DITISS

Cyberforensic

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

DITISS
Cyberforensic
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