Date:21-11-2013

Module Name:Cyber forensics

Q. No. 1

Question When a file is deleted

Answer Choices

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.

Q. No. 2

Question Which of the following is not a property of computer evidence?

Answer Choices

A. Authentic and Accurate. B. Complete and Convincing.
C. Duplicated and Preserved. D. Conform and Human Readable.

Q. No. 3

Question You can use ________, a powerful search tool, to perform keyword searches in Linux and in EnCase software.

Answer Choices

A. grep. B. grub. C. gcc. D. gnu.

Q. No. 4

Question 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 __________.

Answer Choices

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

Q. No. 5

Question When a forensic copy is made, in what format are the contents of the hard drive stored?

Answer Choices

A. As compressed images. B. As bootable files.
C. As executable files. D. As operating system files.

Q. No. 6

Question Which of the following is not a type of volatile evidence?

Answer Choices

A. Routing Tables B. Main Memory C. Log files D. Cached Data

Q. No. 7

Question In establishing what evidence is admissible, many rules of evidence concentrate first on the ______________ of the offered evidence.

Answer Choices

A. Relevancy B. Search and Seizure C. Material D. Admissibility

Q. No. 8

Question Which of the following is a proper acquisition technique?

Answer Choices

A. Disk to Image B. Disk to Disk C. Sparse Acquisition D. All of the above

Q. No. 9

Question Traditional crimes that became easier or more widespread because of telecommunication networks and powerful PCs include all of the following

except

Answer Choices

A. Money laundering B. Illegal drug distribution
C. DoS attacks D. Child pornography

Q. No. 10

Question _____________ devices prevent altering data on drives attached to the suspect computer and also offer very fast acquisition speeds.

Answer Choices

A. Encryption B. Imaging C. Write Blocking D. Hashing

Q. No. 11

Question Which duplication method produces an exact replica of the original drive?

Answer Choices

A. Bit-Stream Copy B. Image Copy C. Mirror Copy D. Drive Image

Q. No. 12

Question To verify the original drive with the forensic copy, you use __________.

Answer Choices

A. a password B. a hash analysis C. disk to disk verification D. none of the above

Q. No. 13

Question The Windows operating system uses a file name's ___________ to associate files with the proper applications.

Answer Choices

A. Signature B. Extension C. MD5 hash value D. Metadata

Q. No. 14

Question As a good forensic practice, why would it be a good idea to wipe a forensic drive before using it?

Answer Choices

A. Chain of Custody B. No need to wipe
C. Different file and operating systems D. Cross-contamination

Q. No. 15

Question The ability to hide data in another file is called

Answer Choices

A. Encryption. B. Steganography. C. Data parsing. D. A and B.

Q. No. 16

Question When two hard drives are on the same data cable, both drives must have which two settings for them to work?

Answer Choices

A. Default and Cable Select B. Primary and Secondary
C. Master and Slave D. First and Second

Q. No. 17

Question USB drives use _______________.

Answer Choices

A. RAM memory B. Cache memory C. Flash memory D. None of the above

Q. No. 18

Question Which of the following is a proper search technique?

Answer Choices

A. Manual Browsing B. Keyword Search
C. Regular Expression Search D. All of the above

Q. No. 19

Question A file header is which of the following?

Answer Choices

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

Q. No. 20

Question Which of the following is not a true operating system?
Answer Choices

A. DOS B. Windows 3.1 C. Windows 2000 D. UNIX

Q. No. 21

Question Computer memory files written to the hard drive are called _____________.

Answer Choices

A. Metadata B. Swap files C. Spool files D. User profiles

Q. No. 22

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

Answer Choices

A. Data in RAM memory B. Running processes
C. Current network connections D. All of the above

Q. No. 23

Question _________________ is the science of hiding messages in messages.

Answer Choices

A. Scanning B. Spoofing C. Steganography D. Steganalysis

Q. No. 24

Question If the Internet History file has been deleted, ____________ may still provide information about what Web sites the user has visited.

Answer Choices

A. Cookies B. Metadata C. User profiles D. Sessions

Q. No. 25

Question Tool used for seizure and acquisition is or are

Answer Choices

A. Trueback B. Hasher C. Cofee D. AOPR

Q. No. 26

Question Packet capturing in a ntework can be done by

Answer Choices

A. NeSA B. Wireshark C.Both a and b D. None of the above

Q. No. 27

Question Which cyber forensics tool is used for forensic analysis

Answer Choices

A. Cyberinvestigator B. Cybercheck C. NeSA D. Wireshark

Q. No. 28

Question The geographic region and email sender is identified by

Answer Choices

A. NeSA B. Wireshark C. Email-Tracer D. Cybercheck

Q. No. 29

Question Static Analysis is also known as

Answer Choices

A. Live Forensics B. Traditional Forensics
B. Computer Forensics D. Disk Forensics

Q. No. 30

Question The procedure for Network forensics include

Answer Choices

A. Capture B. Copy C. either a or b D. both a and b

Q. No. 31

Question The network packets are captured through

Answer Choices

A. Tunnel mode B. Transport mode C. Promiscuous mode D. Normal mode

Q. No. 32

Question Under Estimation Based attacks, watermarks are based on some stochastic criteria such as
Answer Choices

A. maximum likelihood (ML),
B. maximum a posteriori probability (MAP),
C. minimum mean square error (MMSE).
D. All of the above

Q. No. 33

Question The portion of a disk that contains no stored data, but may contain latent data is called
Answer Choices

A. RAM slack B. A cluster C.Swap space D. Unallocated space

Q. No. 34

Question
The state of the electronic crime scene may need to be processed by one or a combination of the following methods *except*

Answer Choices

A. live acquisition of the data
B. immediate detachment from a network server
C. performing a system shutdown
D. pulling the plug from the back of the computer

Q. No. 35

Question Fragile Watermark is used for which main application

Answer Choices

A. Fingerprinting B. Multimedia Authentication
C. Cope Control D. None of the above

Q. No. 36

Question .Steganographic file system program that can completely hide and protect files,folders and drives by making them inaccessible.Which steganographic tool is this?

Answer Choices

A. Anahtar B. Backyard C. Blindside D.Easy Protector

Q. No. 37

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

Answer Choices

[✓ A. Protocol] B. Geometric C. Oracle D. Removal

Q. No. 38

Question Context –free grammars are used in this category of steganography
Answer Choices

[✓ A. Spread Spectrum] B. Distortion Techniques
C.Cover-generation Techniques D.Transform Domain Techniques

Q. No. 39
Question Data to be transmitted is divided into small pieces and each piece is allocated to a frequency channel.this happens in which category of steganography

Answer Choices

A. Direct Sequence Spread Spectrum
B. Frequency Hopping Spread Spectrum
C. None of these
D. Both of these

Q. No. 40

Question: What is the most significant legal issue in computer forensics?

Answer Choices

A. Preserving Evidence B. Seizing Evidence.
C. [✓ Admissibility of Evidence.] D. Discovery of Evidence.