Strathmore
UNIVERSITY

SCHOOL OF COMPUTING AND ENGINEERING SCIENCES (SCES)
BACHELOR OF COMPUTER NETWORKS AND SECURITY
END OF SEMESTER EXAMINATION
CNS 4103 : DIGITAL FORENSICS

DATE:29th July 2024 Time: 10:30-12:30 Hours

Instructions

1. This examination consists of **FIVE** questions.
2. Answer **Question ONE (COMPULSORY)** and any other **TWO** questions.

Question One

i. 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

ii. A JPEG file uses which type of compression?

- **a.** WinZip
- **b.** Lossy
- **c.** Lzip
- **d.** Lossless

iii. What information is *not* in an e-mail header? (Choose all that apply.)

- **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

iv. Building a business case can involve which of the following?

a. Procedures for gathering evidence

b. Testing software

c. Protecting trade secrets

d. All of the above

v. The manager of a digital forensics lab is responsible for which of the following? (Choose all that apply.)

a. Making necessary changes in lab procedures and software

b. Ensuring that staff members have enough training to do the job

c. Knowing the lab objectives

d. None of the above

vi. What is the space on a drive called when a file is deleted? (Choose all that apply.)

a. Disk space

b. Unallocated space

c. Drive space

d. Free space

vii. What does MFT stand for?

viii. The reconstruction function is needed for which of the following purposes? (Choose all that apply.)

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.

ix. 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

x. In testing tools, the term “reproducible results” means that if you work in the same lab on the same machine, you generate the same results. True or False?

xi. The National Software Reference Library provides what type of resource for digital forensics examiners?

a. A list of digital forensics tools that make examinations easier

b. A list of MD5 and SHA1 hash values for all known OSs and applications

c. Reference books and materials for digital forensics

d. A repository for software vendors to register their developed applications

xii. Which Registry key contains associations for file extensions?

a. HFILE_CLASSES_ROOT

b. HKEY_CLASSES_ROOT

c. HFILE_EXTENSIONS

d. HKEY_CLASSES_FILE

xiii. Large digital forensics labs should have at least _____ exits.

xiv. What term refers to labs constructed to shield EMR emissions?

xv. Define the term digital forensics from your own understanding and explain two qualifications a forensics investigator must have.

(5 Marks)

Total (20 Marks

Question Two

i. Digital forensics tools provide standard functionality. Discuss the main functionalities of digital forensics tools with special focus on the Autopsy tool from Sleuth kit clearly stating their purpose. (10 Marks)

ii. Differentiate between verification of a digital forensics tool and validation of a tool using an example. (2 Marks)

iii. Compare and contrast two major differences between NTFS file system and FAT file system. Explain one way in which each makes it both easier and difficult for forensics investigators to examine a disk. (8 Marks)

Total (20 Marks)

Question Three

i. Acquiring digital evidence is an important step in the forensics process. Usually an image of the computer disk is taken for analysis. Explain the following about a forensics image:

a. The difference between a forensics image and a copy of the disk.

b. Some of the areas on disk where criminals could potentially hide data without it being visible to the operating system.

c. Ways in which the disk can be prevented from being tampered with.

(6 Marks)

ii. Memory forensics is a one of the least discussed types of forensics but none the less quite important aspect of digital forensics. outline the following:

a. One reason that makes memory forensics challenging for investigators. (1 Mark)

b. One tool that can be used to analyse evidence from memory. (1 Mark)

c. One crime that can be investigated using memory forensics. (1 Mark)

iii. Email forensics are quite an important technique used in digital forensics because a lot of communication happens on email. Explain the following about email forensics:

a. Two major challenges while conducting email forensics. (2 Marks)

b. One way in which evidence from email can be corroborated (i.e. additional ways in which evidence from email can be supported.) (2 Marks)

c. Briefly discuss what email header analysis is including the major components that need to be examined. (6 Marks)

d. Name one crime that can be investigated using email forensics. (1 Mark)

Total (20 Marks)

Question Four

i. List three different digital crimes that the Kenya Computer Misuse and Cyber Crimes act of 2018 defines. (3 Marks)

ii. You have been asked to investigate the case of a suspect in a drug trafficking case has been using websites to browse through illegal activities and even downloaded some images and documents from these websites. You have acquired an image of his disk and would like to investigate his browsing activities. Explain four sources of evidence that you might find from his browser. (8 Marks)

iii. You have been asked to prepare a proposal for a new digital forensics lab at Strathmore University to support both teaching, research and to be used commercially to conduct corporate investigations for clients. Outline the following:

iv. At least one software that the lab should have

a. One physical security feature the lab should have

b. One role and duty of the manager of the lab

c. One type of certification that the lab should have.

d. One important security procedure that must be observed in the lab.

(5 Marks)

v. Explain any two steps in the digital forensics process and their importance. (4 Marks)

Total (20 Marks)

Question 5

i. Discuss three challenges that digital forensics examiners face when investigating cases and how they can be overcome. (6 Marks)

ii. Locards exchange principle is a fundamental principle in digital forensics. It states, "When 2 bodies come into contact with each other, they leave a trace of each other on each other". With this in mid, what are the key areas you would find evidence of the following activities that you are investigating on a windows machine.

   a. A colleague has been visiting inappropriate websites using Mozilla Firefox; you need to view his browser history.
   b. A file contained sensitive data was downloaded onto a machine, viewed and then deleted from disk. The recycle bin was also emptied not to leave a trace of the file.
   c. A steganography tool was installed to hide a message in a graphics file by a suspected drug trafficker and later uninstalled.

(Si6 Marks)

iii. When writing a digital forensics report, it is crucial to be very clear and objective. Discuss three major components of a digital forensics report and what they contain. (6 Marks).

iv. What are the two different numbering systems used in a digital forensics report? (2 Marks)

Total (20 Marks)