Departamento de Eletrónica, Telecomunicações e Informática da Universidade de Aveiro

Análise Forense de Sistemas Computacionais 2021/2022 (1st Semester)

Final Test 15-01-2022

Duration: 1:30h

Name:_____ No.:_____

Course:_____

Each question is worth 0.5 points on a scale of 0 to 20. Each wrong answer is worth -0.15 points.

1 - A phishing email is one which:

A) Requests a payment for goods you have not received
B) Offers you products in which you may have no interest
C) Encourages you to click on a link to a fraudulent website
D) Contains abusive and threatening language

2 - The principles of information security based on the CIA concept are:

A) Accountability, Clarity and Intelligence
B) Authenticity, Creativity and Innovation
C) Availability, Confidentiality and Integrity
D) Appreciation, Cooperation and Invention

3 - A computer systems subversion technique that consists of masking IP packets using fake sender addresses is known as:

A) Spoofing
B) Sniffing
C) Spamming
D) Cybersquatting

4 - Which option below is not a hashing function used for validation checks?

A) RC4
B) MD5
C) SHA-1
D) CRC32

5 - The process of documenting the seizure of digital evidence and when that evidence changes hands, is known as:

A) Chain of custody
B) Field notes
C) Interim report
D) None of the above

6 - Generating a plan of action and obtaining supporting resources and materials falls under which step in the digital investigation?

A) Preparation
B) System preservation
C) Evidence searching
D) Event reconstruction

7 - When you have developed a theory, what can you do to confirm that your hypothesis is correct?

A) Predict, based on your hypothesis, where artifacts should be located
B) Perform experiments to test results and rule out alternate explanations
C) Conclude, based on your findings, whether the evidence supports the hypothesis
D) All the above

8 - Which option below is not a Linus live CD meant for use as a digital forensics tool?

A) Paladin
B) Kali Linux
C) Ubuntu
D) Caine

9 - What command was developed by the Department of Defense Computer Forensics Laboratory as an enhanced version of dd?

A) dc3dd
B) split
C) dcfldd
D) echo

10 - Which of the following artifacts cannot be acquired with FTK Imager?

A) Protected Registry Files on a Local Machine
B) Drive's host protected area
C) Local Machine Memory
D) Local Machine Pagefile.sys

11 - Which of the following commands creates an alternate data stream?

A) echo text > myfile. txt:stream_name
B) ads create myfile.txt(stream_name) "text"
C) cat text myfile.txt=stream_name
D) echo text

12 - Which of the character encoding systems uses a fixed length for each character?

A) UFT-8
B) UFT-16
C) UFT-32
D) UTF-8 with BOM

13 - The big-endian representation of 0xFB787A23 is:

A) 78 FB 23 7A
B) 7A 23 FB 78
C) 23 7A 78 FB
D) FB 78 7A 23

14 - SGVsbG8gV29ybGQ= may be the result of what type of character encoding?

A) Base64
B) Base58
C) Hexadecimal
D) None of the above

15 - What is Autopsy used for?

A) Finding deleted data
B) Extracting data
C) Analysing extracted data
D) Creating new data

16 - Which of the following is a valid MAC address?

A) 192.168.0.5
B) 00:10:4b:de:fc:e9
C) 0-0-e2-7a-c3-5b-6f
D) 08-00-56-s7-fd-d4

17 - FireFox stores potentially notable information in:

A) DBF format databases
B) ASCII text files
C) SQLite databases
D) Proprietary format files

18 - What term is used to describe a disk's logical structure of platters, tracks, and sectors?

A) Cylinder
B) Trigonometry
C) Geometry
D) Mapping

19 - A typical disk drive stores how many bytes in a single sector?

A) 8
B) 512
C) 1024
D) 4096

20 - The storage capacity of a hard drive with 256 heads, 63 sectors, and 1024 cylinders is:

A) 8455716864 B
B) 7.875 GB
C) 15.75 MB
D) 16515072 B

21 - File slack space is:

A) The space between the end of a volume and the end of a partition
B) The sectors in a cluster that are not occupied by the file in that cluster
C) The space on a disk that is not allocated to files
D) The space left on a disk after a file is deleted

22 - The standard Windows environment supports all the following file systems EXCEPT _____.

A) FAT16
B) ext2
C) FAT32
D) NTFS

23 - When using a target drive that is FAT32 formatted, what is the maximum size limitation for copy the files?

A) 512 MB
B) 4 GB
C) 1 TB
D) 1 PB

24 - The _____ was developed in the mid-1990's by Microsoft to improve FAT in terms of performance and reliability.

A) New Technology File System
B) New Transfer File Standard
C) New Transfer File System
D) New Technology Format Standard

25 - Which of the following file systems was developed for Mac OS?

A) HFS
B) FAT
C) NTFS
D) UFS

26 - You find the following deleted file on disk. How many clusters does this file occupy?
REF.DOC Size:19968 Cluster: 275

A) 200
B) 78
C) 39
D) 21

27 - Which of the following tools does not allow you to acquire memory from the local machine?

A) FTK Imager
B) Wimpmem
C) Autopsy
D) AVML

28 - Which of the following is NOT an artifact that will be irrevocably lost if the computer is shut down?

A) Running processes
B) Opened network ports
C) Data stored in memory
D) System date and time

29 - When collecting data from a compromised computer, consideration should be given to collecting the _____ data first.

A) CMOS
B) Most volatile
C) Magnetic
D) Optical

30 - Which of the following files cannot be parsed by Volatility?

A) pagefile.sys
B) hiberfil.sys
C) windows_memory_dump.dmp
D) vmware_memory_image.vmem

31 - What choice below best depicts the purpose of the Windows Swap file?

A) It's used as a memory reserve by the Windows operating system
B) It helps the computer to boot faster
C) It's used to show better graphics
D) It's used to save persistent files

32 - When we talk about an "image" in the context of a mobile forensics' investigation, what are we talking about?

A) A photo you share on social media
B) A copy of all the data on a device
C) A small sample of data from a device
D) A picture contained on the device

33 - ____ cards are usually found in GSM devices and consist of a microprocessor and internal memory.

A) SIM
B) SDD
C) SD
D) MMC

34 - The primary reason that brute-force methods are not used when trying to access an SIM card with the PIN set is:

A) A four-digit PIN represents 10,000 possible combinations
B) After three failed attempts, the SIM card will become locked
C) PIN disclosure by the offender can be required by a court order
D) None of the above

35 - A _____ involves obtaining a judicial authorization or formal explicit or implicit authorization through the delegation of powers.

A) Closed source of information
B) Opened source of information
C) Primary source of information
D) Secondary source of information

36 - Dark Web can only be access by:

A) Using a VPN
B) Using a Proxy
C) Using a Website Operator
D) Using Special Software

37 - When moving through the TOR Network what happens to the data?

A) It is immediately sent to its destination
B) The data is encrypted once and sent through relays
C) The data is encrypted every relay
D) The data is not encrypted when it goes to each relay

38 - Digital evidence is said to be _____ if it was collected, analysed, handled, and stored in a manner that is acceptable by the law, and there is reasonable evidence to prove so.

A) Legally authentic
B) Legally admissible
C) Technically irrefutable
D) Forensically sound

39 - What is Registry?

A) A hierarchical database used by every computer to store settings and data
B) A hierarchical database used by computers running Windows to store settings and data
C) A relational database used by every computer to store settings and data
D) A relational database used by computers running Windows to store settings and data

40 - What Registry file contains user account management and security settings?

A) default.dat
B) software.dat
C) SAM.dat
D) Ntuser.dat

THE END