UNIVERSITY
OF SCIENCE AND TECHNOLOGY

FACULTY OF COMPUTING AND INFORMATICS

DEPARTMENT OF COMPUTER SCIENCE

QUALIFICATION: BACHELOR OF COMPUTER SCIENCE (SYSTEMS ADMINISTRATION)	
QUALIFICATION CODE: 07BACS	**LEVEL:** 7
COURSE: Computer Forensics	**COURSE CODE:** CFR712S
DATE: July 2022	**SESSION:** 2
DURATION: 3 hours	**MARKS:** 100

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

THIS EXAM QUESTION PAPER CONSISTS OF 5 PAGES

(Excluding this front page)

INSTRUCTIONS

1. Answer ALL the questions on the answer scripts.
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 calculator.

Section A (Multiple Choice) **[30 marks]**

1. Graphics files stored on a computer can't be recovered after they are deleted
   A. True
   B. False

2. Areal density refers to which of the following?
   A. Number of bits per disk
   B. Number of bits per partition
   C. Number of bits per square inch of a disk platter
   D. Number of bits per platter

3. Hashing, filtering, and file header analysis make up which function of digital forensics tools?
   A. Validation and verification
   B. Acquisition
   C. Extraction
   D. Reconstruction

4. The reconstruction function is needed for which of the following purposes? (Choose three.)
   A. Re-create a suspect drive to show what happened
   B. Create a copy of a drive for other investigators.
   C. Recover file headers.
   D. Re-create a drive compromised by malware.

5. Hash values are used for which of the following purposes? (Choose two)
   A. Determining file size
   B. Filtering known good files from potentially suspicious data
   C. Reconstructing file fragments
   D. Validating that the original data hasn't changed

6. The verification function does which of the following?
   A. Proves that a tool performs as intended
   B. Creates segmented files
   C. Proves that two sets of data are identical via hash values
   D. Verifies hex editors

7. Which of the following is true of most drive-imaging tools? (Choose two.)
   A. They perform the same function as a backup.
   B. They ensure that the original drive doesn't become corrupt and damage the digital evidence.
   C. They create a copy of the original drive.
   D. They must be run from the command line.

8. A log report in forensics tools does which of the following?
   A. Tracks file types
   B. Monitors network intrusion attempts
   C. Records an investigator's actions in examining a case
   D. Lists known good files

9. The process of converting raw images to another format is called which of the following?
    A. Data conversion
    B. Transmogrification
    C. Transfiguring
    D. Demosaicing

10. Each type of graphics file has a unique header containing information that distinguishes it from other types of graphics files.
    A. True
    B. False

11. Bitmap (.bmp) files use which of the following types of compression?
    A. WinZip
    B. Lossy
    C. Lzip
    D. Lossless

12. What methods do steganography programs use to hide data in graphics files? (Choose two.)
    A. Insertion
    B. Substitution
    C. Masking
    D. Carving

13. Some clues left on a drive that might indicate steganography include which of the following? (Choose all that apply.)
    A. Multiple copies of a graphics file
    B. Graphics files with the same name but different file sizes
    C. Steganography programs in the suspect's All Programs list
    D. Graphics files with different timestamps

14. The likelihood that a brute-force attack can succeed in cracking a password depends heavily on the password length.
    A. True
    B. False

15. Which of the following is an example of a written report?
    A. A search warrant
    B. An affidavit
    C. Voir dire
    D. All of the above

16. When writing a report, what's the most important aspect of formatting?
    A. A neat appearance
    B. Size of the font
    C. Clear use of symbols and abbreviations
    D. Consistency

17. Automated tools help you collect and report evidence, but you're responsible for doing which of the following?
    A. Explaining your formatting choices
    B. Explaining the significance of the evidence
    C. Explaining in detail how the software works
    D. All of the above

18. A forensic image of a VM includes all snapshots.
    A. True
    B. False

19. In order to be legally defensible, methods used in the recovery of data must ensure that
    A. The original evidence was not altered
    B. No data was added to the original
    C. No data was deleted from the original
    D. All of the above

20. In a forensics context, hidden information about files and folders is called
    A. Artifact data
    B. Metadata
    C. Archive data
    D. Read-only data

21. You can view e-mail headers with notepad with all popular e-mail clients?
    A. True
    B. False

22. To protect original data from any alteration, you _____ (Choose two)
    A. Use gloves when working with the hard drive
    B. Make a forensic copy of the original data
    C. Do your forensic work as quickly as possible
    D. Use the operating system to copy all relevant files

Section B (Structured Questions) **[70 marks]**

Question 1

Explain how the following are useful in computer forensics: (**Please note the question is does NOT say *define***)

i. Dictionary attack

ii. Irfan View

iii. KFF from AccessData

iv. Deposition bank

v. NIST NSRL [10]

Question 2

a. Compare a bitmap to a vector image files. [4]

b. What is carving? Give two technics that be used for carving. [4]

c. Name two ways is the EXIF file format helpful when conducting a digital a forensic investigation. [2]

Question 3

Consider investigating an Email abuse crime at government organisation. Outline the steps you would take to conduct such an investigation. [10]

Question 4

a. List two features that NTFS has that FAT does not. [2]

b. What doe MFT stand for? What is its purpose? [2]

c. You are given the following information about a Windows 10 machine.

Cluster size = 1024B, 8 Sectors make up a cluster

Given that a file's size is given by extracting the last 5 numbers of you student number (e.g., if your student number is 218067546 the file size will be 67546Bytes). Given also that the file is stored in the Windows 10 machine above. Find the size of File slack as well RAM slack that is created by storing such a file (Please show all your work). [6]

Question 5

a. State any three ways by which professional conduct can be breached by an investigator. [3]

b. List three necessary components of a search warrant. [3]

c. List three items that should be in an evidence custody form. [3]

d. Why should evidence media be write protected. [1]

Question 6

a. Describe a scenario where you would use these types of acquisitions of digital evidence:
   i. Static
   ii. Sparse [4]

b. Describe two concerns you should be aware of with remote acquisitions. [2]

c. Give two actions you would consider to be good practice when making images of a suspect's drive in a critical investigation. Justify your answers. [4]

Question 7

a. With reference to the analysis phase of digital forensics; what is scope creep? [2]

b. What causes scope creep? Give two reasons. [2]

c. Describe an advantage to the prosecution of scope creep. [2]

d. Using an example of the bit stream 01001001 explain how a Left shift by 1 bit shift works. [2]

e. Explain the concept of block-wise hashing. [2]

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