FINAL
ALTERNATIVE ASSESSMENT

(COVER PAGE)

Session : **April 2022**

Programme : Diploma In Computer Science (DCS)

Course : DCS2112: Digital Forensics

Date of Examination : 05 August 2022(Friday)

Time : 12.00pm – 02.30pm Reading Time : Nil

Duration : 02 hours 30 minutes

Note: 30 minutes is added into the duration of the examination to factor in any connectivity matters and for you to scan and upload your scripts

Special Instructions :

Answer all the questions. All questions carry equal marks.

Material permitted :

Non-Programmable Scientific Calculator

Materials provided :

Nil

Examiner(s) : Asvhini Subramaniam

Chief Moderator : Victor Raj Kolintiar

This paper consists of 7 printed pages, including the cover page

DIPLOMA IN COMPUTER SCIENCE PROGRAMME (DCS)
DCS2112: DIGITAL FORENSICS
FINAL ALTERNATIVE ASSESSMENT: APRIL 2022 SESSION

SECTION A

Instructions: This section consists of **TWENTY (20)** multiple-choice questions. Answer **TWENTY (20)** questions provided. All questions carry equal marks.

1. Most witnesses are 'witnesses of fact', they can only provide evidence on what they saw, did or heard. Most importantly, they cannot give their opinion on any of the matters about which they give evidence. By contrast, _____ witness is specifically called to give their opinion on a particular matter related to forensic investigation in court.

   A. cybercrime
   B. expert
   C. best
   D. analyst

2. Which of the following is/are computer forensics investigation technique?
   A. Cross-drive analysis
   B. Live analysis
   C. Deleted files
   D. All of the above

3. Volatile data found in which part of the computer?

   A. Registry
   B. Cache
   C. Random Access Memory (RAM)
   D. All of the above

4. The _____ evidence rule specifies that evidence, such as a facsimile copy, will be not admissible if an original document exists and can be obtained.

   A. best
   B. circumstantial
   C. direct
   D. hearsay

5. The GDFM takes the perspective of the digital forensics practitioner showing the core principles and processes involved for a specific case divided into the _____ phase and the analysis phase.

   A. examination
   B. collection
   C. identification
   D. preservation

6. Chat and instant message conversations are stored on computers in _____.

   A. Hard disk
   B. Random Access Memory
   C. Wintex
   D. Slack space

7. Google Chrome web browser introduce _____ to keep the privacy of the end users.

   A. Private Browsing
   B. Incognito Mode
   C. Save Browsing
   D. Offline Mode

8. When the Internet History file has been deleted, **_____** may still provide information about what Web sites the user has visited.
   A. Sessions
   B. Cookies
   C. Metadata
   D. User profiles

9. **_____** is an email investigation technique that's used when the location of a suspect or cybercriminal is unknown. In this technique, the investigators send an email that contains a http: "<img src>" tag to the suspect.

   A. Bait tactic
   B. Email Header Analysis
   C. Sender Mailer Fingerprinting
   D. Software Embedded Identifiers

10. From the following spam mail header, identify the host IP that sent this spam.

    From alisa@gmail.com Sat Aug 30 15:08:35 2022
    Received: from desertoasis.ie.cu.edu.eg (desertoasis [102.184.35.62]) by eng.cu.edu.eg (41.31.5.0/41.31.5.0) with ESMTP id fVR9RAP23061 for ; Sat, 30 Aug 2022 13:07:40 +0200 (EGYP)
    Received: from mydomain.com (stu482510.cmail.com [197.32.11.120]) by desertoasis.ie.cu.edu.eg (41.32.3.0/41.32.3.0)
    with SMTP id fVR9MXwZ018431 for ; Sat, 30 Aug 2022 15:05:13 +0200 (EGYP)
    Message-Id: > 1630386313000.fVR9MXwZ018431@ desertoasis.ie.cu.edu.eg
    From: "german international hostel"
    To: "Claire"
    Subject: CAIRO (HIVE HOSTEL) ROOM PACKAGE
    Date: Sat, 30 Aug 2022 15:08:35 +0200 MIME-Version: 1.0
    X-Priority: 3 X-MSMail-
    Priority: Normal
    Reply-To: "german international hostel"

    A. 41.31.5.0
    B. 41.32.3.0
    C. 197.32.11.120

D. 102.184.35.62

11. Which of the following compression standards recommended by a NIST for fingerprint.

A. Run-length coding
B. Wavelet scalar quantization
C. JPEG compression
D. Huffman coding

12. Listed below are the several anti-forensic techniques that go undetected in a threat, malware detection tool or security analysis EXCEPT

A. Data hiding
B. Artifact wiping
C. Trail obfuscation
D. Code Analysis

13. Which of the following program is run to examine network traffic?

A. NET dump
B. TCP dump
C. Slack dump
D. Core dump

14. An Android device's encrypted data can be wiped remotely using _____.

A. Google Sync
B. iCloud
C. Search My Sync
D. Find my phone service

15. Which of the following is the definition of file header?

A. Synonymous with the file extension
B. A 128-bit value that is unique to a specific file based on its data
C. A unique set of characters following the file name that identifies the file type
D. A unique set of characters at the beginning of a file that identifies the file type

16. The _____ technique is required to physically remove the non-volatile memory chip from the target mobile device that is severely damaged and/or cannot be turn-on for mobile forensic investigation.

A. brute-force
B. chip-off
C. injection
D. pens-and-traps

17. The computer program which provides cryptographic privacy and authentication for data communication, based on public key encryption algorithm is _____

A. TGEP

B. GPP
C. PGP
D. CGE

18. Choose the commonly used hashing algorithms to secure digital evidences.

I. MD-5
II. HMAC
III. RIPE-MD
IV. SHA-1

A. I, II, III
B. II, III, IV
C. I, II, IV
D. I, II, III, and IV

19. Email clients have own file formats or extension for storing email. Choose the file extension of email client of Outlook Express.

I. .dbx
II. .abi
III. .pst
IV. .eml

A. I and IV
B. II and IV
C. I and II
D. I and III

20. Identify the name of one of the two logical root keys that reside in the system hard drive of the Windows Registry.

I. HKEY_LOCAL_MAC
II. HKEY_LOCAL_SYSTEM
III. HKEY_LOCAL_MACHINE
IV. HKEY_USERS

A. I and III
B. II and III
C. I and IV
D. II and IV

SECTION B

Instructions: This section consists of **THREE (3)** questions. Answer all the questions. All questions carry equal marks.

Question 1

(a) Discuss the following acquisition methods with an appropriate example case/evidence file:
(i) Bit stream disk-to-image file
(ii) Bit stream disk-to-disk

(10 marks)

(b) List **FIVE (5)** common cases that required computer specialists to conduct forensics investigation in an organization.

(5 marks)

(c) Discuss the method approach differences between static analysis vs live analysis.

(5 marks)
(Total: 20 marks)

Question 2

(a) Malware consists of programming designed to disrupt or deny operations, gather information that results in loss of privacy or exploitation, gain unauthorized access to system resources and other abusive behavior.
Briefly discussed any **FIVE (5)** symptoms of an infected system.

(10 marks)

(b) Discuss digital evidence that comes under categories of computer-generated records and computer-stored records. Provide your example for this discussion.

(8 marks)

(c) Explain the advantages of obtaining digital hash of your evidence.

(2 marks)
(Total: 20 marks)

Question 3

(a) The classification system provides a framework for forensic examiners to compare the extraction methods used by different tools to acquire data.
State **FIVE (5)** level of tool classification system used in mobile forensics as per guideline given by National Institute of Standards and Technology (NIST).

(5 marks)

(b) Briefly explain **THREE** (3) challenges faced by email forensics investigators.

(6 marks)

(c) Digital evidence must be handle systematically so that it is presentable in court for proving. State and describe any **THREE (3)** characteristics of digital evidence that are admissible in a court of law with appropriate example(s).

(9 marks)

(Total: 20 marks)

~THE END~

DCS2112 (F)/ Apr2022 Session/ formatted