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: June 2022	**SESSION:** 1
DURATION: 3 hours	**MARKS:** 100

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

THIS EXAM QUESTION PAPER CONSISTS OF 7 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) **[35 marks]**

1. 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

2. When validating the results of a forensic analysis, you should do which of the following? (Choose two.)
   A. Calculate the hash value with two different tools.
   B. Use a different tool to compare the results of evidence you find.
   C. Repeat the steps used to obtain the digital evidence, using the same tool, and recalculate the hash value to verify the results.
   D. Use a command-line tool and then a GUI tool.

3. When you carve a graphics file, recovering the image depends on which of the following skills?
   A. Recovering the image from a tape backup
   B. Recognizing the pattern of the data content
   C. Recognizing the pattern of the file header content
   D. Recognizing the pattern of a corrupt file

4. When investigating graphics files, you should convert them into one standard format.
   A. True
   B. False

5. Digital pictures use data compression to accomplish which of the following goals? (Choose two.)
   A. Save space on a hard drive.
   B. Provide a crisp and clear image.
   C. Eliminate redundant data.
   D. Produce a file that can be e-mailed or posted on the internet.

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

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

8. A JPEG file uses which type of compression?
   A. Winzip
   B. Lossy
   C. Lzip
   D. Lossless

9. A JPEG file is an example of a vector graphic.
   A. True
   B. False

10. Which of the following is true about JPEG and TIF files?
    A. They have identical values for the first 2 bytes of their file headers.
    B. They have different values for the first 2 bytes of their file headers.
    C. They differ from other graphics files because their file headers contain more bits.
    D. They differ from other graphics files because their file headers contain fewer bits.

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

12. Some clues left on a drive that might indicate steganography include which of the following? (Choose three.)
    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

13. E-mail headers contain which of the following information? (Choose all that apply.)
    A. The sender and receiver e-mail addresses
    B. An ESMTP number or reference number
    C. The e-mail servers the message travelled through to reach its destination
    D. The IP address of the receiving server
    E. All of the above

14. What's the main piece of information you look for in an e-mail message you're investigating?
    A. Sender or receiver's e-mail address
    B. Originating e-mail domain or IP address
    C. Subject line content
    D. Message number

15. In Microsoft Outlook, what are the e-mail storage files typically found on a client computer?
    A. .pst and .ost
    B. Res1.log and res2.log
    C. Pu020102.db
    D. .evolution

16. When searching a victim's computer for a crime committed with a specific e-mail, which of the following provides information for determining the e-mail's originator? (Choose two.)
    A. E-mail header
    B. Username and password
    C. Firewall log
    D. All of the above

17. All e-mail headers contain the same types of information.
    A. True
    B. False

18. When you access your e-mail, what type of computer architecture are you using?
    A. Mainframe and minicomputers
    B. Domain
    C. Client/server
    D. None of the above

19. Router logs can be used to verify what types of e-mail data?
    A. Message content
    B. Content of attached files
    C. Tracking flows through e-mail server ports
    D. Finding blind copies

20. On a UNIX-like system, which file specifies where to save different types of e-mail log files?
    A. maillog
    B. /var/spool/log
    C. syslog.conf
    D. log

21. What information is not in an e-mail header? (Choose two.)
    A. Blind copy (bcc) addresses
    B. Internet addresses
    C. Domain name
    D. Contents of the message
    E. Type of e-mail server used to send the e-mail

22. Which of the following types of files can provide useful information when you're examining an e-mail server?
    A. .dbf files
    B. .emx files
    C. .log files
    D. .slf files

23. Internet e-mail accessed with a Web browser leaves files in temporary folders.
    A. True
    B. False

24. When confronted with an e-mail server that no longer contains a log with the date information you need for your investigation, and the client has deleted the e-mail, what should you do?
    A. Search available log files for any forwarded messages.
    B. Restore the e-mail server from a backup.
    C. Check the current database files for an existing copy of the e-mail.
    D. Do nothing because after the file has been deleted, it can no longer be recovered.

25. Which of the following is a current protocol standard for e-mail?
    A. ESMTP
    B. MIME
    C. SMTP
    D. HTML

Section B (Structured Questions) **[65 marks]**

Question 1

Explain how the following are useful in computer forensics (**Please note the question is NOT just asking you to define):**

a. Rainbow tables
b. Affidavit/declaration
c. Hash values
d. dd command in Linux
e. Hexeditor [10]

Question 2

a. Distinguish between the following when it comes to acquisition of images in Digital Forensics:
    i. Digital evidence and physical evidence,
    ii. Proprietary formats and advanced forensics formats
    iii. Logical and sparse acquisition [6]

b. State four factors you would consider when determining the best method of acquiring and image for digital forensics investigation purposes. [4]

Question 3

a. In the **Reporting** category of digital forensics tools identify and describe any two sub-function of this stage and one computer forensic tool that could be used for this. [5]

b. State five factors you would take into consideration when choosing a computer forensic tool to purchase for and organization. [5]

Question 4

a. Why is it important for a digital forensics investigator to know about computer file systems? [2]

b. What happens when you delete a file in a computer using the FAT file system? [2]

c. What is the difference between RAM Slack and File Slack? [1]

d. Given that a file has sectors of size 512B and that there are 4 sector per cluster. Find the size of File slack and RAM slack created by storing a file of size **XXXXB** in a Windows system (where XXXX is the last four numbers of your student number e.g. if your student number is 200949492 the file will be of size 9492B. [5]

Question 5

a. Fig 1.1 shows a document called Test 2.txt that has been in WinHex. A Left bit shift by 1 bit is performed on Test 2.txt as shown in Fig 1.2 resulting in data as shown in Fig 1.3. using your Knowledge of hex to binary conversion and bit shifting show that the Left bit shift by 1 on the first Character in the test 2 file i.e. C in ASCII and 45 in Hex resulted in the character with Hex value 86. [5]

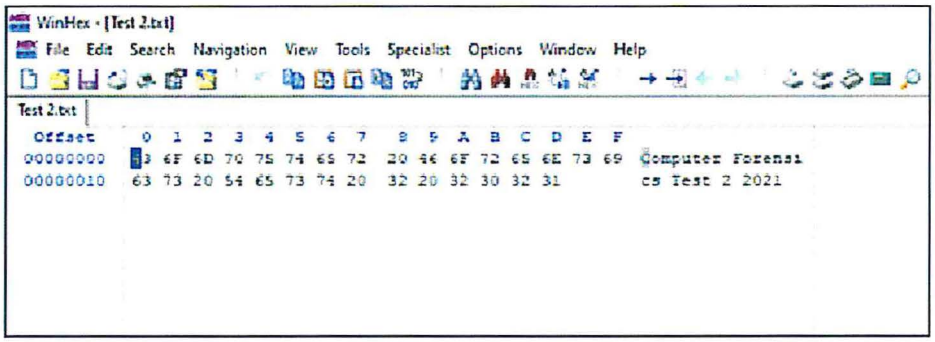

Figure 1.1

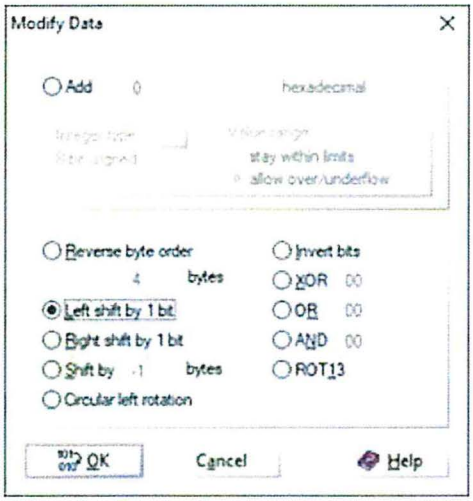

Figure 1.2

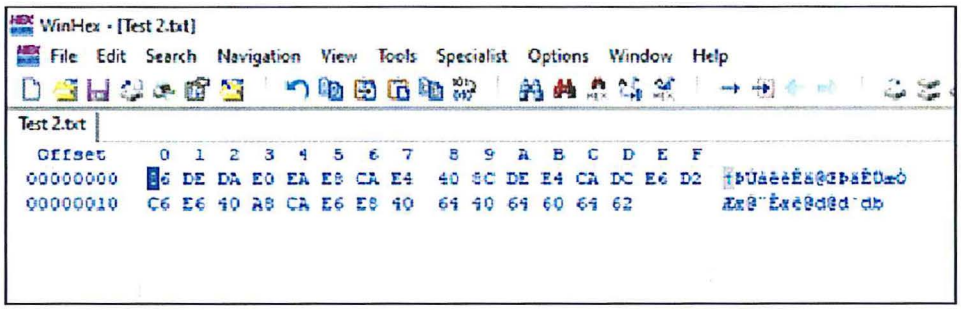

Figure 1.3

b. Match the terms in Table 1 with their corresponding definitions from Table 2. [10]

1	Drive slack
2	Sector
3	Cluster
4	Partition
5	Unallocated space

Table 1

1	Remnant area at the end of a file
2	Smallest unit that can be accessed on a disk
3	Fixed blocks of data such as 1024 bytes
4	Space not used to store an active file
5	Unused space between the end of a file and the end of a sector
6	A logical drive

Table 2

Question 6

Outline any five anti-forensics techniques that are used by criminals. For each technique outlined give one solution that can be used to overcome this technique. [10]

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