**Use the Multiple Choice Answer Sheet provided.**

**Attempt all questions.**

For each question, there are four alternatives, out of which only one is correct.

Choose the most appropriate answer.

1. What is the most significant legal issue in computer forensics?

A. Preserving Evidence

B. Seizing Evidence.

C. Admissibility of Evidence.

D. Discovery of Evidence.

2. When a file is deleted

A. The file remains intact.

B. The FAT entry for the file is zeroed out so it shows that the area is

available for use by a new file.

C. The first character of the directory entry file name is changed to a

special character.

D. All of the above.

3. Which of the following is not a property of computer evidence?

A. Authentic and Accurate.

B. Complete and Convincing.

C. Duplicated and Preserved.

D. Conform and Human Readable.

4. You can use \_\_\_\_\_\_\_\_, a powerful search tool, to perform keyword searches

in Linux and in EnCase software.

A. grep.

B. grub.

C. gcc.

D. gnu.

5. You are a computer forensic examiner at a scene and have determined you

will seize a Linux server, which according to your source of information

contains the database records for the company under investigation for fraud.

The best practice for “taking down” the server for collection is to photograph

the screen, note any running programs or messages and so on, and

\_\_\_\_\_\_\_\_\_\_.

A. Use the normal shutdown procedure

B. Pull the plug from the wall

C. Pull the plug from the rear of the computer

D. Ask the user at the scene to shut down the server

6. When a forensic copy is made, in what format are the contents of the hard

drive stored?

A. As compressed images.

B. As bootable files.

C. As executable files.

D. As operating system files.

7. Under Estimation Based attacks, watermarks are based on some stochastic criteria such as

A. maximum likelihood (ML),

B. maximum a posteriori probability (MAP),

C. minimum mean square error (MMSE).

D. All of the above

8. In establishing what evidence is admissible, many rules of evidence

concentrate first on the \_\_\_\_\_\_\_\_\_\_\_\_\_ of the offered evidence.

A. Relevancy

B. Search and Seizure

C. Material

D. Admissibility

9. Which of the following is a proper acquisition technique?

A. Disk to Image

B. Disk to Disk

C. Sparse Acquisition

D. All of the above

10. Traditional crimes that became easier or more widespread because of

telecommunication networks and powerful PCs include all of the following

*except*

A. Money laundering

B. Illegal drug distribution

C. DoS attacks

D. Child pornography

11. \_\_\_\_\_\_\_\_\_\_\_\_\_ devices prevent altering data on drives attached to the

suspect computer and also offer very fast acquisition speeds.

A. Encryption

B. Imaging

C. Write Blocking

D. Hashing

12. Which method is used for gathering evidences?

A. Copying

B. Preserving

C. Acquisitioning

D. Imaging

13. Which of the following attack is also called as Oracle attack.

A. White Box Attack

B. Black Box Attack

C. Both A and B

D. None of the above

14. The Windows operating system uses a file name’s \_\_\_\_\_\_\_\_\_\_\_ to associate

files with the proper applications.

A. Signature

B. Extension

C. MD5 hash value

D. Metadata

15. As a good forensic practice, why would it be a good idea to wipe a forensic

drive before using it?

A. Chain of Custody

B. No need to wipe

C. Different file and operating systems

D. Cross-contamination

16. The ability to hide data in another file is called

A. Encryption.

B. Steganography.

C. Data parsing.

D. A and B.

17. When two hard drives are on the same data cable, both drives must have

which two settings for them to work?

A. Default and Cable Select

B. Primary and Secondary

C. Master and Slave

D. First and Second

18. USB drives use \_\_\_\_\_\_\_\_\_\_\_\_\_\_.

A. RAM memory

B. Cache memory

C. Flash memory

D. None of the above

19. Fragile Watermark is used for which main application

A. Fingerprinting

B. Multimedia Authentication

C. Cope Control

D. None of the above

20. A file header is which of the following?

A. A unique set of characters at the beginning of a file that identifies the

file type

B. A unique set of characters following the file name that identifies the file

type

C. A 128-bit value that is unique to a specific file based on its data

D. Synonymous with the file extension

21. Which of the following is not a true operating system?

A. DOS

B. Windows 3.1

C. Windows 2000

D. UNIX

22. Computer memory files written to the hard drive are called \_\_\_\_\_\_\_\_\_\_\_\_.

A. Metadata

B. Swap files

C. Spool files

D. User profiles

23. When shutting down a computer, what information is typically lost?

A. Data in RAM memory

B. Running processes

C. Current network connections

D. All of the above

24. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ is the science of hiding messages in messages.

A. Scanning

B. Spoofing

C. Steganography

D. Steganalysis

25. If the Internet History file has been deleted, \_\_\_\_\_\_\_\_\_\_\_\_ may still provide

information about what Web sites the user has visited.

A. Cookies

B. Metadata

C. User profiles

D. Sessions

26. Which of the following attack is based on the concept of invertible attack.

A. Protocol

B. Geometric

C. Oracle

D. Removal

27. Which of the following is a proper search technique?

A. Manual Browsing

B. Keyword Search

C. Regular Expression Search

D. All of the above

28. Which of the following is not a type of volatile evidence?

A. Routing Tables

B. Main Memory

C. Log files

D. Cached Data

29. To verify the original drive with the forensic copy, you use \_\_\_\_\_\_\_\_\_\_.

A. a password

B. a hash analysis

C. disk to disk verification

D. none of the above

30. Which of the following falls into category of Representative attacks

A. Scrambling Attacks

B. Collusion Attack

C. Gradient Attack

D. All of the above

This activity contains 10 questions.

Top of Form

|  |  |  |
| --- | --- | --- |
| ps_bkgd_upper_left | pixel | ps_bkgd_upper_right |
| pixel | |  |  | | --- | --- | |  | Question 1. The most common storage device for the personal computer is the | | problem_type_1 | |  | |  |  | | --- | --- | |  | floppy disk | |  | USB thumb drive | |  | zip disk | |  | Hard disk drive | | | pixel |
| ps_bkgd_lower_left |  | End of Question 1 |

|  |  |  |
| --- | --- | --- |
| ps_bkgd_upper_left | pixel | ps_bkgd_upper_right |
| pixel | |  |  | | --- | --- | |  | Question 2. Computer forensics involves all of the following stated activities *except* | | problem_type_2 | |  | |  |  | | --- | --- | |  | interpretation of computer data | |  | extraction of computer data | |  | manipulation of computer data | |  | preservation of computer data | | | pixel |
| ps_bkgd_lower_left |  | End of Question 2 |

|  |  |  |
| --- | --- | --- |
| ps_bkgd_upper_left | pixel | ps_bkgd_upper_right |
| pixel | |  |  | | --- | --- | |  | Question 3. A set of instructions compiled into a program that performs a particular task is known as: | | problem_type_3 | |  | |  |  | | --- | --- | |  | central processing unit | |  | hardware | |  | software | |  | motherboard | | | pixel |
| ps_bkgd_lower_left |  | End of Question 3 |

|  |  |  |
| --- | --- | --- |
| ps_bkgd_upper_left | pixel | ps_bkgd_upper_right |
| pixel | |  |  | | --- | --- | |  | Question 4. The volatile memory of the computer is known as: | | problem_type_4 | |  | |  |  | | --- | --- | |  | BIOS | |  | ROM | |  | CPU | |  | RAM | | | pixel |
| ps_bkgd_lower_left |  | End of Question 4 |

|  |  |  |
| --- | --- | --- |
| ps_bkgd_upper_left | pixel | ps_bkgd_upper_right |
| pixel | |  |  | | --- | --- | |  | Question 5. According to your text, a drive is prepared in three processes. The processes include all of the following except: | | problem_type_5 | |  | |  |  | | --- | --- | |  | low-level formatting | |  | high-level formatting | |  | partitioning | |  | formatting | | | pixel |
| ps_bkgd_lower_left |  | End of Question 5 |

|  |  |  |
| --- | --- | --- |
| ps_bkgd_upper_left | pixel | ps_bkgd_upper_right |
| pixel | |  |  | | --- | --- | |  | Question 6. The smallest addressable unit of data by a HDD generally consists of: | | problem_type_6 | |  | |  |  | | --- | --- | |  | 528 MB | |  | 8 bits | |  | 512 bytes | |  | 64K | | | pixel |
| ps_bkgd_lower_left |  | End of Question 6 |

|  |  |  |
| --- | --- | --- |
| ps_bkgd_upper_left | pixel | ps_bkgd_upper_right |
| pixel | |  |  | | --- | --- | |  | Question 7. The area that begins at the end of the last sector that contains logical data and terminates at the end of the cluster is known as: | | problem_type_7 | |  | |  |  | | --- | --- | |  | File slack | |  | ROM slack | |  | RAM slack | |  | HDD slack | | | pixel |
| ps_bkgd_lower_left |  | End of Question 7 |

|  |  |  |
| --- | --- | --- |
| ps_bkgd_upper_left | pixel | ps_bkgd_upper_right |
| pixel | |  |  | | --- | --- | |  | Question 8. Areas of files and disks that are not apparent to the user, and sometimes not even to the operating system, is termed: | | problem_type_8 | |  | |  |  | | --- | --- | |  | hidden data | |  | latent data | |  | missing data | |  | exceptional data | | | pixel |
| ps_bkgd_lower_left |  | End of Question 8 |

|  |  |  |
| --- | --- | --- |
| ps_bkgd_upper_left | pixel | ps_bkgd_upper_right |
| pixel | |  |  | | --- | --- | |  | Question 9. The state of the electronic crime scene may need to be processed by one or a combination of the following methods *except* | | problem_type_9 | |  | |  |  | | --- | --- | |  | live acquisition of the data | |  | immediate detachment from a network server | |  | performing a system shutdown | |  | pulling the plug from the back of the computer | | | pixel |
| ps_bkgd_lower_left |  | End of Question 9 |

|  |  |  |
| --- | --- | --- |
| ps_bkgd_upper_left | pixel | ps_bkgd_upper_right |
| pixel | |  |  | | --- | --- | |  | Question 10. The portion of a disk that contains no stored data, but may contain latent data is called | | problem_type_10 | |  | |  |  | | --- | --- | |  | RAM slack | |  | a cluster | |  | swap space | |  | unallocated space | | | pixel |
| *ps_bkgd_lower_left* |  |  |