FINAL
ALTERNATIVE ASSESSMENT

(COVER PAGE)

Session	:	**August 2021**
Programme	:	Diploma in Computer Science (DCS)
Course	:	**DCS2112: Digital Forensics**
Date of Examination	:	4 December 2021 (Saturday)
Time	:	8.00am – 10.30am Reading Time : Nil
Duration	:	2 Hours 30 Minutes

Special Instructions :

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

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

Material permitted :

Non-Programmable Scientific Calculator

Materials provided :

Nil

Examiner(s)	:	**Asvhini Subramaniam,** Andrew Ho
Chief Moderator	:	Usha Jayahkudy

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

DIPLOMA IN COMPUTER SCIENCE PROGRAMME (DCS)
DCS2112: DIGITAL FORENSICS
FINAL ALTERNATIVE ASSESSMENT: AUGUST 2021 SESSION

SECTION A (40 Marks)

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

1. Actions taken to secure and collect digital evidence should not affect the _____ of that evidence.

   A. portion
   B. content
   C. confidentiality
   D. integrity

2. File _____ is a process used in computer forensics to extract data from a disk drive or other storage device without the assistance of the file system.

   A. carving
   B. clustering
   C. partitioning
   D. recovery

3. Following are related to Linux file systems **EXCEPT**

   A. JFS
   B. NTFS
   C. ReiserFS
   D. XFS

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. 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. expert
   B. digital
   C. cybercrime
   D. Analyst

6. Which binary coding is used most often for e-mail purposes?

   A. IMAP
   B. MIME
   C. SMTP
   D. Uuencode

7. Which file is required to extract data for forensic analysis from the Microsoft Edge web browser?

   A. WebCacheV01.dat
   B. Index.dat
   C. History.plist
   D. Cache.db

8. The legal process leading to a trial with the purpose of proving criminal or civil liability.

   A. industrial espionage
   B. Private investigation
   C. Public investigation
   D. Litigation

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 ali007@cmail.com Fri Aug 31 13:08:31 2021
    Received: from desertoasis.ie.cu.edu.eg (desertoasis [102.184.33.62]) by eng.cu.edu.eg (41.31.5.0/41.31.5.0) with ESMTP id fVR9RAP23061 for ; Tue, 31 Aug 2021 13:07:40 +0200 (EGYP)
    Received: from mydomain.com (stu482510.cmail.com [197.32.11.124]) by desertoasis.ie.cu.edu.eg (41.32.3.0/41.32.3.0)
    with SMTP id fVR9MXwZ018431 for ; Tue, 31 Aug 2021 13:05:13 +0200 (EGYP)
    Message-Id: > 1630386313000.fVR9MXwZ018431@ desertoasis.ie.cu.edu.eg
    From: " egypt international hostel"
    To: "Claire"
    Subject: CAIRO (GIZA HOSTEL) ROOM PACKAGE
    Date: Tue, 31 Aug 2021 13:01:28 +0200 MIME-Version: 1.0
    X-Priority: 3 X-MSMail-
    Priority: Normal
    Reply-To: "egypt international hostel"

    A. 41.31.5.0
    B. 41.32.3.0

C. 197.32.11.124
D. 102.184.33.62

11. Nick, is required to export the emails for forensic investigation from an offline suspects' computer which uses the Microsoft Outlook Express email client. Followings are possible file formats he will be attained from this task **EXCEPT**

A. .DBX
B. .EMAIL
C. .IDX
D. .MBOX

12. When analyzing an email, Fabian found the following timestamp information:

1304327103

What is the actual day, month, year, and time if the timestamp was recorded in Malaysia GMT+8:00?

A. Monday, May 2, 2011 9:05:03 AM
B. Monday, May 2, 2011 5:05:03 PM
C. Monday, May 2, 2011 9:05:03 PM
D. Tuesday, May 3, 2011 5:05:03 AM

13. Digital forensic researchers use "**X**" to better analyze a particular malware's techniques and behaviors. "**X**" also provides actionable threat intelligence that can be shared within the digital forensic community to further improve a business organization's incident response and remediation strategies.

What is "**X**"?

A. Baseline
B. Big Data
C. Indicators of Compromise
D. Security metrics

14. Which of the following is the correct order of the Digital Forensics examination process?

A. Reporting -> Analysis -> Acquisition
B. Analysis -> Acquisition -> Reporting
C. Acquisition -> Analysis -> Reporting
D. Reporting -> Acquisition -> Analysis

15. Following tools that can be used by Kelly, who just starting to learn about network forensics investigation **EXCEPT**

A. Fiddler
B. TeamViewer
C. TCPdump
D. Wireshark

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. An investigation can only be carried out when _____.

    A. there is a suspicion that a crime has been committed
    B. a person has a criminal history
    C. a witness to an incident owns a mobile device
    D. when working within a 'high security' company

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. What are the names of the two paging files used in Windows 8?

    I. Swapfile.sys
    II. Pagefile.sys
    III. Virtualmem.sys
    IV. Pagingfile.sys

    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 (60 Marks)

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

Question 1

(a) List and explain any **FOUR (4)** challenges faced by a digital forensics professionals.
(8 marks)

(b) Forensics investigators often work as part of a team, known as the *investigations triad*. State and describe the **THREE (3)** disciplines involve in the investigation triad.
(6 marks)

(c) Additional precautionary steps should be measured in handling optical disc and magnetic disc evidence.

(i) Describe **THREE (3)** special precautions that should be strictly observed to avoid damaging the optical disc evidence.
(3 marks)

(ii) Describe **THREE (3)** special precautions that should be strictly observed to avoid damaging the magnetic disc evidence.
(3 marks)
(Total: 20 marks)

Question 2

(a) Data compression is the process of coding data from a larger form to a smaller form. Graphics files and most compression tools use one of two data compression schemes. Compare and contrast the **TWO (2)** compression schemes with an example utility program.
(10 marks)

(b) (i) Identify and discuss **FOUR (4)** anti-forensics techniques commonly used by cyber criminals to avoid and make digital forensics investigation difficult to be performed.
(8 marks)

(ii) State any **TWO (2)** fundamental techniques of malware forensics and analysis.
(2 marks)
(Total: 20 marks)

Question 3

(a) Digital evidence must be handle systematically so that it is presentable in court for proving. State and describe any **FIVE (5)** characteristics of digital evidence that are admissible in a court of law.

(10 marks)

(b) Initially, a digital forensic investigator could get only data from the phone contact book, short messaging services, call logs, and multimedia files. With smartphones becoming a norm these days, a digital forensic investigator is asked to extract more data. Aside from the above mentioned, list and explain **FIVE (5)** other types of mobile forensic artifacts that can be acquired from smartphones.

(10 marks)
(Total: 20 marks)

~THE END~