# EC-Council

## Exam Questions 312-49v10

Computer Hacking Forensic Investigator (CHFI-v10)

**NEW QUESTION 1**
- (Exam Topic 1)
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. APIPA
B. IANA
C. CVE
D. RIPE

**Answer:** C


**NEW QUESTION 2**
- (Exam Topic 1)
What will the following URL produce in an unpatched IIS Web Server? http://www.thetargetsite.com/scripts/..%
co%af../..%co%af../windows/system32/cmd.exe?/c+dir+c:\

A. Directory listing of C: drive on the web server
B. Insert a Trojan horse into the C: drive of the web server
C. Execute a buffer flow in the C: drive of the web server
D. Directory listing of the C:\windows\system32 folder on the web server

**Answer:** A


**NEW QUESTION 3**
- (Exam Topic 1)
Law enforcement officers are conducting a legal search for which a valid warrant was obtained.
While conducting the search, officers observe an item of evidence for an unrelated crime that was not included in the warrant. The item was clearly visible to the officers and immediately identified as evidence. What is the term used to describe how this evidence is admissible?

A. Plain view doctrine
B. Corpus delicti
C. Locard Exchange Principle
D. Ex Parte Order

**Answer:** A


**NEW QUESTION 4**
- (Exam Topic 1)
You have completed a forensic investigation case. You would like to destroy the data contained in various disks at the forensics lab due to sensitivity of the case. How would you permanently erase the data on the hard disk?

A. Throw the hard disk into the fire
B. Run the powerful magnets over the hard disk
C. Format the hard disk multiple times using a low level disk utility
D. Overwrite the contents of the hard disk with Junk data

**Answer:** A


**NEW QUESTION 5**
- (Exam Topic 1)
The objective of this act was to protect consumers' personal financial information held by financial institutions and their service providers.

A. Gramm-Leach-Bliley Act
B. Sarbanes-Oxley 2002
C. California SB 1386
D. HIPAA

**Answer:** A


**NEW QUESTION 6**
- (Exam Topic 1)
Jason is the security administrator of ACMA metal Corporation. One day he notices the company's Oracle database server has been compromised and the customer information along with financial data has been stolen. The financial loss will be in millions of dollars if the database gets into the hands of the competitors. Jason wants to report this crime to the law enforcement agencies immediately.
Which organization coordinates computer crimes investigations throughout the United States?

A. Internet Fraud Complaint Center
B. Local or national office of the U.
C. Secret Service
D. National Infrastructure Protection Center
E. CERT Coordination Center

**Answer:** B

**NEW QUESTION 7**
- (Exam Topic 1)
Area density refers to:

A. the amount of data per disk
B. the amount of data per partition
C. the amount of data per square inch
D. the amount of data per platter

**Answer:** A


**NEW QUESTION 8**
- (Exam Topic 1)
The following excerpt is taken from a honeypot log. The log captures activities across three days. There are several intrusion attempts; however, a few are successful.
(Note: The objective of this question is to test whether the student can read basic information from log entries and interpret the nature of attack.)
Apr 24 14:46:46 [4663]: spp_portscan: portscan detected from 194.222.156.169
Apr 24 14:46:46 [4663]: IDS27/FIN Scan: 194.222.156.169:56693 -> 172.16.1.107:482
Apr 24 18:01:05 [4663]: IDS/DNS-version-query: 212.244.97.121:3485 -> 172.16.1.107:53
Apr 24 19:04:01 [4663]: IDS213/ftp-passwd-retrieval: 194.222.156.169:1425 -> 172.16.1.107:21
Apr 25 08:02:41 [5875]: spp_portscan: PORTSCAN DETECTED from 24.9.255.53
Apr 25 02:08:07 [5875]: IDS277/DNS-version-query: 63.226.81.13:4499 -> 172.16.1.107:53
Apr 25 02:08:07 [5875]: IDS277/DNS-version-query: 63.226.81.13:4630 -> 172.16.1.101:53
Apr 25 02:38:17 [5875]: IDS/RPC-rpcinfo-query: 212.251.1.94:642 -> 172.16.1.107:111
Apr 25 19:37:32 [5875]: IDS230/web-cgi-space-wildcard: 198.173.35.164:4221 -> 172.16.1.107:80
Apr 26 05:45:12 [6283]: IDS212/dns-zone-transfer: 38.31.107.87:2291 -> 172.16.1.101:53
Apr 26 06:43:05 [6283]: IDS181/nops-x86: 63.226.81.13:1351 -> 172.16.1.107:53
Apr 26 06:44:25 victim7 PAM_pwdb[12509]: (login) session opened for user simple by (uid=0)
Apr 26 06:44:36 victim7 PAM_pwdb[12521]: (su) session opened for user simon by simple(uid=506) Apr 26 06:45:34 [6283]: IDS175/socks-probe: 24.112.167.35:20 -> 172.16.1.107:1080
Apr 26 06:52:10 [6283]: IDS127/telnet-login-incorrect: 172.16.1.107:23 -> 213.28.22.189:4558
From the options given below choose the one which best interprets the following entry: Apr 26 06:43:05 [6283]: IDS181/nops-x86: 63.226.81.13:1351 -> 172.16.1.107:53

A. An IDS evasion technique
B. A buffer overflow attempt
C. A DNS zone transfer
D. Data being retrieved from 63.226.81.13

**Answer:** A


**NEW QUESTION 9**
- (Exam Topic 1)
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. logical
B. anti-magnetic
C. magnetic
D. optical

**Answer:** D


**NEW QUESTION 10**
- (Exam Topic 1)
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. Root Internet servers
B. Border Gateway Protocol
C. Gateway of last resort
D. Reverse DNS

**Answer:** C


**NEW QUESTION 10**
- (Exam Topic 1)
You are working as a Computer forensics investigator for a corporation on a computer abuse case. You discover evidence that shows the subject of your investigation is also embezzling money from the company. The company CEO and the corporate legal counsel advise you to contact law enforcement and provide them with the evidence that you have found. The law enforcement officer that responds requests that you put a network sniffer on your network and monitor all traffic to the subject's computer. You inform the officer that you will not be able to comply with that request because doing so would:

A. Violate your contract
B. Cause network congestion
C. Make you an agent of law enforcement
D. Write information to the subject's hard drive

**Answer:** C

**NEW QUESTION 14**
- (Exam Topic 1)
What TCP/UDP port does the toolkit program netstat use?

A. Port 7
B. Port 15
C. Port 23
D. Port 69

**Answer:** B

**NEW QUESTION 19**
- (Exam Topic 1)
If you discover a criminal act while investigating a corporate policy abuse, it becomes a publicsector investigation and should be referred to law enforcement?

A. true
B. false

**Answer:** A

**NEW QUESTION 24**
- (Exam Topic 1)
You have been asked to investigate after a user has reported a threatening e-mail they have received from an external source. Which of the following are you most interested in when trying to trace the source of the message?

A. The X509 Address
B. The SMTP reply Address
C. The E-mail Header
D. The Host Domain Name

**Answer:** C

**NEW QUESTION 26**
- (Exam Topic 2)
Preparing an image drive to copy files to is the first step in Linux forensics. For this purpose, what would the following command accomplish?
dcfldd if=/dev/zero of=/dev/hda bs=4096 conv=noerror, sync

A. Fill the disk with zeros
B. Low-level format
C. Fill the disk with 4096 zeros
D. Copy files from the master disk to the slave disk on the secondary IDE controller

**Answer:** A

**NEW QUESTION 27**
- (Exam Topic 2)
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:** A

**NEW QUESTION 30**
- (Exam Topic 2)
What stage of the incident handling process involves reporting events?

A. Containment
B. Follow-up
C. Identification
D. Recovery

**Answer:** C

**NEW QUESTION 32**
- (Exam Topic 2)
Steven has been given the task of designing a computer forensics lab for the company he works for. He has found documentation on all aspects of how to design a lab except the number of exits needed. How many exits should Steven include in his design for the computer forensics lab?

A. Three
B. One
C. Two
D. Four

**Answer:**

B

## NEW QUESTION 35
- (Exam Topic 2)
Which of the following commands shows you the names of all open shared files on a server and the number of file locks on each file?

A. Net config
B. Net file
C. Net share
D. Net sessions

**Answer:** B

## NEW QUESTION 36
- (Exam Topic 2)
To check for POP3 traffic using Ethereal, what port should an investigator search by?

A. 143
B. 25
C. 110
D. 125

**Answer:** C

## NEW QUESTION 37
- (Exam Topic 2)
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. Click-jacking
B. Compromising a legitimate site
C. Spearphishing
D. Malvertising

**Answer:** D

## NEW QUESTION 40
- (Exam Topic 2)
When using an iPod and the host computer is running Windows, what file system will be used?

A. iPod+
B. HFS
C. FAT16
D. FAT32

**Answer:** D

## NEW QUESTION 41
- (Exam Topic 1)
An "idle" system is also referred to as what?

A. PC not connected to the Internet
B. Zombie
C. PC not being used
D. Bot

**Answer:** B

## NEW QUESTION 45
- (Exam Topic 2)
Which network attack is described by the following statement?
"At least five Russian major banks came under a continuous hacker attack, although online client services were not disrupted. The attack came from a wide-scale botnet involving at least 24,000 computers, located in 30 countries."

A. DDoS
B. Sniffer Attack
C. Buffer Overflow
D. Man-in-the-Middle Attack

**Answer:** A

## NEW QUESTION 50
- (Exam Topic 1)
You are assisting in the investigation of a possible Web Server Hack. The company who called you stated that customers reported to them that whenever they entered the web address of the company in their browser, what they received was a porno graphic web site. The company checked the web server and nothing appears wrong. When you type in the IP address of the web site in your browser everything appears normal. What is the name of the attack that affects the DNS

cache of the name resolution servers, resulting in those servers directing users to the wrong web site?

A. ARP Poisoning
B. DNS Poisoning
C. HTTP redirect attack
D. IP Spoofing

**Answer:** B


**NEW QUESTION 52**
- (Exam Topic 1)
Lance wants to place a honeypot on his network. Which of the following would be your recommendations?

A. Use a system that has a dynamic addressing on the network
B. Use a system that is not directly interacting with the router
C. Use it on a system in an external DMZ in front of the firewall
D. It doesn't matter as all replies are faked

**Answer:** D


**NEW QUESTION 57**
- (Exam Topic 1)
What will the following command accomplish?

A. Test ability of a router to handle over-sized packets
B. Test the ability of a router to handle under-sized packets
C. Test the ability of a WLAN to handle fragmented packets
D. Test the ability of a router to handle fragmented packets

**Answer:** A


**NEW QUESTION 58**
- (Exam Topic 1)
The use of warning banners helps a company avoid litigation by overcoming an employee assumed _____. When connecting to the company's intranet, network or Virtual Private Network(VPN) and will allow the company's investigators to monitor, search and retrieve information stored within the network.

A. Right to work
B. Right of free speech
C. Right to Internet Access
D. Right of Privacy

**Answer:** D


**NEW QUESTION 59**
- (Exam Topic 1)
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 1030
B. Title 18, Section 2703(d)
C. Title 18, Section Chapter 90
D. Title 18, Section 2703(f)

**Answer:** D


**NEW QUESTION 62**
- (Exam Topic 1)
Which part of the Windows Registry contains the user's password file?

A. HKEY_LOCAL_MACHINE
B. HKEY_CURRENT_CONFIGURATION
C. HKEY_USER
D. HKEY_CURRENT_USER

**Answer:** A


**NEW QUESTION 66**
- (Exam Topic 1)
You are assisting a Department of Defense contract company to become compliant with the stringent security policies set by the DoD. One such strict rule is that firewalls must only allow incoming connections that were first initiated by internal computers. What type of firewall must you implement to abide by this policy?

A. Packet filtering firewall
B. Circuit-level proxy firewall
C. Application-level proxy firewall
D. Stateful firewall

**Answer:** D

**NEW QUESTION 69**
- (Exam Topic 1)
What should you do when approached by a reporter about a case that you are working on or have worked on?

A. Refer the reporter to the attorney that retained you
B. Say, "no comment"
C. Answer all the reporter's questions as completely as possible
D. Answer only the questions that help your case

**Answer:** A


**NEW QUESTION 73**
- (Exam Topic 1)
If a suspect computer is located in an area that may have toxic chemicals, you must:

A. coordinate with the HAZMAT team
B. determine a way to obtain the suspect computer
C. assume the suspect machine is contaminated
D. do not enter alone

**Answer:** A


**NEW QUESTION 77**
- (Exam Topic 1)
Item 2If you come across a sheepdip machine at your client site, what would you infer?

A. A sheepdip coordinates several honeypots
B. A sheepdip computer is another name for a honeypot
C. A sheepdip computer is used only for virus-checking.
D. A sheepdip computer defers a denial of service attack

**Answer:** C


**NEW QUESTION 78**
- (Exam Topic 1)
In the context of file deletion process, which of the following statement holds true?

A. When files are deleted, the data is overwritten and the cluster marked as available
B. The longer a disk is in use, the less likely it is that deleted files will be overwritten
C. While booting, the machine may create temporary files that can delete evidence
D. Secure delete programs work by completely overwriting the file in one go

**Answer:** C


**NEW QUESTION 80**
- (Exam Topic 1)
You should make at least how many bit-stream copies of a suspect drive?

A. 1
B. 2
C. 3
D. 4

**Answer:** B


**NEW QUESTION 85**
- (Exam Topic 1)
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. Tracert
B. Smurf scan
C. Ping trace
D. ICMP ping sweep

**Answer:** D


**NEW QUESTION 90**
- (Exam Topic 1)
To preserve digital evidence, an investigator should .

A. Make two copies of each evidence item using a single imaging tool
B. Make a single copy of each evidence item using an approved imaging tool
C. Make two copies of each evidence item using different imaging tools
D. Only store the original evidence item

**Answer:** C

**NEW QUESTION 91**
- (Exam Topic 1)
_____ is simply the application of Computer Investigation and analysis techniques in the interests of determining potential legal evidence.

A. Network Forensics
B. Computer Forensics
C. Incident Response
D. Event Reaction

**Answer:** B

**NEW QUESTION 94**
- (Exam Topic 1)
Which of the following file system is used by Mac OS X?

A. EFS
B. HFS+
C. EXT2
D. NFS

**Answer:** B

**NEW QUESTION 95**
- (Exam Topic 1)
You are conducting an investigation of fraudulent claims in an insurance company that involves complex text searches through large numbers of documents. Which of the following tools would allow you to quickly and efficiently search for a string within a file on the bitmap image of the target computer?

A. Stringsearch
B. grep
C. dir
D. vim

**Answer:** B

**NEW QUESTION 99**
- (Exam Topic 1)
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. Any data not yet flushed to the system will be lost
B. All running processes will be lost
C. The /tmp directory will be flushed
D. Power interruption will corrupt the pagefile

**Answer:** A

**NEW QUESTION 102**
- (Exam Topic 1)
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. Only an HTTPS session can be hijacked
B. HTTP protocol does not maintain session
C. Only FTP traffic can be hijacked
D. Only DNS traffic can be hijacked

**Answer:** B

**NEW QUESTION 107**
- (Exam Topic 1)
Kimberly is studying to be an IT security analyst at a vocational school in her town. The school offers many different programming as well as networking languages. What networking protocol language should she learn that routers utilize?

A. ATM
B. UDP
C. BPG
D. OSPF

**Answer:** D

**NEW QUESTION 112**
- (Exam Topic 1)
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 conducted a network sweep on port 111
B. The attacker has scanned and exploited the system using Buffer Overflow
C. The attacker has used a Trojan on port 32773
D. The attacker has installed a backdoor

**Answer:** A


**NEW QUESTION 114**
- (Exam Topic 1)
The offset in a hexadecimal code is:

A. The last byte after the colon
B. The 0x at the beginning of the code
C. The 0x at the end of the code
D. The first byte after the colon

**Answer:** B


**NEW QUESTION 118**
- (Exam Topic 1)
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. Inculpatory evidence
B. Mandatory evidence
C. Exculpatory evidence
D. Terrible evidence

**Answer:** C


**NEW QUESTION 122**
- (Exam Topic 1)
Hackers can gain access to Windows Registry and manipulate user passwords, DNS settings, access rights or others features that they may need in order to accomplish their objectives. One simple method for loading an application at startup is to add an entry (Key) to the following Registry Hive:

A. HKEY_LOCAL_MACHINE\hardware\windows\start
B. HKEY_LOCAL_USERS\Software\Microsoft\old\Version\Load
C. HKEY_CURRENT_USER\Microsoft\Default
D. HKEY_LOCAL_MACHINE\Software\Microsoft\CurrentVersion\Run

**Answer:** D


**NEW QUESTION 126**
- (Exam Topic 1)
After passively scanning the network of Department of Defense (DoD), you switch over to active scanning to identify live hosts on their network. DoD is a large organization and should respond to any number of scans. You start an ICMP ping sweep by sending an IP packet to the broadcast address. Only five hosts respond to your ICMP pings; definitely not the number of hosts you were expecting. Why did this ping sweep only produce a few responses?

A. Only IBM AS/400 will reply to this scan
B. Only Windows systems will reply to this scan
C. A switched network will not respond to packets sent to the broadcast address
D. Only Unix and Unix-like systems will reply to this scan

**Answer:** D


**NEW QUESTION 128**
- (Exam Topic 1)
Volatile Memory is one of the leading problems for forensics. Worms such as code Red are memory resident and do write themselves to the hard drive, if you turn the system off they disappear. In a lab environment, which of the following options would you suggest as the most appropriate to overcome the problem of capturing volatile memory?

A. Use VMware to be able to capture the data in memory and examine it
B. Give the Operating System a minimal amount of memory, forcing it to use a swap file
C. Create a Separate partition of several hundred megabytes and place the swap file there
D. Use intrusion forensic techniques to study memory resident infections

**Answer:** C


**NEW QUESTION 133**
- (Exam Topic 1)
Why are Linux/Unix based computers better to use than Windows computers for idle scanning?

A. Linux/Unix computers are easier to compromise
B. Linux/Unix computers are constantly talking
C. Windows computers are constantly talking
D. Windows computers will not respond to idle scans

**Answer:** C


**NEW QUESTION 136**
- (Exam Topic 1)
E- mail logs contain which of the following information to help you in your investigation? (Choose four.)

A. user account that was used to send the account
B. attachments sent with the e-mail message
C. unique message identifier
D. contents of the e-mail message
E. date and time the message was sent

**Answer:** ACDE


**NEW QUESTION 139**
- (Exam Topic 1)
Why should you note all cable connections for a computer you want to seize as evidence?

A. to know what outside connections existed
B. in case other devices were connected
C. to know what peripheral devices exist
D. to know what hardware existed

**Answer:** A


**NEW QUESTION 141**
- (Exam Topic 1)
When examining the log files from a Windows IIS Web Server, how often is a new log file created?

A. the same log is used at all times
B. a new log file is created everyday
C. a new log file is created each week
D. a new log is created each time the Web Server is started

**Answer:** A


**NEW QUESTION 146**
- (Exam Topic 1)
Profiling is a forensics technique for analyzing evidence with the goal of identifying the perpetrator from their various activity. After a computer has been compromised by a hacker, which of the following would be most important in forming a profile of the incident?

A. The manufacturer of the system compromised
B. The logic, formatting and elegance of the code used in the attack
C. The nature of the attack
D. The vulnerability exploited in the incident

**Answer:** B


**NEW QUESTION 149**
- (Exam Topic 1)
The efforts to obtain information before a trail by demanding documents, depositions, questioned and answers written under oath, written requests for admissions of fact and examination of the scene is a description of what legal term?

A. Detection
B. Hearsay
C. Spoliation
D. Discovery

**Answer:** D

**NEW QUESTION 154**
- (Exam Topic 1)
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. Never run a scan on your forensics workstation because it could change your systems configuration
C. Scan your forensics workstation at intervals of no more than once every five minutes during an investigation
D. Scan your Forensics workstation before beginning an investigation

**Answer:** D

**NEW QUESTION 159**
- (Exam Topic 1)
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. A preponderance of the evidence
C. Probable cause
D. Beyond a reasonable doubt

**Answer:** C

**NEW QUESTION 162**
- (Exam Topic 1)
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. 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.
D. All forms should be placed in the report file because they are now primary evidence in the case.

**Answer:** B

**NEW QUESTION 166**
- (Exam Topic 1)
Which of the following should a computer forensics lab used for investigations have?

A. isolation
B. restricted access
C. open access
D. an entry log

**Answer:** B

**NEW QUESTION 168**
- (Exam Topic 1)
The MD5 program is used to:

A. wipe magnetic media before recycling it
B. make directories on an evidence disk
C. view graphics files on an evidence drive
D. verify that a disk is not altered when you examine it

**Answer:** D

**NEW QUESTION 172**
- (Exam Topic 1)
You are called in to assist the police in an investigation involving a suspected drug dealer. The suspects house was searched by the police after a warrant was obtained and they located a floppy disk in the suspects bedroom. The disk contains several files, but they appear to be password protected. What are two common methods used by password cracking software that you can use to obtain the password?

A. Limited force and library attack
B. Brute Force and dictionary Attack
C. Maximum force and thesaurus Attack
D. Minimum force and appendix Attack

**Answer:** B

**NEW QUESTION 176**
- (Exam Topic 1)

When you carve an image, recovering the image depends on which of the following skills?

A. Recognizing the pattern of the header content
B. Recovering the image from a tape backup
C. Recognizing the pattern of a corrupt file
D. Recovering the image from the tape backup

**Answer:** A


**NEW QUESTION 177**
- (Exam Topic 1)
How many characters long is the fixed-length MD5 algorithm checksum of a critical system file?

A. 128
B. 64
C. 32
D. 16

**Answer:** C


**NEW QUESTION 180**
- (Exam Topic 1)
You are trying to locate Microsoft Outlook Web Access Default Portal using Google search on the Internet. What search string will you use to locate them?

A. allinurl:"exchange/logon.asp"
B. intitle:"exchange server"
C. locate:"logon page"
D. outlook:"search"

**Answer:** A


**NEW QUESTION 183**
- (Exam Topic 1)
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. Deletes the entire members table
B. Inserts the Error! Reference source not found.email address into the members table
C. Retrieves the password for the first user in the members table
D. This command will not produce anything since the syntax is incorrect

**Answer:** A


**NEW QUESTION 188**
- (Exam Topic 1)
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. 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
B. make an MD5 hash of the evidence and compare it to the standard database developed by NIST
C. there is no reason to worry about this possible claim because state labs are certified
D. sign a statement attesting that the evidence is the same as it was when it entered the lab

**Answer:** A


**NEW QUESTION 192**
- (Exam Topic 1)
Bill is the accounting manager for Grummon and Sons LLC in Chicago. On a regular basis, he needs to send PDF documents containing sensitive information through E-mail to his customers.
Bill protects the PDF documents with a password and sends them to their intended recipients. Why PDF passwords do not offer maximum protection?

A. PDF passwords can easily be cracked by software brute force tools
B. PDF passwords are converted to clear text when sent through E-mail
C. PDF passwords are not considered safe by Sarbanes-Oxley
D. When sent through E-mail, PDF passwords are stripped from the document completely

**Answer:** A


**NEW QUESTION 195**
- (Exam Topic 1)
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 Personal Application Protocol
C. the Globally Unique ID

D. the Individual ASCII String

**Answer:** C


**NEW QUESTION 200**
- (Exam Topic 1)
Which federal computer crime law specifically refers to fraud and related activity in connection with access devices like routers?

A. 18 U.S.
B. 1029
C. 18 U.S.
D. 1362
E. 18 U.S.
F. 2511
G. 18 U.S.
H. 2703

**Answer:** A


**NEW QUESTION 203**
- (Exam Topic 1)
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. It can recover deleted file space and search it for dat
C. However, it does not allow the investigator to preview them
D. The tools scans for i-node information, which is used by other tools in the tool kit
E. It is too specific to the MAC OS and forms a core component of the toolkit

**Answer:** A


**NEW QUESTION 208**
- (Exam Topic 1)
Sectors in hard disks typically contain how many bytes?

A. 256
B. 512
C. 1024
D. 2048

**Answer:** B


**NEW QUESTION 213**
- (Exam Topic 1)
Jim performed a vulnerability analysis on his network and found no potential problems. He runs another utility that executes exploits against his system to verify the results of the vulnerability test.
The second utility executes five known exploits against his network in which the vulnerability analysis said were not exploitable. What kind of results did Jim receive from his vulnerability analysis?

A. False negatives
B. False positives
C. True negatives
D. True positives

**Answer:** A


**NEW QUESTION 215**
- (Exam Topic 1)
When obtaining a warrant, it is important to:

A. particularlydescribe the place to be searched and particularly describe the items to be seized
B. generallydescribe the place to be searched and particularly 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 generally describe the items to be seized

**Answer:** A


**NEW QUESTION 218**
- (Exam Topic 1)
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 file header
C. the file footer
D. the sector map

**Answer:** B

**NEW QUESTION 219**
- (Exam Topic 1)
Before you are called to testify as an expert, what must an attorney do first?

A. engage in damage control
B. prove that the tools you used to conduct your examination are perfect
C. read your curriculum vitae to the jury
D. qualify you as an expert witness

**Answer:** D

**NEW QUESTION 220**
- (Exam Topic 1)
As a CHFI professional, which of the following is the most important to your professional reputation?

A. Your Certifications
B. The correct, successful management of each and every case
C. The free that you charge
D. The friendship of local law enforcement officers

**Answer:** B

**NEW QUESTION 222**
- (Exam Topic 1)
At what layer of the OSI model do routers function on?

A. 4
B. 3
C. 1
D. 5

**Answer:** B

**NEW QUESTION 226**
- (Exam Topic 1)
This organization maintains a database of hash signatures for known software.

A. International Standards Organization
B. Institute of Electrical and Electronics Engineers
C. National Software Reference Library
D. American National standards Institute

**Answer:** C

**NEW QUESTION 227**
- (Exam Topic 1)
What header field in the TCP/IP protocol stack involves the hacker exploit known as the Ping of Death?

A. ICMP header field
B. TCP header field
C. IP header field
D. UDP header field

**Answer:** B

**NEW QUESTION 232**
- (Exam Topic 1)
You just passed your ECSA exam and are about to start your first consulting job running security audits for a financial institution in Los Angeles. The IT manager of the company you will be working for tries to see if you remember your ECSA class. He asks about the methodology you will be using to test the company's network. How would you answer?

A. Microsoft Methodology
B. Google Methodology
C. IBM Methodology
D. LPT Methodology

**Answer:** D

**NEW QUESTION 237**
- (Exam Topic 4)
What command-line tool enables forensic Investigator to establish communication between an Android device and a forensic workstation in order to perform data acquisition from the device?

A. APK Analyzer
B. SDK Manager
C. Android Debug Bridge
D. Xcode

**Answer:** C


**NEW QUESTION 239**
- (Exam Topic 4)
Jacob, a cybercrime investigator, joined a forensics team to participate in a criminal case involving digital evidence. After the investigator collected all the evidence and presents it to the court, the judge dropped the case and the defense attorney pressed charges against Jacob and the rest of the forensics team for unlawful search and seizure. What forensics privacy issue was not addressed prior to collecting the evidence?

A. Compliance with the Second Amendment of the U.
B. Constitution
C. Compliance with the Third Amendment of the U.
D. Constitution
E. None of these
F. Compliance with the Fourth Amendment of the U.
G. Constitution

**Answer:** D


**NEW QUESTION 240**
- (Exam Topic 4)
When Investigating a system, the forensics analyst discovers that malicious scripts were Injected Into benign and trusted websites. The attacker used a web application to send malicious code. In the form of a browser side script, to a different end-user. What attack was performed here?

A. Brute-force attack
B. Cookie poisoning attack
C. Cross-site scripting attack
D. SQL injection attack

**Answer:** C


**NEW QUESTION 243**
- (Exam Topic 4)
Which Federal Rule of Evidence speaks about the Hearsay exception where the availability of the declarant Is immaterial and certain characteristics of the declarant such as present sense Impression, excited utterance, and recorded recollection are also observed while giving their testimony?

A. Rule 801
B. Rule 802
C. Rule 804
D. Rule 803

**Answer:** D


**NEW QUESTION 246**
- (Exam Topic 4)
According to RFC 3227, which of the following is considered as the most volatile item on a typical system?

A. Registers and cache
B. Temporary system files
C. Archival media
D. Kernel statistics and memory

**Answer:** A


**NEW QUESTION 247**
- (Exam Topic 4)
During an Investigation. Noel found a SIM card from the suspect's mobile. The ICCID on the card is 8944245252001451548.
What does the first four digits (89 and 44) In the ICCID represent?

A. TAC and industry identifier
B. Country code and industry identifier
C. Industry identifier and country code
D. Issuer identifier number and TAC

**Answer:** C


**NEW QUESTION 249**
- (Exam Topic 4)
A forensic analyst has been tasked with investigating unusual network activity Inside a retail company's network. Employees complain of not being able to access services, frequent rebooting, and anomalies In log files. The Investigator requested log files from the IT administrator and after carefully reviewing them, he finds the following log entry:

```
12:34:35 192.2.3.4 HEAD GET /login.asp?username=blah" or 1=1 ~ 12:34:35 192.2.3.4 HEAD GET
/login.asp?username=blah"   or )1=1   (--   12:34:35 192.2.3.4   HEAD   GET
/login.asp?username+blah" or exec master..xp_cmdshell 'net user test testpass - -
```

What type of attack was performed on the companies' web application?

A. Directory transversal
B. Unvalidated input
C. Log tampering
D. SQL injection

**Answer:** D


**NEW QUESTION 251**
- (Exam Topic 4)
Which of the following tools will allow a forensic Investigator to acquire the memory dump of a suspect machine so that It may be Investigated on a forensic workstation to collect evidentiary data like processes and Tor browser artifacts?

A. DB Browser SQLite
B. Bulk Extractor
C. Belkasoft Live RAM Capturer and AccessData FTK imager
D. Hex Editor

**Answer:** C


**NEW QUESTION 254**
- (Exam Topic 4)
Consider a scenario where a forensic investigator is performing malware analysis on a memory dump acquired from a victims computer. The investigator uses Volatility Framework to analyze RAM contents; which plugin helps investigator to identify hidden processes or injected code/DLL in the memory dump?

A. pslist
B. malscan
C. mallist
D. malfind

**Answer:** D


**NEW QUESTION 259**
- (Exam Topic 4)
Which OWASP loT vulnerability talks about security flaws such as lack of firmware validation, lack of secure delivery, and lack of anti-rollback mechanisms on loT devices?

A. Lack of secure update mechanism
B. Use of insecure or outdated components
C. Insecure default settings
D. Insecure data transfer and storage

**Answer:** A


**NEW QUESTION 261**
- (Exam Topic 4)
Web browsers can store relevant information from user activities. Forensic investigators may retrieve files, lists, access history, cookies, among other digital footprints. Which tool can contribute to this task?

A. Most Recently Used (MRU) list
B. MZCacheView
C. Google Chrome Recovery Utility
D. Task Manager

**Answer:** B


**NEW QUESTION 264**
- (Exam Topic 4)
Jeff is a forensics investigator for a government agency's cyber security office. Jeff Is tasked with acquiring a memory dump of a Windows 10 computer that was involved In a DDoS attack on the government agency's web application. Jeff is onsite to collect the memory. What tool could Jeff use?

A. Volatility
B. Autopsy
C. RAM Mapper
D. Memcheck

**Answer:** A


**NEW QUESTION 268**
- (Exam Topic 4)
You are an information security analyst at a large pharmaceutical company. While performing a routine review of audit logs, you have noticed a significant amount

of egress traffic to various IP addresses on destination port 22 during off-peak hours. You researched some of the IP addresses and found that many of them are in Eastern Europe. What is the most likely cause of this traffic?

A. Malicious software on internal system is downloading research data from partner 5FTP servers in Eastern Europe
B. Internal systems are downloading automatic Windows updates
C. Data is being exfiltrated by an advanced persistent threat (APT)
D. The organization's primary internal DNS server has been compromised and is performing DNS zone transfers to malicious external entities

**Answer:** C


**NEW QUESTION 269**
- (Exam Topic 4)
A file requires 10 KB space to be saved on a hard disk partition. An entire cluster of 32 KB has been allocated for this file. The remaining, unused space of 22 KB on this cluster will be Identified as .

A. Swap space
B. Cluster space
C. Slack space
D. Sector space

**Answer:** D


**NEW QUESTION 273**
- (Exam Topic 4)
A call detail record (CDR) provides metadata about calls made over a phone service. From the following data fields, which one Is not contained in a CDR.

A. The call duration
B. A unique sequence number identifying the record
C. The language of the call
D. Phone number receiving the call

**Answer:** C


**NEW QUESTION 274**
- (Exam Topic 4)
Maria has executed a suspicious executable file In a controlled environment and wants to see if the file adds/modifies any registry value after execution via Windows Event Viewer. Which of the following event ID should she look for In this scenario?

A. Event ID 4657
B. Event ID 4624
C. Event ID 4688
D. Event ID 7040

**Answer:** A


**NEW QUESTION 278**
- (Exam Topic 4)
Cybercriminals sometimes use compromised computers to commit other crimes, which may involve using computers or networks to spread malware or Illegal Information. Which type of cybercrime stops users from using a device or network, or prevents a company from providing a software service to its customers?

A. Denial-of-Service (DoS) attack
B. Malware attack
C. Ransomware attack
D. Phishing

**Answer:** C


**NEW QUESTION 282**
- (Exam Topic 4)
Which of the following applications will allow a forensic investigator to track the user login sessions and user transactions that have occurred on an MS SQL Server?

A. ApexSQL Audit
B. netcat
C. Notepad++
D. Event Log Explorer

**Answer:** A


**NEW QUESTION 286**
- (Exam Topic 4)
Fill In the missing Master Boot Record component.
* 1. Master boot code
* 2. Partition table
* 3. _____

A. Boot loader

B. Signature word
C. Volume boot record
D. Disk signature

**Answer:** A

**NEW QUESTION 290**
- (Exam Topic 4)
Assume there Is a file named myflle.txt In C: drive that contains hidden data streams. Which of the following commands would you Issue to display the contents of a data stream?

A. echo text > program: source_file
B. myfile.dat: st ream 1
C. C:\MORE < myfile.txt:siream1
D. C:\>ECHO text_message > myfile.txt:stream1

**Answer:** A

**NEW QUESTION 294**
- (Exam Topic 4)
"To ensure that the digital evidence is collected, preserved, examined, or transferred In a manner safeguarding the accuracy and reliability of the evidence, law enforcement, and forensics organizations must establish and maintain an effective quality system" Is a principle established by:

A. NCIS
B. NIST
C. EC-Council
D. SWGDE

**Answer:** B

**NEW QUESTION 297**
- (Exam Topic 4)
Fred, a cybercrime Investigator for the FBI, finished storing a solid-state drive In a static resistant bag and filled out the chain of custody form. Two days later. John grabbed the solid-state drive and created a clone of It (with write blockers enabled) In order to Investigate the drive. He did not document the chain of custody though. When John was finished, he put the solid-state drive back in the static resistant and placed it back in the evidence locker. A day later, the court trial began and upon presenting the evidence and the supporting documents, the chief Justice outright rejected them. Which of the following statements strongly support the reason for rejecting the evidence?

A. Block clones cannot be created with solid-state drives
B. Write blockers were used while cloning the evidence
C. John did not document the chain of custody
D. John investigated the clone instead of the original evidence itself

**Answer:** C

**NEW QUESTION 300**
- (Exam Topic 4)
Harry has collected a suspicious executable file from an infected system and seeks to reverse its machine code to Instructions written in assembly language. Which tool should he use for this purpose?

A. Ollydbg
B. oledump
C. HashCalc
D. BinText

**Answer:** A

**NEW QUESTION 302**
- (Exam Topic 4)
A cybercriminal is attempting to remove evidence from a Windows computer. He deletes the file evldence1.doc. sending it to Windows Recycle Bin. The cybercriminal then empties the Recycle Bin. After having been removed from the Recycle Bin. what will happen to the data?

A. The data will remain in its original clusters until it is overwritten
B. The data will be moved to new clusters in unallocated space
C. The data will become corrupted, making it unrecoverable
D. The data will be overwritten with zeroes

**Answer:** A

**NEW QUESTION 304**
- (Exam Topic 4)
Jack is reviewing file headers to verify the file format and hopefully find more Information of the file. After a careful review of the data chunks through a hex editor; Jack finds the binary value Oxffd8ff. Based on the above Information, what type of format is the file/image saved as?

A. BMP
B. GIF
C. ASCII

D. JPEG

**Answer:** D


**NEW QUESTION 307**
- (Exam Topic 4)
Williamson is a forensic investigator. While investigating a case of data breach at a company, he is maintaining a document that records details such as the forensic processes applied on the collected evidence, particulars of people handling It. the dates and times when it Is being handled, and the place of storage of the evidence. What do you call this document?

A. Consent form
B. Log book
C. Authorization form
D. Chain of custody

**Answer:** D


**NEW QUESTION 308**
- (Exam Topic 4)
Donald made an OS disk snapshot of a compromised Azure VM under a resource group being used by the affected company as a part of forensic analysis process. He then created a vhd file out of the snapshot and stored it in a file share and as a page blob as backup in a storage account under different region. What Is the next thing he should do as a security measure?

A. Recommend changing the access policies followed by the company
B. Delete the snapshot from the source resource group
C. Delete the OS disk of the affected VM altogether
D. Create another VM by using the snapshot

**Answer:** C


**NEW QUESTION 311**
- (Exam Topic 4)
A breach resulted from a malware attack that evaded detection and compromised the machine memory without installing any software or accessing the hard drive. What technique did the adversaries use to deliver the attack?

A. Fileless
B. Trojan
C. JavaScript
D. Spyware

**Answer:** A


**NEW QUESTION 312**
- (Exam Topic 4)
When installed on a Windows machine, which port does the Tor browser use to establish a network connection via Tor nodes?

A. 7680
B. 49667/49668
C. 9150/9151
D. 49664/49665

**Answer:** C


**NEW QUESTION 315**
- (Exam Topic 4)
For the purpose of preserving the evidentiary chain of custody, which of the following labels is not appropriate?

A. Relevant circumstances surrounding the collection
B. General description of the evidence
C. Exact location the evidence was collected from
D. SSN of the person collecting the evidence

**Answer:** D


**NEW QUESTION 317**
- (Exam Topic 4)
SO/IEC 17025 is an accreditation for which of the following:

A. CHFI issuing agency
B. Encryption
C. Forensics lab licensing
D. Chain of custody

**Answer:** C


**NEW QUESTION 322**

- (Exam Topic 4)
Recently, an Internal web app that a government agency utilizes has become unresponsive, Betty, a network engineer for the government agency, has been tasked to determine the cause of the web application's unresponsiveness. Betty launches WIreshark and begins capturing the traffic on the local network. While analyzing the results, Betty noticed that a syn flood attack was underway. How did Betty know a syn flood attack was occurring?

A. Wireshark capture shows multiple ACK requests and SYN responses from single/multiple IP address(es)
B. Wireshark capture does not show anything unusual and the issue is related to the web application
C. Wireshark capture shows multiple SYN requests and RST responses from single/multiple IP address(es)
D. Wireshark capture shows multiple SYN requests and ACK responses from single/multiple IP address(es)

**Answer:** C


**NEW QUESTION 327**
- (Exam Topic 4)
Robert needs to copy an OS disk snapshot of a compromised VM to a storage account in different region for further investigation. Which of the following should he use in this scenario?

A. Azure CLI
B. Azure Monitor
C. Azure Active Directory
D. Azure Portal

**Answer:** D


**NEW QUESTION 328**
- (Exam Topic 4)
Identify the location of Recycle Bin on a Windows 7 machine that uses NTFS file system to store and retrieve files on the hard disk.

A. Drive:\$Recycle.Bin
B. DriveARECYCLER
C. C:\RECYCLED
D. DriveARECYCLED

**Answer:** A


**NEW QUESTION 332**
- (Exam Topic 4)
Which of the following tools is used to dump the memory of a running process, either immediately or when an error condition occurs?

A. FATKit
B. Coreography
C. Belkasoft Live RAM Capturer
D. CacheInf

**Answer:** C


**NEW QUESTION 336**
- (Exam Topic 4)
An Investigator Is checking a Cisco firewall log that reads as follows:
Aug 21 2019 09:16:44: %ASA-1-106021: Deny ICMP reverse path check from 10.0.0.44 to 10.0.0.33 on Interface outside
What does %ASA-1-106021 denote?

A. Mnemonic message
B. Type of traffic
C. Firewall action
D. Type of request

**Answer:** C


**NEW QUESTION 340**
- (Exam Topic 4)
"In exceptional circumstances, where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to explain his/her actions and the impact of those actions on the evidence, in the court." Which ACPO principle states this?

A. Principle 1
B. Principle 3
C. Principle 4
D. Principle 2

**Answer:** D


**NEW QUESTION 344**
- (Exam Topic 4)
Debbie has obtained a warrant to search a known pedophiles house. Debbie went to the house and executed the search warrant to seize digital devices that have been recorded as being used for downloading Illicit Images. She seized all digital devices except a digital camera. Why did she not collect the digital camera?

A. The digital camera was not listed as one of the digital devices in the warrant

B. The vehicle Debbie was using to transport the evidence was already full and could not carry more items
C. Debbie overlooked the digital camera because it is not a computer system
D. The digital camera was ol
E. had a cracked screen, and did not have batterie
F. Therefore, it could not have been used in a crime.

**Answer:** A


**NEW QUESTION 345**
- (Exam Topic 4)
Malware analysis can be conducted in various manners. An investigator gathers a suspicious executable file and uploads It to VirusTotal in order to confirm whether the file Is malicious, provide information about Its functionality, and provide Information that will allow to produce simple network signatures. What type of malware analysis was performed here?

A. Static
B. Volatile
C. Dynamic
D. Hybrid

**Answer:** D


**NEW QUESTION 350**
- (Exam Topic 4)
Choose the layer in iOS architecture that provides frameworks for iOS app development?

A. Media services
B. Cocoa Touch
C. Core services
D. Core OS

**Answer:** C


**NEW QUESTION 353**
- (Exam Topic 3)
In a computer that has Dropbox client installed, which of the following files related to the Dropbox client store information about local Dropbox installation and the Dropbox user account, along with email IDs linked with the account?

A. config.db
B. install.db
C. sigstore.db
D. filecache.db

**Answer:** A


**NEW QUESTION 357**
- (Exam Topic 3)
An investigator is analyzing a checkpoint firewall log and comes across symbols. What type of log is he looking at?



A. Security event was monitored but not stopped
B. Malicious URL detected
C. An email marked as potential spam
D. Connection rejected

**Answer:** C


**NEW QUESTION 362**
- (Exam Topic 3)
Which principle states that "anyone or anything, entering a crime scene takes something of the scene with them, and leaves something of themselves behind when they leave"?

A. Locard's Exchange Principle
B. Enterprise Theory of Investigation
C. Locard's Evidence Principle
D. Evidence Theory of Investigation

**Answer:** A


**NEW QUESTION 365**
- (Exam Topic 3)
Select the data that a virtual memory would store in a Windows-based system.

A. Information or metadata of the files
B. Documents and other files
C. Application data
D. Running processes

**Answer:** D


**NEW QUESTION 369**
- (Exam Topic 3)
Which of the following file system uses Master File Table (MFT) database to store information about every file and directory on a volume?

A. FAT File System
B. ReFS
C. exFAT
D. NTFS File System

**Answer:** D


**NEW QUESTION 373**
- (Exam Topic 3)
The Recycle Bin exists as a metaphor for throwing files away, but it also allows a user to retrieve and restore files. Once the file is moved to the recycle bin, a record is added to the log file that exists in the Recycle Bin. Which of the following files contains records that correspond to each deleted file in the Recycle Bin?

A. INFO2
B. INFO1
C. LOGINFO1
D. LOGINFO2

**Answer:** D


**NEW QUESTION 377**
- (Exam Topic 3)
An investigator has found certain details after analysis of a mobile device. What can reveal the manufacturer information?

A. Equipment Identity Register (EIR)
B. Electronic Serial Number (ESN)
C. International mobile subscriber identity (IMSI)
D. Integrated circuit card identifier (ICCID)

**Answer:** B


**NEW QUESTION 378**
- (Exam Topic 3)
Which ISO Standard enables laboratories to demonstrate that they comply with quality assurance and provide valid results?

A. ISO/IEC 16025
B. ISO/IEC 18025
C. ISO/IEC 19025
D. ISO/IEC 17025

**Answer:** D


**NEW QUESTION 380**
- (Exam Topic 3)
What system details can an investigator obtain from the NetBIOS name table cache?

A. List of files opened on other systems
B. List of the system present on a router
C. List of connections made to other systems
D. List of files shared between the connected systems

**Answer:** C


**NEW QUESTION 384**
- (Exam Topic 3)
What do you call the process of studying the changes that have taken place across a system or a machine after a series of actions or incidents?

A. Windows Services Monitoring
B. System Baselining
C. Start-up Programs Monitoring
D. Host integrity Monitoring

**Answer:** D


**NEW QUESTION 387**

- (Exam Topic 3)
Hard disk data addressing is a method of allotting addresses to each ___ of data on a hard disk.

A. Physical block
B. Operating system block
C. Hard disk block
D. Logical block

**Answer:** A


**NEW QUESTION 392**
- (Exam Topic 3)
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. Locard's Principle
D. Hearsay

**Answer:** B


**NEW QUESTION 395**
- (Exam Topic 3)
Raw data acquisition format creates ___ of a data set or suspect drive.

A. Segmented image files
B. Simple sequential flat files
C. Compressed image files
D. Segmented files

**Answer:** B


**NEW QUESTION 396**
- (Exam Topic 3)
What does the bytes 0x0B-0x53 represent in the boot sector of NTFS volume on Windows 2000?

A. Jump instruction and the OEM ID
B. BIOS Parameter Block (BPB) and the OEM ID
C. BIOS Parameter Block (BPB) and the extended BPB
D. Bootstrap code and the end of the sector marker

**Answer:** C


**NEW QUESTION 400**
- (Exam Topic 3)
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 shutting down a computer from a powered-on or on 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 starting a computer from a powered-down or off state

**Answer:** D


**NEW QUESTION 405**
- (Exam Topic 3)
Which among the following U.S. laws requires financial institutions—companies that offer consumers financial products or services such as loans, financial or investment advice, or insurance—to protect their customers' information against security threats?

A. SOX
B. HIPAA
C. GLBA
D. FISMA

**Answer:** C


**NEW QUESTION 410**
- (Exam Topic 3)
What document does the screenshot represent?

A. Expert witness form
B. Search warrant form
C. Chain of custody form
D. Evidence collection form

**Answer:** D

**NEW QUESTION 412**
- (Exam Topic 3)
Ron, a computer forensics expert, is investigating a case involving corporate espionage. He has recovered several mobile computing devices from the crime scene. One of the evidence that Ron possesses is a mobile phone from Nokia that was left in ON condition. Ron needs to recover the IMEI number of the device to establish the identity of the device owner. Which of the following key combinations can he use to recover the IMEI number?

A. #*06*#
B. *#06#
C. #06#*
D. *IMEI#

**Answer:** A

**NEW QUESTION 413**
- (Exam Topic 3)
Which forensic investigation methodology believes that criminals commit crimes solely to benefit their
criminal enterprises?

A. Scientific Working Group on Digital Evidence
B. Daubert Standard
C. Enterprise Theory of Investigation
D. Fyre Standard

**Answer:** C

**NEW QUESTION 418**
- (Exam Topic 3)
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. Hex Editor
B. Internet Evidence Finder
C. Process Monitor
D. Report Viewer

**Answer:** C

**NEW QUESTION 423**
- (Exam Topic 3)
Email archiving is a systematic approach to save and protect the data contained in emails so that it can be accessed fast at a later date. There are two main archive types, namely Local Archive and Server Storage Archive. Which of the following statements is correct while dealing with local archives?

A. Server storage archives are the server information and settings stored on a local system, whereas the local archives are the local email client information stored on the mail server
B. It is difficult to deal with the webmail as there is no offline archive in most case
C. So consult your counsel on the case as to the best way to approach and gain access to the required data on servers
D. Local archives should be stored together with the server storage archives in order to be admissible in a court of law
E. Local archives do not have evidentiary value as the email client may alter the message data

**Answer:** B

**NEW QUESTION 426**
- (Exam Topic 3)
Smith is an IT technician that has been appointed to his company's network vulnerability assessment team. He is the only IT employee on the team. The other team members include employees from
Accounting, Management, Shipping, and Marketing. Smith and the team members are having their first meeting to discuss how they will proceed. What is the first step they should do to create the network
vulnerability assessment plan?

A. Their first step is to make a hypothesis of what their final findings will be.
B. Their first step is to create an initial Executive report to show the management team.
C. Their first step is to analyze the data they have currently gathered from the company or interviews.
D. Their first step is the acquisition of required documents, reviewing of security policies and compliance.

**Answer:** D


**NEW QUESTION 431**
- (Exam Topic 3)
What is the purpose of using Obfuscator in malware?

A. Execute malicious code in the system
B. Avoid encryption while passing through a VPN
C. Avoid detection by security mechanisms
D. Propagate malware to other connected devices

**Answer:** C


**NEW QUESTION 436**
- (Exam Topic 3)
What malware analysis operation can the investigator perform using the jv16 tool?

A. Files and Folder Monitor
B. Installation Monitor
C. Network Traffic Monitoring/Analysis
D. Registry Analysis/Monitoring

**Answer:** D


**NEW QUESTION 440**
- (Exam Topic 3)
An investigator has extracted the device descriptor for a 1GB thumb drive that looks like: Disk&Ven_Best_Buy&Prod_Geek_Squad_U3&Rev_6.15. What does the "Geek_Squad" part represent?

A. Product description
B. Manufacturer Details
C. Developer description
D. Software or OS used

**Answer:** A


**NEW QUESTION 444**
- (Exam Topic 3)
Which of the following does not describe the type of data density on a hard disk?

A. Volume density
B. Track density
C. Linear or recording density
D. Areal density

**Answer:** A


**NEW QUESTION 447**
- (Exam Topic 3)
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 spamming
B. Phishing
C. Email spoofing
D. Mail bombing

**Answer:** D


**NEW QUESTION 449**
- (Exam Topic 3)
Which of the following is a non-zero data that an application allocates on a hard disk cluster in systems running on Windows OS?

A. Sparse File
B. Master File Table
C. Meta Block Group
D. Slack Space

**Answer:** B


## NEW QUESTION 450
- (Exam Topic 3)
What is an investigator looking for in the rp.log file stored in a system running on Windows 10 operating system?

A. Restore point interval
B. Automatically created restore points
C. System CheckPoints required for restoring
D. Restore point functions

**Answer:** C


## NEW QUESTION 453
- (Exam Topic 3)
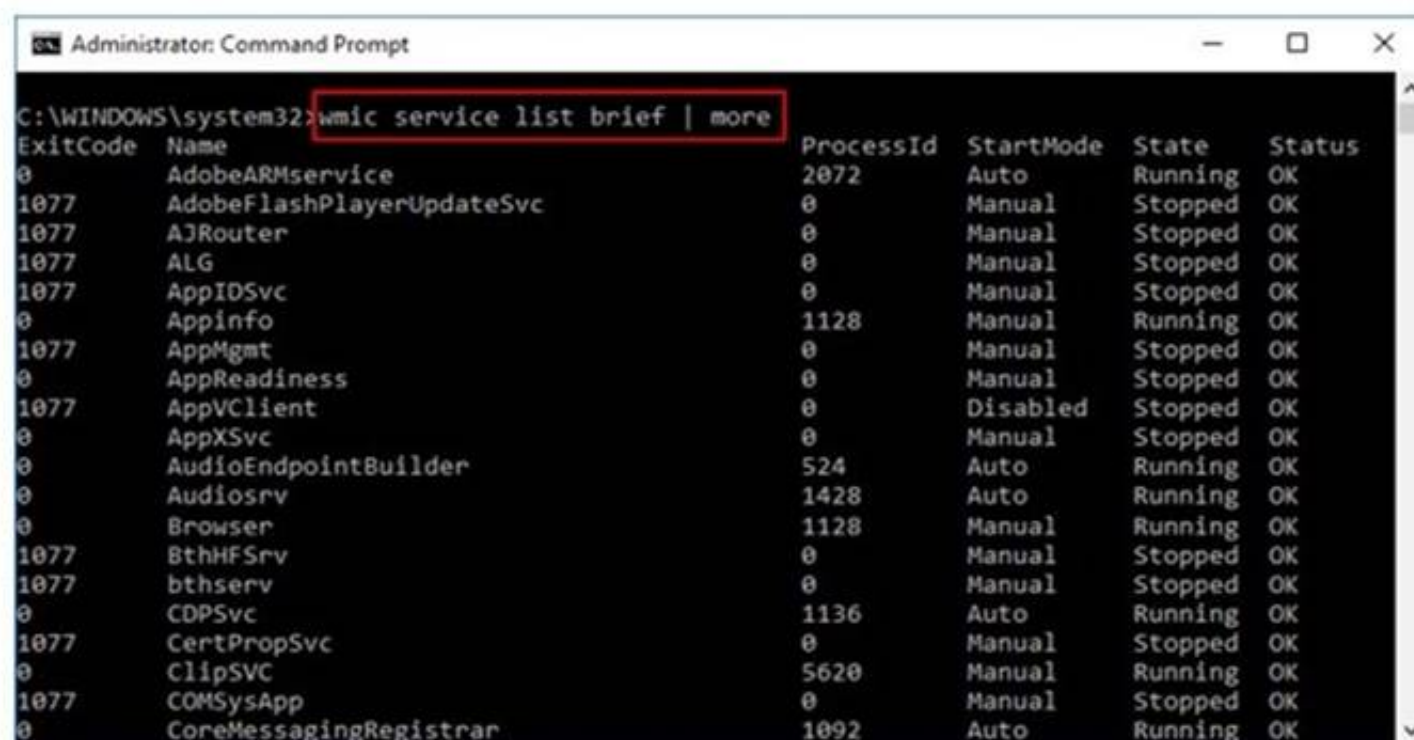What is the name of the first reserved sector in File allocation table?

A. Volume Boot Record
B. Partition Boot Sector
C. Master Boot Record
D. BIOS Parameter Block

**Answer:** C


## NEW QUESTION 457
- (Exam Topic 3)
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 closed recently
C. List of services recently started
D. List of services installed

**Answer:** D


## NEW QUESTION 460
- (Exam Topic 3)
During an investigation of an XSS attack, the investigator comes across the term "[a-zA-Z0-9\%]+" in analyzed evidence details. What is the expression used for?

A. Checks for upper and lower-case alphanumeric string inside the tag, or its hex representation
B. Checks for forward slash used in HTML closing tags, its hex or double-encoded hex equivalent
C. Checks for opening angle bracket, its hex or double-encoded hex equivalent
D. Checks for closing angle bracket, hex or double-encoded hex equivalent

**Answer:** B


## NEW QUESTION 461
- (Exam Topic 3)
In which registry does the system store the Microsoft security IDs?

A. HKEY_CLASSES_ROOT (HKCR)
B. HKEY_CURRENT_CONFIG (HKCC)
C. HKEY_CURRENT_USER (HKCU)
D. HKEY_LOCAL_MACHINE (HKLM)

**Answer:** D


## NEW QUESTION 464
- (Exam Topic 3)
Which of the following is NOT an anti-forensics technique?

A. Data Deduplication
B. Steganography
C. Encryption
D. Password Protection

**Answer:** A


## NEW QUESTION 466
- (Exam Topic 3)
Which command can provide the investigators with details of all the loaded modules on a Linux-based system?

A. list modules -a
B. lsmod
C. plist mod -a
D. lsof -m

**Answer:** B


## NEW QUESTION 468
- (Exam Topic 3)
Adam, a forensic analyst, is preparing VMs for analyzing a malware. Which of the following is NOT a best practice?

A. Isolating the host device
B. Installing malware analysis tools
C. Using network simulation tools
D. Enabling shared folders

**Answer:** D


## NEW QUESTION 470
- (Exam Topic 3)
Which U.S. law sets the rules for sending emails for commercial purposes, establishes the minimum requirements for commercial messaging, gives the recipients of emails the right to ask the senders to stop emailing them, and spells out the penalties in case the above said rules are violated?

A. NO-SPAM Act
B. American: NAVSO P-5239-26 (RLL)
C. CAN-SPAM Act
D. American: DoD 5220.22-M

**Answer:** C


## NEW QUESTION 475
- (Exam Topic 3)
POP3 is an Internet protocol, which is used to retrieve emails from a mail server. Through which port does an email client connect with a POP3 server?

A. 110
B. 143
C. 25
D. 993

**Answer:** A


## NEW QUESTION 480
- (Exam Topic 3)
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 sequence numbers are specified
B. Start and end points for log files are not specified
C. Start and end points for log files are specified
D. Start and end points for log sequence numbers are not specified

**Answer:** B

**NEW QUESTION 481**
- (Exam Topic 3)
When a user deletes a file, the system creates a $I file to store its details. What detail does the $I file not contain?

A. File Size
B. File origin and modification
C. Time and date of deletion
D. File Name

**Answer:** B

**NEW QUESTION 485**
- (Exam Topic 3)
Which of the following statements is TRUE with respect to the Registry settings in the user start-up folder
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce\.

A. All the values in this subkey run when specific user logs on, as this setting is user-specific
B. The string specified in the value run executes when user logs on
C. All the values in this key are executed at system start-up
D. All values in this subkey run when specific user logs on and then the values are deleted

**Answer:** D

**NEW QUESTION 486**
- (Exam Topic 3)
Which of the following Linux command searches through the current processes and lists the process IDs those match the selection criteria to stdout?

A. pstree
B. pgrep
C. ps
D. grep

**Answer:** B

**NEW QUESTION 489**
- (Exam Topic 3)
Which of the following application password cracking tool can discover all password-protected items on a computer and decrypts them?

A. TestDisk for Windows
B. R-Studio
C. Windows Password Recovery Bootdisk
D. Passware Kit Forensic

**Answer:** D

**NEW QUESTION 491**
- (Exam Topic 3)
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 deletion
B. Disk cleaning
C. Disk degaussing
D. Disk magnetization

**Answer:** C

**NEW QUESTION 495**
- (Exam Topic 3)
Which of the following is a precomputed table containing word lists like dictionary files and brute force lists and their hash values?

A. Directory Table
B. Rainbow Table
C. Master file Table (MFT)
D. Partition Table

**Answer:** B

**NEW QUESTION 499**
- (Exam Topic 3)
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. Core Services
B. Media services
C. Cocoa Touch
D. Core OS

**Answer:** D


**NEW QUESTION 500**
- (Exam Topic 3)
Centralized binary logging is a process in which many websites write binary and unformatted log data to a single log file. What extension should the investigator look to find its log file?

A. .cbl
B. .log
C. .ibl
D. .txt

**Answer:** C


**NEW QUESTION 505**
- (Exam Topic 3)
One technique for hiding information is to change the file extension from the correct one to the 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 header
B. The File Allocation Table
C. The file footer
D. The sector map

**Answer:** A


**NEW QUESTION 507**
- (Exam Topic 3)
You are working as an independent computer forensics investigator and received a call from a systems administrator for a local school system requesting your assistance. One of the students at the local high school is suspected of downloading inappropriate images from the Internet to a PC in the Computer Lab. When you arrive at the school, the systems administrator hands you a hard drive and tells you that he made a "simple backup copy" of the hard drive in the PC and put it on this drive and requests that you examine the drive for evidence of the suspected images. You inform him that a "simple backup copy" will not provide deleted files or recover file fragments. What type of copy do you need to make to ensure that the evidence found is complete and admissible in future proceeding?

A. Robust copy
B. Incremental backup copy
C. Bit-stream copy
D. Full backup copy

**Answer:** C


**NEW QUESTION 509**
- (Exam Topic 3)
Which of the following standard represents a legal precedent set in 1993 by the Supreme Court of the United States regarding the admissibility of expert witnesses' testimony during federal legal proceedings?

A. SWGDE & SWGIT
B. IOCE
C. Frye
D. Daubert

**Answer:** D


**NEW QUESTION 511**
- (Exam Topic 3)
What is the capacity of Recycle bin in a system running on Windows Vista?

A. 2.99GB
B. 3.99GB
C. Unlimited
D. 10% of the partition space

**Answer:** C


**NEW QUESTION 514**
- (Exam Topic 3)
Which among the following web application threats is resulted when developers expose various internal implementation objects, such as files, directories, database records, or key-through references?

A. Remote File Inclusion
B. Cross Site Scripting
C. Insecure Direct Object References
D. Cross Site Request Forgery

**Answer:** C

**NEW QUESTION 518**
- (Exam Topic 3)
Which of the following does Microsoft Exchange E-mail Server use for collaboration of various e-mail applications?

A. Simple Mail Transfer Protocol (SMTP)
B. Messaging Application Programming Interface (MAPI)
C. Internet Message Access Protocol (IMAP)
D. Post Office Protocol version 3 (POP3)

**Answer:** B


**NEW QUESTION 522**
- (Exam Topic 3)
In which of these attacks will a steganalyst use a random message to generate a stego-object by using some steganography tool, to find the steganography algorithm used to hide the information?

A. Chosen-message attack
B. Known-cover attack
C. Known-message attack
D. Known-stego attack

**Answer:** A


**NEW QUESTION 525**
- (Exam Topic 3)
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. PTP
C. Time Protocol
D. NTP

**Answer:** D


**NEW QUESTION 526**
- (Exam Topic 3)
Which among the following tools can help a forensic investigator to access the registry files during postmortem analysis?

A. RegistryChangesView
B. RegDIIView
C. RegRipper
D. ProDiscover

**Answer:** C


**NEW QUESTION 528**
- (Exam Topic 3)
Which component in the hard disk moves over the platter to read and write information?

A. Actuator
B. Spindle
C. Actuator Axis
D. Head

**Answer:** D


**NEW QUESTION 531**
- (Exam Topic 3)
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. PEiD
C. Comodo Programs Manager
D. Dependency Walker

**Answer:** B


**NEW QUESTION 536**
- (Exam Topic 3)
Which of the following stand true for BIOS Parameter Block?

A. The BIOS Partition Block describes the physical layout of a data storage volume
B. The BIOS Partition Block is the first sector of a data storage device
C. The length of BIOS Partition Block remains the same across all the file systems
D. The BIOS Partition Block always refers to the 512-byte boot sector

**Answer:** A


**NEW QUESTION 541**
- (Exam Topic 3)
Which of the following is a MAC-based File Recovery Tool?

A. VirtualLab
B. GetDataBack
C. Cisdem DataRecovery 3
D. Smart Undeleter

**Answer:** C


**NEW QUESTION 546**
- (Exam Topic 3)
Graphics Interchange Format (GIF) is a RGB bitmap image format for images with up to 256 distinct colors per frame.

A. 8-bit
B. 32-bit
C. 16-bit
D. 24-bit

**Answer:** A


**NEW QUESTION 547**
- (Exam Topic 3)
Jim's company regularly performs backups of their critical servers. But the company can't afford to send backup tapes to an off-site vendor for long term storage and archiving. Instead Jim's company keeps the backup tapes in a safe in the office. Jim's company is audited each year, and the results from this year's audit show a risk because backup tapes aren't stored off-site. The Manager of Information Technology has a plan to take the backup tapes home with him and wants to know what two things he can do to secure the backup tapes while in transit?

A. Encrypt the backup tapes and use a courier to transport them.
B. Encrypt the backup tapes and transport them in a lock box
C. Degauss the backup tapes and transport them in a lock box.
D. Hash the backup tapes and transport them in a lock box.

**Answer:** B


**NEW QUESTION 549**
- (Exam Topic 3)
Which of the following is a device monitoring tool?

A. Capsa
B. Driver Detective
C. Regshot
D. RAM Capturer

**Answer:** A


**NEW QUESTION 550**
- (Exam Topic 3)
Which of the following techniques delete the files permanently?

A. Steganography
B. Artifact Wiping
C. Data Hiding
D. Trail obfuscation

**Answer:** B


**NEW QUESTION 555**
- (Exam Topic 3)
As a part of the investigation, Caroline, a forensic expert, was assigned the task to examine the transaction logs pertaining to a database named Transfers. She used SQL Server Management Studio to collect the active transaction log files of the database. Caroline wants to extract detailed information on the logs, including AllocUnitId, page id, slot id, etc. Which of the following commands does she need to execute in order to extract the desired information?

A. DBCC LOG(Transfers, 1)
B. DBCC LOG(Transfers, 3)
C. DBCC LOG(Transfers, 0)
D. DBCC LOG(Transfers, 2)

**Answer:** D


**NEW QUESTION 557**
- (Exam Topic 3)

Which of these ISO standards define the file system for optical storage media, such as CD-ROM and DVD-ROM?

A. ISO 9660
B. ISO 13346
C. ISO 9960
D. ISO 13490

**Answer:** A


**NEW QUESTION 560**
- (Exam Topic 3)
Which of the following files contains the traces of the applications installed, run, or uninstalled from a system?

A. Virtual Files
B. Image Files
C. Shortcut Files
D. Prefetch Files

**Answer:** C


**NEW QUESTION 564**
- (Exam Topic 3)
To reach a bank web site, the traffic from workstations must pass through a firewall. You have been asked to review the firewall configuration to ensure that workstations in network 10.10.10.0/24 can only reach the bank web site 10.20.20.1 using https. Which of the following firewall rules meets this requirement?

A. if (source matches 10.10.10.0/24 and destination matches 10.20.20.1 and port matches 443) then permit
B. if (source matches 10.10.10.0/24 and destination matches 10.20.20.1 and port matches 80 or 443) then permit
C. if (source matches 10.10.10.0 and destination matches 10.20.20.1 and port matches 443) then permit

**Answer:** A


**NEW QUESTION 568**
- (Exam Topic 3)
Which of the following is a part of a Solid-State Drive (SSD)?

A. Head
B. Cylinder
C. NAND-based flash memory
D. Spindle

**Answer:** C


**NEW QUESTION 569**
- (Exam Topic 3)
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 purely technical and are not considered forms of social engineering
B. In a pharming attack a victim is redirected to a fake website by modifying their host configuration file or by exploiting vulnerabilities in DN
C. 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
D. In a phishing attack a victim is redirected to a fake website by modifying their host configuration file or by exploiting vulnerabilities in DN
E. 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
F. Both pharming and phishing attacks are identical

**Answer:** B


**NEW QUESTION 574**
- (Exam Topic 3)
Which Event Correlation approach assumes and predicts what an attacker can do next after the attack by studying statistics and probability?

A. Profile/Fingerprint-Based Approach
B. Bayesian Correlation
C. Time (Clock Time) or Role-Based Approach
D. Automated Field Correlation

**Answer:** B


**NEW QUESTION 578**
- (Exam Topic 3)
Which of the following is found within the unique instance ID key and helps investigators to map the entry from USBSTOR key to the MountedDevices key?

A. ParentIDPrefix
B. LastWrite
C. UserAssist key
D. MRUListEx key

**Answer:** A

**NEW QUESTION 579**
- (Exam Topic 3)
The Apache server saves diagnostic information and error messages that it encounters while processing requests. The default path of this file is usr/local/apache/logs/error.log in Linux. Identify the Apache error log from the following logs.

A. http://victim.com/scripts/..%c0%af../..%c0%af../..%c0%af../..%c0%af../..%c0%af../..%c0%af../..%c0%af../winnt/system32/cmd.exe?/c+dir+C:\Winnt\system32\Logfiles\W3SVC1
B. [Wed Oct 11 14:32:52 2000] [error] [client 127.0.0.1] client denied by server configuration:/export/home/live/ap/htdocs/test
C. 127.0.0.1 - frank [10/Oct/2000:13:55:36 -0700]"GET /apache_pb.gif HTTP/1.0" 200 2326
D. 127.0.0.1 - - [10/Apr/2007:10:39:11 +0300] ] [error] "GET /apache_pb.gif HTTP/1.0" 200 2326

**Answer:** B


**NEW QUESTION 582**
- (Exam Topic 3)
Identify the term that refers to individuals who, by virtue of their knowledge and expertise, express an independent opinion on a matter related to a case based on the information that is provided.

A. Expert Witness
B. Evidence Examiner
C. Forensic Examiner
D. Defense Witness

**Answer:** A


**NEW QUESTION 587**
- (Exam Topic 3)
Checkpoint Firewall logs can be viewed through a Check Point Log viewer that uses icons and colors in the log table to represent different security events and their severity. What does the icon in the checkpoint logs represent?

A. The firewall rejected a connection
B. A virus was detected in an email
C. The firewall dropped a connection
D. An email was marked as potential spam

**Answer:** C


**NEW QUESTION 591**
- (Exam Topic 3)
In Windows, prefetching is done to improve system performance. There are two types of prefetching: boot prefetching and application prefetching. During boot prefetching, what does the Cache Manager do?

A. Determines the data associated with value EnablePrefetcher
B. Monitors the first 10 seconds after the process is started
C. Checks whether the data is processed
D. Checks hard page faults and soft page faults

**Answer:** C


**NEW QUESTION 593**
- (Exam Topic 3)
Which part of Metasploit framework helps users to hide the data related to a previously deleted file or currently unused by the allocated file.

A. Waffen FS
B. RuneFS
C. FragFS
D. Slacker

**Answer:** D


**NEW QUESTION 598**
- (Exam Topic 3)
Which of the following file formats allows the user to compress the acquired data as well as keep it randomly accessible?

A. Proprietary Format
B. Generic Forensic Zip (gfzip)
C. Advanced Forensic Framework 4
D. Advanced Forensics Format (AFF)

**Answer:** B


**NEW QUESTION 599**
- (Exam Topic 2)
Given the drive dimensions as follows and assuming a sector has 512 bytes, what is the capacity of the described hard drive?
22,164 cylinders/disk
80 heads/cylinder

63 sectors/track

A. 53.26 GB
B. 57.19 GB
C. 11.17 GB
D. 10 GB

**Answer:** A


## NEW QUESTION 600

- (Exam Topic 2)
Where is the startup configuration located on a router?

A. Static RAM
B. BootROM
C. NVRAM
D. Dynamic RAM

**Answer:** C


## NEW QUESTION 603

- (Exam Topic 2)
What must an investigator do before disconnecting an iPod from any type of computer?

A. Unmount the iPod
B. Mount the iPod
C. Disjoin the iPod
D. Join the iPod

**Answer:** A


## NEW QUESTION 608

- (Exam Topic 2)
In the following email header, where did the email first originate from?

```
Microsoft Mail Internet Headers Version 2.0
Received: from smtp1.somedomain.com ([199.190.129.133]) by somedomain.com
with Microsoft SMTPSVC(6.0.3790.1830);
        Fri, 1 Jun 2007 09:43:08 -0500
Received: from david1.state.us.gov.us (david1.state.ok.gov [172.16.28.115])
        by smtp1.somedomain.com (8.13.1/8.12.11) with ESMTP id l51EfCEh032241
        for <someone@somedomain.com>; Fri, 1 Jun 2007 09:41:13 -0500
Received: from simon1.state.ok.gov.us ([172.18.0.199]) by
david1.state.ok.gov.us with Microsoft SMTPSVC(6.0.3790.1830);
        Fri, 1 Jun 2007 09:41:13 -0500
X-Ninja-PIM: Scanned by Ninja
X-Ninja-AttachmentFiltering: (no action)
X-MimeOLE: Produced By Microsoft Exchange V6.5.7235.2
Content-class: urn:content-classes:message
Return-Receipt-To: "Johnson, Jimmy" <jimmy@somewherelese.com>
MIME-Version: 1.0
```

A. Somedomain.com
B. Smtp1.somedomain.com
C. Simon1.state.ok.gov.us
D. David1.state.ok.gov.us

**Answer:** C


## NEW QUESTION 610

- (Exam Topic 2)
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. Microsoft Outlook
B. Eudora
C. Mozilla Thunderbird
D. Microsoft Outlook Express

**Answer:** D


## NEW QUESTION 615

- (Exam Topic 2)
What type of analysis helps to identify the time and sequence of events in an investigation?

A. Time-based
B. Functional
C. Relational
D. Temporal

**Answer:** D

**NEW QUESTION 620**
- (Exam Topic 2)
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 1
C. Increased by 1
D. Decreased by 2

**Answer:** C

**NEW QUESTION 621**
- (Exam Topic 2)
Netstat is a tool for collecting information regarding network connections. It provides a simple view of TCP and UDP connections, and their state and network traffic statistics. Which of the following commands shows you the TCP and UDP network connections, listening ports, and the identifiers?

A. netstat – r
B. netstat – ano
C. netstat – b
D. netstat – s

**Answer:** B

**NEW QUESTION 624**
- (Exam Topic 2)
Under confession, an accused criminal admitted to encrypting child pornography pictures and then hiding them within other pictures. What technique did the accused criminal employ?

A. Typography
B. Steganalysis
C. Picture encoding
D. Steganography

**Answer:** D

**NEW QUESTION 625**
- (Exam Topic 2)
Cylie is investigating a network breach at a state organization in Florida. She discovers that the intruders were able to gain access into the company firewalls by overloading them with IP packets. Cylie then discovers through her investigation that the intruders hacked into the company phone system and used the hard drives on their PBX system to store shared music files. What would this attack on the company PBX system be called?

A. Phreaking
B. Squatting
C. Crunching
D. Pretexting

**Answer:** A

**NEW QUESTION 630**
- (Exam Topic 2)
Which program is the bootloader when Windows XP starts up?

A. KERNEL.EXE
B. NTLDR
C. LOADER
D. LILO

**Answer:** B

**NEW QUESTION 635**
- (Exam Topic 2)
Jack Smith is a forensics investigator who works for Mason Computer Investigation Services. He is investigating a computer that was infected by Ramen Virus.

```
C:\WINDOWS\system32\cmd.exe

C:\>netstat -an

Active Connections

  Proto  Local Address          Foreign Address
  TCP    0.0.0.0:135            0.0.0.0:0
  TCP    0.0.0.0:242            0.0.0.0:0
  TCP    0.0.0.0:445            0.0.0.0:0
  TCP    0.0.0.0:990            0.0.0.0:0
  TCP    0.0.0.0:2584           0.0.0.0:0
  TCP    0.0.0.0:2585           0.0.0.0:0
  TCP    0.0.0.0:2967           0.0.0.0:0
  TCP    0.0.0.0:3389           0.0.0.0:0
  TCP    0.0.0.0:12174          0.0.0.0:0
  TCP    0.0.0.0:38292          0.0.0.0:0
  TCP    127.0.0.1:242          127.0.0.1:1042
  TCP    127.0.0.1:1042         127.0.0.1:242
  TCP    127.0.0.1:1044         0.0.0.0:0
  TCP    127.0.0.1:1046         0.0.0.0:0
  TCP    127.0.0.1:1078         0.0.0.0:0
  TCP    127.0.0.1:2584         127.0.0.1:2909
  TCP    127.0.0.1:2909         127.0.0.1:2584
  TCP    127.0.0.1:5679         0.0.0.0:0
  TCP    127.0.0.1:7438         0.0.0.0:0
  TCP    172.16.28.75:139       0.0.0.0:0
  TCP    172.16.28.75:1067      172.16.28.102:445
  TCP    172.16.28.75:1071      172.16.28.103:139
  TCP    172.16.28.75:1116      172.16.28.102:1026
  TCP    172.16.28.75:1135      172.16.28.101:389
  TCP    172.16.28.75:1138      172.16.28.104:445
  TCP    172.16.28.75:1148      172.16.28.101:389
  TCP    172.16.28.75:1610      172.16.28.101:139
  TCP    172.16.28.75:2589      172.16.28.101:389
  TCP    172.16.28.75:2793      172.16.28.106:445
  TCP    172.16.28.75:3801      172.16.28.104:1148
  TCP    172.16.28.75:3890      172.16.28.104:135
  TCP    172.16.28.75:3891      172.16.28.104:1056
  TCP    172.16.28.75:3892      172.16.28.104:1155
  TCP    172.16.28.75:3893      172.16.28.102:135
  TCP    172.16.28.75:3896      172.16.28.101:135
  TCP    172.16.28.75:3899      172.16.28.104:135
  TCP    172.16.28.75:3900      172.16.28.104:1056
  TCP    172.16.28.75:3901      172.16.28.104:1155
```

He runs the netstat command on the machine to see its current connections. In the following screenshot, what do the 0.0.0.0 IP addresses signify?

A. Those connections are established
B. Those connections are in listening mode
C. Those connections are in closed/waiting mode
D. Those connections are in timed out/waiting mode

**Answer:** B


**NEW QUESTION 640**
- (Exam Topic 2)
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. The change in the routing fabric to bypass the affected router
B. More RESET packets to the affected router to get it to power back up
C. RESTART packets to the affected router to get it to power back up
D. STOP packets to all other routers warning of where the attack originated

**Answer:** A


**NEW QUESTION 641**
- (Exam Topic 2)
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 is a journaling file system
C. NTFS has lower cluster size space
D. FAT is an older and inefficient file system

**Answer:** C


**NEW QUESTION 644**
- (Exam Topic 2)
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. Network
B. Transport
C. Data Link
D. Session

**Answer:** A


**NEW QUESTION 647**
- (Exam Topic 2)
Davidson Trucking is a small transportation company that has three local offices in Detroit Michigan. Ten female employees that work for the company have gone to an attorney reporting that male employees repeatedly harassed them and that management did nothing to stop the problem. Davidson has employee policies that outline all company guidelines, including awareness on harassment and how it will not be tolerated. When the case is brought to court, whom should the prosecuting attorney call upon for not upholding company policy?

A. IT personnel
B. Employees themselves
C. Supervisors
D. Administrative assistant in charge of writing policies

**Answer:** C


**NEW QUESTION 649**
- (Exam Topic 2)
Which of the following tool can the investigator use to analyze the network to detect Trojan activities?

A. Regshot
B. TRIPWIRE
C. RAM Computer
D. Capsa

**Answer:** D


**NEW QUESTION 650**
- (Exam Topic 2)
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. He should search in C:\Windows\System32\RECYCLED folder
B. The Recycle Bin does not exist on the hard drive
C. The files are hidden and he must use switch to view them
D. Only FAT system contains RECYCLED folder and not NTFS

**Answer:** C


**NEW QUESTION 654**
- (Exam Topic 2)
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. Cain & Abel
D. Xplico

**Answer:** D


**NEW QUESTION 655**
- (Exam Topic 2)
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. IOCE
B. SWGDE & SWGIT
C. Frye
D. Daubert

**Answer:** D


**NEW QUESTION 656**
- (Exam Topic 2)
Sniffers that place NICs in promiscuous mode work at what layer of the OSI model?

A. Network
B. Transport
C. Physical
D. Data Link

**Answer:** C


**NEW QUESTION 659**
- (Exam Topic 2)
Smith, a network administrator with a large MNC, was the first to arrive at a suspected crime scene involving criminal use of compromised computers. What should be his first response while maintaining the integrity of evidence?

A. Record the system state by taking photographs of physical system and the display
B. Perform data acquisition without disturbing the state of the systems
C. Open the systems, remove the hard disk and secure it
D. Switch off the systems and carry them to the laboratory

**Answer:** A


**NEW QUESTION 663**
- (Exam Topic 2)
When investigating a wireless attack, what information can be obtained from the DHCP logs?

A. The operating system of the attacker and victim computers
B. IP traffic between the attacker and the victim
C. MAC address of the attacker
D. If any computers on the network are running in promiscuous mode

**Answer:** C


**NEW QUESTION 666**
- (Exam Topic 2)
Why would you need to find out the gateway of a device when investigating a wireless attack?

A. The gateway will be the IP of the proxy server used by the attacker to launch the attack
B. The gateway will be the IP of the attacker computer
C. The gateway will be the IP used to manage the RADIUS server
D. The gateway will be the IP used to manage the access point

**Answer:** D


**NEW QUESTION 669**
- (Exam Topic 2)
Your company's network just finished going through a SAS 70 audit. This audit reported that overall, your network is secure, but there are some areas that needs improvement. The major area was SNMP security. The audit company recommended turning off SNMP, but that is not an option since you have so many remote nodes to keep track of. What step could you take to help secure SNMP on your network?

A. Block all internal MAC address from using SNMP
B. Block access to UDP port 171
C. Block access to TCP port 171
D. Change the default community string names

**Answer:** D


**NEW QUESTION 672**
- (Exam Topic 2)
Which US law does the interstate or international transportation and receiving of child pornography fall under?

A. §18. U.S.
B. 1466A
C. §18. U.S.C 252
D. §18. U.S.C 146A
E. §18. U.S.C 2252

**Answer:** D


**NEW QUESTION 676**
- (Exam Topic 2)
You have been given the task to investigate web attacks on a Windows-based server. Which of the following commands will you use to look at the sessions the machine has opened with other systems?

A. Net sessions
B. Net config
C. Net share
D. Net use

**Answer:** D

**NEW QUESTION 680**
- (Exam Topic 2)
Ivanovich, a forensics investigator, is trying to extract complete information about running processes from a system. Where should he look apart from the RAM and virtual memory?

A. Swap space
B. Application data
C. Files and documents
D. Slack space

**Answer:** A


**NEW QUESTION 683**
- (Exam Topic 2)
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. Expert in criminal investigation
B. Subject matter specialist
C. Witness present at the crime scene
D. Expert law graduate appointed by attorney

**Answer:** B


**NEW QUESTION 687**
- (Exam Topic 2)
What does the 63.78.199.4(161) denotes in a Cisco router log?
Mar 14 22:57:53.425 EST: %SEC-6-IPACCESSLOGP: list internet-inbound denied udp 66.56.16.77(1029) -> 63.78.199.4(161), 1 packet

A. Destination IP address
B. Source IP address
C. Login IP address
D. None of the above

**Answer:** A


**NEW QUESTION 692**
- (Exam Topic 2)
Sectors are pie-shaped regions on a hard disk that store data. Which of the following parts of a hard disk do not contribute in determining the addresses of data?

A. Sectors
B. Interface
C. Cylinder
D. Heads

**Answer:** B


**NEW QUESTION 697**
- (Exam Topic 2)
Who is responsible for the following tasks?

A. Non-forensics staff
B. Lawyers
C. System administrators
D. Local managers or other non-forensic staff

**Answer:** A


**NEW QUESTION 698**
- (Exam Topic 2)
What layer of the OSI model do TCP and UDP utilize?

A. Data Link
B. Network
C. Transport
D. Session

**Answer:** C


**NEW QUESTION 702**
- (Exam Topic 2)
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\Exchsrvr\servername.log
B. D:\Exchsrvr\Message Tracking\servername.log
C. C:\Exchsrvr\Message Tracking\servername.log

D. C:\Program Files\Microsoft Exchange\srvr\servername.log

**Answer:** A


**NEW QUESTION 704**
- (Exam Topic 2)
Which of the following are small pieces of data sent from a website and stored on the user's computer by the user's web browser to track, validate, and maintain specific user information?

A. Temporary Files
B. Open files
C. Cookies
D. Web Browser Cache

**Answer:** C


**NEW QUESTION 706**
- (Exam Topic 2)
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. Citizen Informant Search Warrant
B. Electronic Storage Device Search Warrant
C. John Doe Search Warrant
D. Service Provider Search Warrant

**Answer:** B


**NEW QUESTION 709**
- (Exam Topic 2)
John is working on his company policies and guidelines. The section he is currently working on covers company documents; how they should be handled, stored, and eventually destroyed. John is concerned about the process whereby outdated documents are destroyed. What type of shredder should John write in the guidelines to be used when destroying documents?

A. Strip-cut shredder
B. Cross-cut shredder
C. Cross-hatch shredder
D. Cris-cross shredder

**Answer:** B


**NEW QUESTION 710**
- (Exam Topic 2)
Which of the following technique creates a replica of an evidence media?

A. Data Extraction
B. Backup
C. Bit Stream Imaging
D. Data Deduplication

**Answer:** C


**NEW QUESTION 714**
- (Exam Topic 2)
When should an MD5 hash check be performed when processing evidence?

A. After the evidence examination has been completed
B. On an hourly basis during the evidence examination
C. Before and after evidence examination
D. Before the evidence examination has been completed

**Answer:** C


**NEW QUESTION 716**
- (Exam Topic 2)
When is it appropriate to use computer forensics?

A. If copyright and intellectual property theft/misuse has occurred
B. If employees do not care for their boss management techniques
C. If sales drop off for no apparent reason for an extended period of time
D. If a financial institution is burglarized by robbers

**Answer:** A


**NEW QUESTION 717**

- (Exam Topic 2)
Which among the following files provides email header information in the Microsoft Exchange server?

A. gwcheck.db
B. PRIV.EDB
C. PUB.EDB
D. PRIV.STM

**Answer:** B


**NEW QUESTION 721**
- (Exam Topic 2)
In Steganalysis, which of the following describes a Known-stego attack?

A. The hidden message and the corresponding stego-image are known
B. During the communication process, active attackers can change cover
C. Original and stego-object are available and the steganography algorithm is known
D. Only the steganography medium is available for analysis

**Answer:** C


**NEW QUESTION 725**
- (Exam Topic 2)
What is the slave device connected to the secondary IDE controller on a Linux OS referred to?

A. hda
B. hdd
C. hdb
D. hdc

**Answer:** B


**NEW QUESTION 729**
- (Exam Topic 2)
Where does Encase search to recover NTFS files and folders?

A. MBR
B. MFT
C. Slack space
D. HAL

**Answer:** B


**NEW QUESTION 734**
- (Exam Topic 2)
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 Document
C. MS-office Word OneNote
D. MS-office Word PowerPoint

**Answer:** A


**NEW QUESTION 737**
- (Exam Topic 2)
Which of the following stages in a Linux boot process involve initialization of the system's hardware?

A. BIOS Stage
B. Bootloader Stage
C. BootROM Stage
D. Kernel Stage

**Answer:** A


**NEW QUESTION 742**
- (Exam Topic 2)
Which of the following is a database in which information about every file and directory on an NT File System (NTFS) volume is stored?

A. Volume Boot Record
B. Master Boot Record
C. GUID Partition Table
D. Master File Table

**Answer:** D

**NEW QUESTION 747**
- (Exam Topic 2)
What file is processed at the end of a Windows XP boot to initialize the logon dialog box?

A. NTOSKRNL.EXE
B. NTLDR
C. LSASS.EXE
D. NTDETECT.COM

**Answer:** A


**NEW QUESTION 750**
- (Exam Topic 2)
Which code does the FAT file system use to mark the file as deleted?

A. ESH
B. 5EH
C. H5E
D. E5H

**Answer:** D


**NEW QUESTION 752**
- (Exam Topic 2)
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. Unplug all connected devices
C. Power off all devices if currently on
D. Photograph and document the peripheral devices

**Answer:** D


**NEW QUESTION 755**
- (Exam Topic 2)
When marking evidence that has been collected with the aa/ddmmyy/nnnn/zz format, what does the nnn denote?

A. The year the evidence was taken
B. The sequence number for the parts of the same exhibit
C. The initials of the forensics analyst
D. The sequential number of the exhibits seized

**Answer:** D


**NEW QUESTION 757**
- (Exam Topic 2)
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. Rule-Based Approach
B. Automated Field Correlation
C. Field-Based Approach
D. Graph-Based Approach

**Answer:** B


**NEW QUESTION 761**
- (Exam Topic 2)
An executive has leaked the company trade secrets through an external drive. What process should the investigation team take if they could retrieve his system?

A. Postmortem Analysis
B. Real-Time Analysis
C. Packet Analysis
D. Malware Analysis

**Answer:** A


**NEW QUESTION 763**
- (Exam Topic 2)
Which MySQL log file contains information on server start and stop?

A. Slow query log file
B. General query log file
C. Binary log

D. Error log file

**Answer:** D


**NEW QUESTION 764**
- (Exam Topic 2)
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. One working day
B. Two working days
C. Immediately
D. Four hours

**Answer:** A


**NEW QUESTION 765**
- (Exam Topic 2)
What must be obtained before an investigation is carried out at a location?

A. Search warrant
B. Subpoena
C. Habeas corpus
D. Modus operandi

**Answer:** A


**NEW QUESTION 768**
- (Exam Topic 2)
What is the location of the binary files required for the functioning of the OS in a Linux system?

A. /run
B. /bin
C. /root
D. /sbin

**Answer:** B


**NEW QUESTION 772**
- (Exam Topic 2)
When marking evidence that has been collected with the "aaa/ddmmyy/nnnn/zz" format, what does the "nnnn" denote?

A. The initials of the forensics analyst
B. The sequence number for the parts of the same exhibit
C. The year he evidence was taken
D. The sequential number of the exhibits seized by the analyst

**Answer:** D


**NEW QUESTION 776**
- (Exam Topic 2)
An investigator is searching through the firewall logs of a company and notices ICMP packets that are larger than 65,536 bytes. What type of activity is the investigator seeing?

A. Smurf
B. Ping of death
C. Fraggle
D. Nmap scan

**Answer:** B


**NEW QUESTION 781**
- (Exam Topic 2)
In Windows Security Event Log, what does an event id of 530 imply?

A. Logon Failure – Unknown user name or bad password
B. Logon Failure – User not allowed to logon at this computer
C. Logon Failure – Account logon time restriction violation
D. Logon Failure – Account currently disabled

**Answer:** C


**NEW QUESTION 782**
- (Exam Topic 2)
Which password cracking technique uses details such as length of password, character sets used to construct the password, etc.?

A. Dictionary attack
B. Brute force attack
C. Rule-based attack
D. Man in the middle attack

**Answer:** A

**NEW QUESTION 785**
- (Exam Topic 2)
Files stored in the Recycle Bin in its physical location are renamed as Dxy.ext, where "x" represents the _____.

A. Drive name
B. Original file name's extension
C. Sequential number
D. Original file name

**Answer:** A

**NEW QUESTION 789**
- (Exam Topic 2)
Heather, a computer forensics investigator, is assisting a group of investigators working on a large computer fraud case involving over 20 people. These 20 people, working in different offices, allegedly siphoned off money from many different client accounts. Heather responsibility is to find out how the accused people communicated between each other. She has searched their email and their computers and has not found any useful evidence. Heather then finds some possibly useful evidence under the desk of one of the accused.
In an envelope she finds a piece of plastic with numerous holes cut out of it. Heather then finds the same exact piece of plastic with holes at many of the other accused peoples desks. Heather believes that the 20 people involved in the case were using a cipher to send secret messages in between each other. What type of cipher was used by the accused in this case?

A. Grill cipher
B. Null cipher
C. Text semagram
D. Visual semagram

**Answer:** A

**NEW QUESTION 794**
- (Exam Topic 2)
Casey has acquired data from a hard disk in an open source acquisition format that allows her to generate compressed or uncompressed image files. What format did she use?

A. Portable Document Format
B. Advanced Forensics Format (AFF)
C. Proprietary Format
D. Raw Format

**Answer:** B

**NEW QUESTION 797**
- (Exam Topic 2)
A picture file is recovered from a computer under investigation. During the investigation process, the file is enlarged 500% to get a better view of its contents. The picture quality is not degraded at all from this process. What kind of picture is this file. What kind of picture is this file?

A. Raster image
B. Vector image
C. Metafile image
D. Catalog image

**Answer:** B

**NEW QUESTION 802**
- (Exam Topic 2)
Before performing a logical or physical search of a drive in Encase, what must be added to the program?

A. File signatures
B. Keywords
C. Hash sets
D. Bookmarks

**Answer:** B

**NEW QUESTION 805**
- (Exam Topic 2)
A master boot record (MBR) is the first sector ("sector zero") of a data storage device. What is the size of MBR?

A. Depends on the capacity of the storage device
B. 1048 Bytes

C. 4092 Bytes
D. 512 Bytes

**Answer:** D

**NEW QUESTION 806**
- (Exam Topic 2)
How often must a company keep log files for them to be admissible in a court of law?

A. All log files are admissible in court no matter their frequency
B. Weekly
C. Monthly
D. Continuously

**Answer:** D

**NEW QUESTION 811**
- (Exam Topic 2)
Linux operating system has two types of typical bootloaders namely LILO (Linux Loader) and GRUB (Grand Unified Bootloader). In which stage of the booting process do the bootloaders become active?

A. Bootloader Stage
B. Kernel Stage
C. BootROM Stage
D. BIOS Stage

**Answer:** A

**NEW QUESTION 814**
......

# Thank You for Trying Our Product

## We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

## 312-49v10 Practice Exam Features:

* 312-49v10 Questions and Answers Updated Frequently

* 312-49v10 Practice Questions Verified by Expert Senior Certified Staff

* 312-49v10 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* 312-49v10 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

## 100% Actual & Verified — Instant Download, Please Click
[Order The 312-49v10 Practice Test Here](https://www.surepassexam.com/312-49v10-exam-dumps.html)