

EC-Council

Exam Questions 312-49v10

Computer Hacking Forensic Investigator (CHFI-v10)



NEW QUESTION 1

- (Exam Topic 1)

You have been asked to investigate the possibility of computer fraud in the finance department of a company. It is suspected that a staff member has been committing finance fraud by printing cheques that have not been authorized. You have exhaustively searched all data files on a bitmap image of the target computer, but have found no evidence. You suspect the files may not have been saved. What should you examine next in this case?

- A. The registry
- B. The swap file
- C. The recycle bin
- D. The metadata

Answer: B

NEW QUESTION 2

- (Exam Topic 1)

Windows identifies which application to open a file with by examining which of the following?

- A. The File extension
- B. The file attributes
- C. The file Signature at the end of the file
- D. The file signature at the beginning of the file

Answer: A

NEW QUESTION 3

- (Exam Topic 1)

A suspect is accused of violating the acceptable use of computing resources, as he has visited adult websites and downloaded images. The investigator wants to demonstrate that the suspect did indeed visit these sites. However, the suspect has cleared the search history and emptied the cookie cache. Moreover, he has removed any images he might have downloaded. What can the investigator do to prove the violation?

- A. Image the disk and try to recover deleted files
- B. Seek the help of co-workers who are eye-witnesses
- C. Check the Windows registry for connection data (you may or may not recover)
- D. Approach the websites for evidence

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)

What type of attack occurs when an attacker can force a router to stop forwarding packets by flooding the router with many open connections simultaneously so that all the hosts behind the router are effectively disabled?

- A. digital attack
- B. denial of service
- C. physical attack
- D. ARP redirect

Answer: B

NEW QUESTION 6

- (Exam Topic 1)

On Linux/Unix based Web servers, what privilege should the daemon service be run under?

- A. Guest
- B. Root
- C. You cannot determine what privilege runs the daemon service
- D. Something other than root

Answer: D

NEW QUESTION 7

- (Exam Topic 1)

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 that 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. Bit-stream Copy
- B. Robust Copy
- C. Full backup Copy
- D. Incremental Backup Copy

Answer: C

NEW QUESTION 8

- (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 9

- (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 10

- (Exam Topic 1)

When reviewing web logs, you see an entry for resource not found in the HTTP status code filed. What is the actual error code that you would see in the log for resource not found?

- A. 202
- B. 404
- C. 505
- D. 909

Answer: B

NEW QUESTION 10

- (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 15

- (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 18

- (Exam Topic 2)

How many times can data be written to a DVD+R disk?

- A. Twice
- B. Once

- C. Zero
- D. Infinite

Answer: B

NEW QUESTION 20

- (Exam Topic 2)

When making the preliminary investigations in a sexual harassment case, how many investigators are you recommended having?

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

Answer: B

NEW QUESTION 21

- (Exam Topic 2)

Which of the following Registry components include offsets to other cells as well as the LastWrite time for the key?

- A. Value list cell
- B. Value cell
- C. Key cell
- D. Security descriptor cell

Answer: C

NEW QUESTION 26

- (Exam Topic 2)

What will the following command accomplish? `dd if=/dev/xxx of=mbr.backup bs=512 count=1`

- A. Back up the master boot record
- B. Restore the master boot record
- C. Mount the master boot record on the first partition of the hard drive
- D. Restore the first 512 bytes of the first partition of the hard drive

Answer: A

NEW QUESTION 27

- (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 31

- (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 36

- (Exam Topic 2)

Which of the following is a record of the characteristics of a file system, including its size, the block size, the empty and the filled blocks and their respective counts, the size and location of the inode tables, the disk block map and usage information, and the size of the block groups?

- A. Inode bitmap block
- B. Superblock
- C. Block bitmap block
- D. Data block

Answer: B

NEW QUESTION 40

- (Exam Topic 1)

Software firewalls work at which layer of the OSI model?

- A. Application
- B. Network
- C. Transport
- D. Data Link

Answer: D

NEW QUESTION 43

- (Exam Topic 1)

What term is used to describe a cryptographic technique for embedding information into something else for the sole purpose of hiding that information from the casual observer?

- A. rootkit
- B. key escrow
- C. steganography
- D. Offset

Answer: C

NEW QUESTION 46

- (Exam Topic 1)

You are working as Computer Forensics investigator and are called by the owner of an accounting firm to investigate possible computer abuse by one of the firm's employees. You meet with the owner of the firm and discover that the company has never published a policy stating that they reserve the right to inspect their computing assets at will. What do you do?

- A. Inform the owner that conducting an investigation without a policy is not a problem because the company is privately owned
- B. Inform the owner that conducting an investigation without a policy is a violation of the 4th amendment
- C. Inform the owner that conducting an investigation without a policy is a violation of the employee's expectation of privacy
- D. Inform the owner that conducting an investigation without a policy is not a problem because a policy is only necessary for government agencies

Answer: C

NEW QUESTION 47

- (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 49

- (Exam Topic 1)

Under which Federal Statutes does FBI investigate for computer crimes involving e-mail scams and mail fraud?

- A. 18 U.S.
- B. 1029 Possession of Access Devices
- C. 18 U.S.
- D. 1030 Fraud and related activity in connection with computers
- E. 18 U.S.
- F. 1343 Fraud by wire, radio or television
- G. 18 U.S.
- H. 1361 Injury to Government Property
- I. 18 U.S.
- J. 1362 Government communication systems
- K. 18 U.S.
- L. 1831 Economic Espionage Act
- M. 18 U.S.
- N. 1832 Trade Secrets Act

Answer: B

NEW QUESTION 53

- (Exam Topic 1)

Simon is a former employee of Trinitron XML Inc. He feels he was wrongly terminated and wants to hack into his former company's network. Since Simon remembers some of the server names, he attempts to run the axfr and ixfr commands using DIG. What is Simon trying to accomplish here?

- A. Send DOS commands to crash the DNS servers
- B. Perform DNS poisoning
- C. Perform a zone transfer
- D. Enumerate all the users in the domain

Answer: C

NEW QUESTION 57

- (Exam Topic 1)

In conducting a computer abuse investigation you become aware that the suspect of the investigation is using ABC Company as his Internet Service Provider (ISP). You contact ISP and request that they provide you assistance with your investigation. What assistance can the ISP provide?

- A. The ISP can investigate anyone using their service and can provide you with assistance
- B. The ISP can investigate computer abuse committed by their employees, but must preserve the privacy of their customers and therefore cannot assist you without a warrant
- C. The ISP can't conduct any type of investigations on anyone and therefore can't assist you
- D. ISP's never maintain log files so they would be of no use to your investigation

Answer: B

NEW QUESTION 58

- (Exam Topic 1)

In Microsoft file structures, sectors are grouped together to form:

- A. Clusters
- B. Drives
- C. Bitstreams
- D. Partitions

Answer: A

NEW QUESTION 62

- (Exam Topic 1)

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

- A. deltree command
- B. CMOS
- C. Boot.sys
- D. Scandisk utility

Answer: C

NEW QUESTION 65

- (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 66

- (Exam Topic 1)

Melanie was newly assigned to an investigation and asked to make a copy of all the evidence from the compromised system. Melanie did a DOS copy of all the files on the system. What would be the primary reason for you to recommend a disk imaging tool?

- A. A disk imaging tool would check for CRC32s for internal self-checking and validation and have MD5 checksum
- B. Evidence file format will contain case data entered by the examiner and encrypted at the beginning of the evidence file
- C. A simple DOS copy will not include deleted files, file slack and other information
- D. There is no case for an imaging tool as it will use a closed, proprietary format that if compared to the original will not match up sector for sector

Answer: C

NEW QUESTION 68

- (Exam Topic 1)

What method of computer forensics will allow you to trace all ever-established user accounts on a Windows 2000 sever the course of its lifetime?

- A. forensic duplication of hard drive
- B. analysis of volatile data
- C. comparison of MD5 checksums
- D. review of SIDs in the Registry

Answer: C

NEW QUESTION 73

- (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 76

- (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 81

- (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 86

- (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 89

- (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 93

- (Exam Topic 1)

What are the security risks of running a "repair" installation for Windows XP?

- A. Pressing Shift+F10 gives the user administrative rights
- B. Pressing Shift+F1 gives the user administrative rights
- C. Pressing Ctrl+F10 gives the user administrative rights
- D. There are no security risks when running the "repair" installation for Windows XP

Answer: A

NEW QUESTION 95

- (Exam Topic 1)

Julia is a senior security analyst for Berber Consulting group. She is currently working on a contract for a small accounting firm in Florida. They have given her permission to perform social engineering attacks on the company to see if their in-house training did any good. Julia calls the main number for the accounting firm and talks to the receptionist. Julia says that she is an IT technician from the company's main office in Iowa. She states that she needs the receptionist's network username and password to troubleshoot a problem they are having. Julia says that Bill Hammond, the CEO of the company, requested this information. After hearing the name of the CEO, the receptionist gave Julia all the information she asked for. What principal of social engineering did Julia use?

- A. Social Validation
- B. Scarcity
- C. Friendship/Liking
- D. Reciprocation

Answer: D

NEW QUESTION 97

- (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 101

- (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 106

- (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 111

- (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 115

- (Exam Topic 1)

You are a computer forensics investigator working with local police department and you are called to assist in an investigation of threatening emails. The complainant has printer out 27 email messages from the suspect and gives the printouts to you. You inform her that you will need to examine her computer because you need access to the in order to track the emails back to the suspect.

- A. Routing Table
- B. Firewall log
- C. Configuration files
- D. Email Header

Answer: D

NEW QUESTION 119

- (Exam Topic 1)

In what way do the procedures for dealing with evidence in a criminal case differ from the procedures for dealing with evidence in a civil case?

- A. evidence must be handled in the same way regardless of the type of case
- B. evidence procedures are not important unless you work for a law enforcement agency
- C. evidence in a criminal case must be secured more tightly than in a civil case
- D. evidence in a civil case must be secured more tightly than in a criminal case

Answer: C

NEW QUESTION 124

- (Exam Topic 1)

Harold is a security analyst who has just run the `rdisk /s` command to grab the backup SAM files on a computer. Where should Harold navigate on the computer to find the file?

- A. %systemroot%\system32\LSA
- B. %systemroot%\system32\drivers\etc
- C. %systemroot%\repair
- D. %systemroot%\LSA

Answer: C

NEW QUESTION 129

- (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 132

- (Exam Topic 1)

Larry is an IT consultant who works for corporations and government agencies. Larry plans on shutting down the city's network using BGP devices and zombies? What type of Penetration Testing is Larry planning to carry out?

- A. Router Penetration Testing
- B. DoS Penetration Testing
- C. Firewall Penetration Testing
- D. Internal Penetration Testing

Answer: B

NEW QUESTION 137

- (Exam Topic 1)

You are contracted to work as a computer forensics investigator for a regional bank that has four 30 TB storage area networks that store customer data. What method would be most efficient for you to acquire digital evidence from this network?

- A. create a compressed copy of the file with DoubleSpace
- B. create a sparse data copy of a folder or file
- C. make a bit-stream disk-to-image file
- D. make a bit-stream disk-to-disk file

Answer: C

NEW QUESTION 139

- (Exam Topic 1)

How many bits is Source Port Number in TCP Header packet?

- A. 16
- B. 32
- C. 48
- D. 64

Answer: A

NEW QUESTION 142

- (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 143

- (Exam Topic 1)

A(n) is one that's performed by a computer program rather than the attacker manually performing the steps in the attack sequence.

- A. blackout attack
- B. automated attack
- C. distributed attack
- D. central processing attack

Answer: B

NEW QUESTION 144

- (Exam Topic 1)

You are a security analyst performing a penetration tests for a company in the Midwest. After some initial reconnaissance, you discover the IP addresses of some Cisco routers used by the company. You type in the following URL that includes the IP address of one of the routers:

`http://172.168.4.131/level/99/exec/show/config`

After typing in this URL, you are presented with the entire configuration file for that router. What have you discovered?

- A. HTTP Configuration Arbitrary Administrative Access Vulnerability
- B. HTML Configuration Arbitrary Administrative Access Vulnerability
- C. Cisco IOS Arbitrary Administrative Access Online Vulnerability
- D. URL Obfuscation Arbitrary Administrative Access Vulnerability

Answer: A

NEW QUESTION 148

- (Exam Topic 1)

In General, Involves the investigation of data that can be retrieved from the hard disk or other disks of a computer by applying scientific methods to retrieve the data.

- A. Network Forensics
- B. Data Recovery
- C. Disaster Recovery
- D. Computer Forensics

Answer: D

NEW QUESTION 152

- (Exam Topic 1)

What is the target host IP in the following command?

- A. 172.16.28.95
- B. 10.10.150.1
- C. Firewall does not scan target hosts
- D. This command is using FIN packets, which cannot scan target hosts

Answer: A

NEW QUESTION 156

- (Exam Topic 1)

When using Windows acquisitions tools to acquire digital evidence, it is important to use a well-tested hardware write-blocking device to:

- A. Automate Collection from image files
- B. Avoiding copying data from the boot partition
- C. Acquire data from host-protected area on a disk
- D. Prevent Contamination to the evidence drive

Answer: D

NEW QUESTION 157

- (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 160

- (Exam Topic 1)

What is the name of the Standard Linux Command that is also available as windows application that can be used to create bit-stream images?

- A. mcopy
- B. image
- C. MD5
- D. dd

Answer: D

NEW QUESTION 164

- (Exam Topic 1)

Diskcopy is:

- A. a utility by AccessData
- B. a standard MS-DOS command
- C. Digital Intelligence utility
- D. dd copying tool

Answer: B

Explanation:

diskcopy is a STANDARD DOS utility. C:\WINDOWS>diskcopy /? Copies the contents of one floppy disk to another.

NEW QUESTION 169

- (Exam Topic 1)

The refers to handing over the results of private investigations to the authorities because of indications of criminal activity.

- A. Locard Exchange Principle
- B. Clark Standard
- C. Kelly Policy
- D. Silver-Platter Doctrine

Answer: D

NEW QUESTION 174

- (Exam Topic 1)

Which of the following refers to the data that might still exist in a cluster even though the original file has been overwritten by another file?

- A. Sector
- B. Metadata
- C. MFT
- D. Slack Space

Answer: D

NEW QUESTION 178

- (Exam Topic 1)

This is original file structure database that Microsoft originally designed for floppy disks. It is written to the outermost track of a disk and contains information about each file stored on the drive.

- A. Master Boot Record (MBR)
- B. Master File Table (MFT)
- C. File Allocation Table (FAT)
- D. Disk Operating System (DOS)

Answer: C

NEW QUESTION 183

- (Exam Topic 1)

When obtaining a warrant, it is important to:

- A. particularly describe the place to be searched and particularly describe the items to be seized
- B. generally describe the place to be searched and particularly describe the items to be seized
- C. generally describe the place to be searched and generally describe the items to be seized
- D. particularly describe the place to be searched and generally describe the items to be seized

Answer: A

NEW QUESTION 184

- (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 187

- (Exam Topic 1)

When monitoring for both intrusion and security events between multiple computers, it is essential that the computers' clocks are synchronized. Synchronized time allows an administrator to reconstruct what took place during an attack against multiple computers. Without synchronized time, it is very difficult to determine exactly when specific events took place, and how events interlace. What is the name of the service used to synchronize time among multiple computers?

- A. Universal Time Set
- B. Network Time Protocol
- C. SyncTime Service
- D. Time-Sync Protocol

Answer: B

NEW QUESTION 189

- (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 192

- (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 193

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

Answer: D

NEW QUESTION 198

- (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 200

- (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 205

- (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 210

- (Exam Topic 4)

The working of the Tor browser is based on which of the following concepts?

- A. Both static and default routing
- B. Default routing
- C. Static routing
- D. Onion routing

Answer: D

NEW QUESTION 215

- (Exam Topic 4)

In Java, when multiple applications are launched, multiple Dalvik Virtual Machine instances occur that consume memory and time. To avoid that, Android implements a process that enables low memory consumption and quick start-up time. What is the process called?

- A. init
- B. Media server
- C. Zygote
- D. Daemon

Answer: C

NEW QUESTION 219

- (Exam Topic 4)

Which of the following is considered as the starting point of a database and stores user data and database objects in an MS SQL server?

- A. Ibddata1
- B. Application data files (ADF)
- C. Transaction log data files (LDF)
- D. Primary data files (MDF)

Answer: C

NEW QUESTION 222

- (Exam Topic 4)

The information security manager at a national legal firm has received several alerts from the intrusion detection system that a known attack signature was detected against the organization's file server. What should the information security manager do first?

- A. Report the incident to senior management
- B. Update the anti-virus definitions on the file server
- C. Disconnect the file server from the network
- D. Manually investigate to verify that an incident has occurred

Answer: C

NEW QUESTION 227

- (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 231

- (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 234

- (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 235

- (Exam Topic 4)

James, a forensics specialist, was tasked with investigating a Windows XP machine that was used for malicious online activities. During the investigation, he recovered certain deleted files from Recycle Bin to identify attack clues. Identify the location of Recycle Bin in Windows XP system.

- A. Drive:\\$Recycle.Bin\
- B. local/share/Trash
- C. Drive:\RECYCLER\
- D. Drive\ARECYCLED

Answer: C

NEW QUESTION 238

- (Exam Topic 4)

Frank, a cloud administrator in his company, needs to take backup of the OS disks of two Azure VMs that store business-critical data. Which type of Azure blob storage can he use for this purpose?

- A. Append blob
- B. Medium blob
- C. Block blob
- D. Page blob

Answer: D

NEW QUESTION 241

- (Exam Topic 4)

Sally accessed the computer system that holds trade secrets of the company where she is employed. She knows she accessed it without authorization and all access (authorized and unauthorized) to this computer is monitored. To cover her tracks, Sally deleted the log entries on this computer. What among the following best describes her action?

- A. Password sniffing
- B. Anti-forensics
- C. Brute-force attack
- D. Network intrusion

Answer: B

NEW QUESTION 244

- (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 245

- (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 246

- (Exam Topic 4)

Which of the following Windows event logs record events related to device drives and hardware changes?

- A. Forwarded events log
- B. System log
- C. Application log
- D. Security log

Answer: B

NEW QUESTION 250

- (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 255

- (Exam Topic 4)

A clothing company has recently deployed a website on its latest product line to increase its conversion rate and base of customers. Andrew, the network administrator recently appointed by the company, has been assigned with the task of protecting the website from intrusion and vulnerabilities. Which of the following tools should Andrew consider deploying in this scenario?

- A. ModSecurity
- B. CryptaPix
- C. Recuva
- D. Kon-Boot

Answer: A

NEW QUESTION 258

- (Exam Topic 4)

Steve received a mail that seemed to have come from her bank. The mail has instructions for Steve to click on a link and provide information to avoid the suspension of her account. The link in the mail redirected her to a form asking for details such as name, phone number, date of birth, credit card number or PIN, CW code, SNNs, and email address. On a closer look, Steve realized that the URL of the form is not the same as that of her bank's. Identify the type of external attack performed by the attacker in the above scenario?

- A. Phishing
- B. Espionage
- C. Tailgating
- D. Brute-force

Answer: A

NEW QUESTION 263

- (Exam Topic 3)

Which of the following email headers specifies an address for mailer-generated errors, like "no such user" bounce messages, to go to (instead of the sender's address)?

- A. Mime-Version header
- B. Content-Type header
- C. Content-Transfer-Encoding header
- D. Errors-To header

Answer: D

NEW QUESTION 267

- (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 271

- (Exam Topic 4)

Data density of a disk drive is calculated by using

- A. Slack space, bit density, and slack density.
- B. Track space, bit area, and slack space.

- C. Track density, areal density, and slack density.
- D. Track density, areal density, and bit density.

Answer: D

NEW QUESTION 273

- (Exam Topic 3)

Which list contains the most recent actions performed by a Windows User?

- A. MRU
- B. Activity
- C. Recents
- D. Windows Error Log

Answer: A

NEW QUESTION 276

- (Exam Topic 3)

What technique is used by JPEGs for compression?

- A. TIFF-8
- B. ZIP
- C. DCT
- D. TCD

Answer: C

NEW QUESTION 279

- (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 280

- (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 Baselineing
- C. Start-up Programs Monitoring
- D. Host integrity Monitoring

Answer: D

NEW QUESTION 282

- (Exam Topic 3)

Self-Monitoring, Analysis, and Reporting Technology (SMART) is built into the hard drives to monitor and report system activity. Which of the following is included in the report generated by SMART?

- A. Power Off time
- B. Logs of high temperatures the drive has reached
- C. All the states (running and discontinued) associated with the OS
- D. List of running processes

Answer: B

NEW QUESTION 283

- (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 287

- (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?

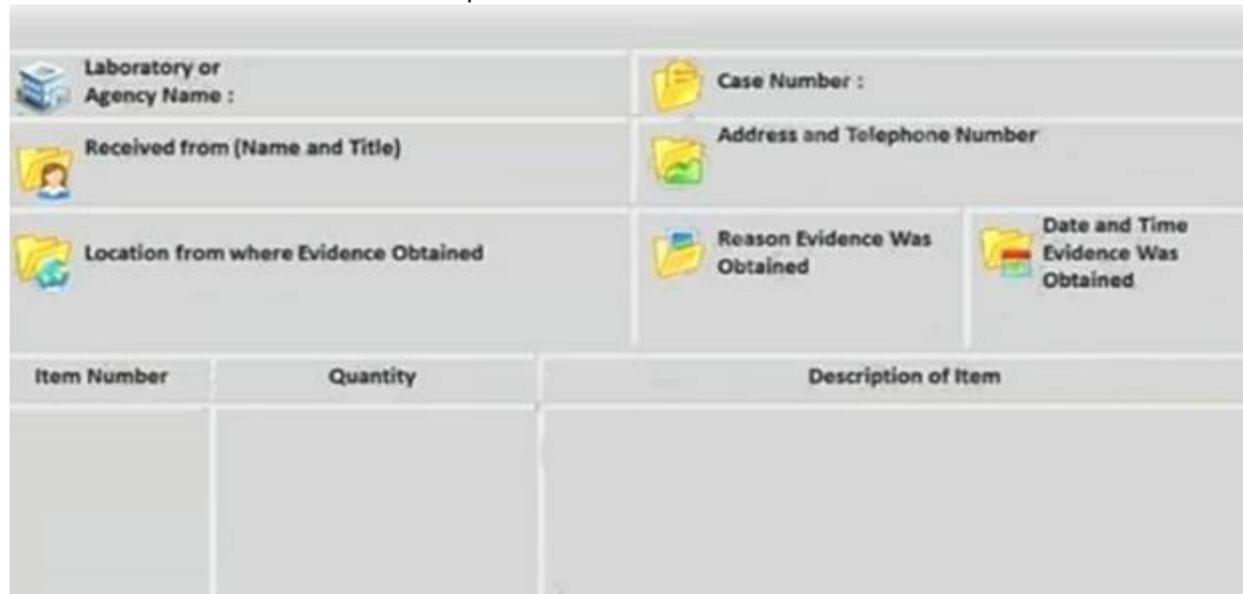
- A. SOX
- B. HIPAA
- C. GLBA
- D. FISMA

Answer: C

NEW QUESTION 292

- (Exam Topic 3)

What document does the screenshot represent?



Laboratory or Agency Name :		Case Number :
Received from (Name and Title)		Address and Telephone Number
Location from where Evidence Obtained	Reason Evidence Was Obtained	Date and Time Evidence Was Obtained
Item Number	Quantity	Description of Item

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

Answer: D

NEW QUESTION 295

- (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 298

- (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 302

- (Exam Topic 3)

As a Certified Ethical Hacker, you were contracted by a private firm to conduct an external security assessment through penetration testing . What document describes the specifics of the testing, the associated violations, and essentially protects both the organization's interest and your liabilities as a tester?

- A. Project Scope
- B. Rules of Engagement
- C. Non-Disclosure Agreement
- D. Service Level Agreement

Answer: B

NEW QUESTION 307

- (Exam Topic 3)

Which one of the following is not a first response procedure?

- A. Preserve volatile data
- B. Fill forms
- C. Crack passwords
- D. Take photos

Answer: C

NEW QUESTION 309

- (Exam Topic 3)

Which of the following files store the MySQL database data permanently, including the data that had been deleted, helping the forensic investigator in examining the case and finding the culprit?

- A. mysql-bin
- B. mysql-log
- C. iblog
- D. ibdata1

Answer: D

NEW QUESTION 312

- (Exam Topic 3)

A forensic examiner is examining a Windows system seized from a crime scene. During the examination of a suspect file, he discovered that the file is password protected. He tried guessing the password using the suspect's available information but without any success. Which of the following tool can help the investigator to solve this issue?

- A. Cain & Abel
- B. Xplico
- C. Recuva
- D. Colasoft's Capsa

Answer: A

NEW QUESTION 313

- (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 314

- (Exam Topic 3)

In Linux OS, different log files hold different information, which help the investigators to analyze various issues during a security incident. What information can the investigators obtain from the log file var/log/dmesg?

- A. Kernel ring buffer information
- B. All mail server message logs
- C. Global system messages
- D. Debugging log messages

Answer: A

NEW QUESTION 317

- (Exam Topic 3)

A section of your forensics lab houses several electrical and electronic equipment. Which type of fire extinguisher you must install in this area to contain any fire incident?

- A. Class B
- B. Class D
- C. Class C
- D. Class A

Answer: C

NEW QUESTION 319

- (Exam Topic 3)

Gill is a computer forensics investigator who has been called upon to examine a seized computer. This computer, according to the police, was used by a hacker who gained access to numerous banking institutions to steal customer information. After preliminary investigations, Gill finds in the computer's log files that the hacker was able to gain access to these banks through the use of Trojan horses. The hacker then used these Trojan horses to obtain remote access to the

companies' domain controllers. From this point, Gill found that the hacker pulled off the SAM files from the domain controllers to then attempt and crack network passwords. What is the most likely password cracking technique used by this hacker to break the user passwords from the SAM files?

- A. Syllable attack
- B. Hybrid attack
- C. Brute force attack
- D. Dictionary attack

Answer: D

NEW QUESTION 322

- (Exam Topic 3)

Which of the following statements is incorrect when preserving digital evidence?

- A. Verify if the monitor is in on, off, or in sleep mode
- B. Turn on the computer and extract Windows event viewer log files
- C. Remove the plug from the power router or modem
- D. Document the actions and changes that you observe in the monitor, computer, printer, or in other peripherals

Answer: B

NEW QUESTION 325

- (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 328

- (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 330

- (Exam Topic 3)

Consider that you are investigating a machine running an Windows OS released prior to Windows Vista. You are trying to gather information about the deleted files by examining the master database file named INFO2 located at C:\Recycler\<USER SID>. You read an entry named "Dd5.exe". What does Dd5.exe mean?

- A. D driv
- B. fifth file deleted, a .exe file
- C. D drive, fourth file restored, a .exe file
- D. D drive, fourth file deleted, a .exe file
- E. D drive, sixth file deleted, a .exe file

Answer: B

NEW QUESTION 333

- (Exam Topic 3)

Which of the following registry hive gives the configuration information about which application was used to open various files on the system?

- A. HKEY_CLASSES_ROOT
- B. HKEY_CURRENT_CONFIG
- C. HKEY_LOCAL_MACHINE
- D. HKEY_USERS

Answer: A

NEW QUESTION 338

- (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 341

- (Exam Topic 3)

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

- A. A virtual system with internet connection
- B. A normal system without internet connect
- C. A normal system with internet connection
- D. A virtual system with network simulation for internet connection

Answer: D

NEW QUESTION 342

- (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 343

- (Exam Topic 3)

What is the location of a Protective MBR in a GPT disk layout?

- A. Logical Block Address (LBA) 2
- B. Logical Block Address (LBA) 0
- C. Logical Block Address (LBA) 1
- D. Logical Block Address (LBA) 3

Answer: C

NEW QUESTION 345

- (Exam Topic 3)

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

- A. Cloud as a subject
- B. Cloud as a tool
- C. Cloud as an object
- D. Cloud as a service

Answer: A

NEW QUESTION 350

- (Exam Topic 3)

Investigators can use the Type Allocation Code (TAC) to find the model and origin of a mobile device. Where is TAC located in mobile devices?

- A. International Mobile Equipment Identifier (IMEI)
- B. Integrated circuit card identifier (ICCID)
- C. International mobile subscriber identity (IMSI)
- D. Equipment Identity Register (EIR)

Answer: A

NEW QUESTION 355

- (Exam Topic 3)

Which among the following search warrants allows the first responder to search and seize the victim's computer components such as hardware, software, storage devices, and documentation?

- A. John Doe Search Warrant
- B. Citizen Informant Search Warrant
- C. Electronic Storage Device Search Warrant
- D. Service Provider Search Warrant

Answer: C

NEW QUESTION 359

- (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 364

- (Exam Topic 3)

Amelia has got an email from a well-reputed company stating in the subject line that she has won a prize money, whereas the email body says that she has to pay a certain amount for being eligible for the contest. Which of the following acts does the email breach?

- A. CAN-SPAM Act
- B. HIPAA
- C. GLBA
- D. SOX

Answer: A

NEW QUESTION 367

- (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 371

- (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 373

- (Exam Topic 3)

CAN-SPAM act requires that you:

- A. Don't use deceptive subject lines
- B. Don't tell the recipients where you are located
- C. Don't identify the message as an ad
- D. Don't use true header information

Answer: A

NEW QUESTION 375

- (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 378

- (Exam Topic 3)

Which tool allows dumping the contents of process memory without stopping the process?

- A. psdump.exe
- B. pmdump.exe
- C. processdump.exe
- D. pdump.exe

Answer: B

NEW QUESTION 379

- (Exam Topic 3)

Pick the statement which does not belong to the Rule 804. Hearsay Exceptions; Declarant Unavailable.

- A. Statement of personal or family history
- B. Prior statement by witness
- C. Statement against interest
- D. Statement under belief of impending death

Answer: D

NEW QUESTION 384

- (Exam Topic 3)

Which Linux command when executed displays kernel ring buffers or information about device drivers loaded into the kernel?

- A. pgrep
- B. dmesg
- C. fsck
- D. grep

Answer: B

NEW QUESTION 389

- (Exam Topic 3)

What does Locard's Exchange Principle state?

- A. Any information of probative value that is either stored or transmitted in a digital form
- B. Digital evidence must have some characteristics to be disclosed in the court of law
- C. Anyone or anything, entering a crime scene takes something of the scene with them, and leaves something of themselves behind when they leave
- D. Forensic investigators face many challenges during forensics investigation of a digital crime, such as extracting, preserving, and analyzing the digital evidence

Answer: C

NEW QUESTION 391

- (Exam Topic 3)

Report writing is a crucial stage in the outcome of an investigation. Which information should not be included in the report section?

- A. Speculation or opinion as to the cause of the incident
- B. Purpose of the report
- C. Author of the report
- D. Incident summary

Answer: A

NEW QUESTION 395

- (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 399

- (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 400

- (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 401

- (Exam Topic 3)

For what purpose do the investigators use tools like iPhoneBrowser, iFunBox, OpenSSHSSH, and iMazing?

- A. Bypassing iPhone passcode
- B. Debugging iPhone
- C. Rooting iPhone
- D. Copying contents of iPhone

Answer: A

NEW QUESTION 402

- (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 405

- (Exam Topic 3)

Which of the following statements is TRUE about SQL Server error logs?

- A. SQL Server error logs record all the events occurred on the SQL Server and its databases
- B. Forensic investigator uses SQL Server Profiler to view error log files
- C. Error logs contain IP address of SQL Server client connections
- D. Trace files record, user-defined events, and specific system events

Answer: B

NEW QUESTION 408

- (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 412

- (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 417

- (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 419

- (Exam Topic 3)

Chong-lee, a forensics executive, suspects that a malware is continuously making copies of files and folders on a victim system to consume the available disk space. What type of test would confirm his claim?

- A. File fingerprinting
- B. Identifying file obfuscation
- C. Static analysis
- D. Dynamic analysis

Answer: A

NEW QUESTION 423

- (Exam Topic 3)

NTFS sets a flag for the file once you encrypt it and creates an EFS attribute where it stores Data Decryption Field (DDF) and Data Recovery Field (DDR). Which of the following is not a part of DDF?

- A. Encrypted FEK
- B. Checksum
- C. EFS Certificate Hash
- D. Container Name

Answer: B

NEW QUESTION 425

- (Exam Topic 2)

Which password cracking technique uses every possible combination of character sets?

- A. Rainbow table attack
- B. Brute force attack
- C. Rule-based attack
- D. Dictionary attack

Answer: B

NEW QUESTION 430

- (Exam Topic 2)

What is one method of bypassing a system BIOS password?

- A. Removing the processor
- B. Removing the CMOS battery
- C. Remove all the system memory
- D. Login to Windows and disable the BIOS password

Answer: B

NEW QUESTION 434

- (Exam Topic 2)

Smith, a forensic examiner, was analyzing a hard disk image to find and acquire deleted sensitive files. He stumbled upon a \$Recycle.Bin folder in the root directory of the disk. Identify the operating system in use.

- A. Windows 98
- B. Linux
- C. Windows 8.1
- D. Windows XP

Answer: D

NEW QUESTION 435

- (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 436

- (Exam Topic 2)

Company ABC has employed a firewall, IDS, Antivirus, Domain Controller, and SIEM. The company's domain controller goes down. From which system would you begin your investigation?

- A. Domain Controller
- B. Firewall
- C. SIEM
- D. IDS

Answer: C

NEW QUESTION 439

- (Exam Topic 2)

The investigator wants to examine changes made to the system's registry by the suspect program. Which of the following tool can help the investigator?

- A. TRIPWIRE
- B. RAM Capturer
- C. Regshot
- D. What's Running

Answer: C

NEW QUESTION 441

- (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 443

- (Exam Topic 2)

Which of the following Event Correlation Approach is an advanced correlation method that assumes and predicts what an attacker can do next after the attack by studying the statistics and probability and uses only two variables?

- A. Bayesian Correlation
- B. Vulnerability-Based Approach
- C. Rule-Based Approach
- D. Route Correlation

Answer: A

NEW QUESTION 447

- (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 451

- (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 454

- (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 459

- (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 463

- (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 464

- (Exam Topic 2)

What type of equipment would a forensics investigator store in a StrongHold bag?

- A. PDAPDA?
- B. Backup tapes
- C. Hard drives
- D. Wireless cards

Answer: D

NEW QUESTION 469

- (Exam Topic 2)

When searching through file headers for picture file formats, what should be searched to find a JPEG file in hexadecimal format?

- A. FF D8 FF E0 00 10
- B. FF FF FF FF FF FF
- C. FF 00 FF 00 FF 00
- D. EF 00 EF 00 EF 00

Answer: A

NEW QUESTION 473

- (Exam Topic 2)

What will the following command accomplish in Linux? `fdisk /dev/hda`

- A. Partition the hard drive
- B. Format the hard drive
- C. Delete all files under the /dev/hda folder
- D. Fill the disk with zeros

Answer: A

NEW QUESTION 474

- (Exam Topic 2)

What is the primary function of the tool CHKDSK in Windows that authenticates the file system reliability of a volume?

- A. Repairs logical file system errors
- B. Check the disk for hardware errors
- C. Check the disk for connectivity errors
- D. Check the disk for Slack Space

Answer: A

NEW QUESTION 476

- (Exam Topic 2)

Which of the following reports are delivered under oath to a board of directors/managers/panel of the jury?

- A. Written Formal Report
- B. Verbal Formal Report
- C. Verbal Informal Report
- D. Written Informal Report

Answer: B

NEW QUESTION 478

- (Exam Topic 2)

All Blackberry email is eventually sent and received through what proprietary RIM-operated mechanism?

- A. Blackberry Message Center
- B. Microsoft Exchange
- C. Blackberry WAP gateway
- D. Blackberry WEP gateway

Answer: A

NEW QUESTION 480

- (Exam Topic 2)

The process of restarting a computer that is already turned on through the operating system is called?

- A. Warm boot
- B. Ice boot
- C. Hot Boot
- D. Cold boot

Answer: A

NEW QUESTION 485

- (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 489

- (Exam Topic 2)

The surface of a hard disk consists of several concentric rings known as tracks; each of these tracks has smaller partitions called disk blocks. What is the size of each block?

- A. 512 bits
- B. 512 bytes
- C. 256 bits
- D. 256 bytes

Answer: B

NEW QUESTION 493

- (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 495

- (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 499

- (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 502

- (Exam Topic 2)

A small law firm located in the Midwest has possibly been breached by a computer hacker looking to obtain information on their clientele. The law firm does not have any on-site IT employees, but wants to search for evidence of the breach themselves to prevent any possible media attention. Why would this not be recommended?

- A. Searching for evidence themselves would not have any ill effects

- B. Searching could possibly crash the machine or device
- C. Searching creates cache files, which would hinder the investigation
- D. Searching can change date/time stamps

Answer: D

NEW QUESTION 503

- (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 508

- (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 510

- (Exam Topic 2)

Which forensic investigating concept trails the whole incident from how the attack began to how the victim was affected?

- A. Point-to-point
- B. End-to-end
- C. Thorough
- D. Complete event analysis

Answer: B

NEW QUESTION 511

- (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 514

- (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 517

- (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 520

- (Exam Topic 2)

Jason discovered a file named \$RIYG6VR.doc in the C:\\$Recycle.Bin\\ while analyzing a hard disk image for the deleted data. What inferences can he make from the file name?

- A. It is a doc file deleted in seventh sequential order
- B. RIYG6VR.doc is the name of the doc file deleted from the system
- C. It is file deleted from R drive
- D. It is a deleted doc file

Answer: D

NEW QUESTION 524

- (Exam Topic 2)

Why should you never power on a computer that you need to acquire digital evidence from?

- A. When the computer boots up, files are written to the computer rendering the data nclean
- B. When the computer boots up, the system cache is cleared which could destroy evidence
- C. When the computer boots up, data in the memory buffer is cleared which could destroy evidence
- D. Powering on a computer has no affect when needing to acquire digital evidence from it

Answer: A

NEW QUESTION 527

- (Exam Topic 2)

This type of testimony is presented by someone who does the actual fieldwork and does not offer a view in court.

- A. Civil litigation testimony
- B. Expert testimony
- C. Victim advocate testimony
- D. Technical testimony

Answer: D

NEW QUESTION 530

- (Exam Topic 2)

What type of attack sends spoofed UDP packets (instead of ping packets) with a fake source address to the IP broadcast address of a large network?

- A. Fraggle
- B. Smurf scan
- C. SYN flood
- D. Teardrop

Answer: A

NEW QUESTION 532

- (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 535

- (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 538

- (Exam Topic 2)

While presenting his case to the court, Simon calls many witnesses to the stand to testify. Simon decides to call Hillary Taft, a lay witness, to the stand. Since Hillary is a lay witness, what field would she be considered an expert in?

- A. Technical material related to forensics
- B. No particular field
- C. Judging the character of defendants/victims
- D. Legal issues

Answer: B

NEW QUESTION 542

- (Exam Topic 2)

The following is a log file screenshot from a default installation of IIS 6.0.

```
#Software: Microsoft Internet Information Services 6.0
#Version: 1.0
#Date: 2007-01-22 15:42:36
#Fields: date time s-sitename s-ip cs-method cs-uri-stem cs-uri-query s-port cs-user
2007-01-22 15:42:36 w3svc1 172.16.28.102 GET /index.html - 80 - 172.16.28.80
Mozilla/4.0+(compatible;+MSIE+6.0;+windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 w3svc1 172.16.28.102 GET /Development/index.asp - 80 - 172.16.28
Mozilla/4.0+(compatible;+MSIE+6.0;+windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 w3svc1 172.16.28.102 GET /Development/css/olcStyle.css - 80 - 17
Mozilla/4.0+(compatible;+MSIE+6.0;+windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 w3svc1 172.16.28.102 GET /Favicon.ico - 80 - 172.16.28.80 Avant+
2007-01-22 15:42:36 w3svc1 172.16.28.102 GET /Development/css/dhtml_horiz.css - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 w3svc1 172.16.28.102 GET /Development/images/index_01.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 w3svc1 172.16.28.102 GET /Development/images/index_02.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 w3svc1 172.16.28.102 GET /Development/images/index_03.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 w3svc1 172.16.28.102 GET /Development/images/index_04.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 w3svc1 172.16.28.102 GET /Development/images/index_06.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 w3svc1 172.16.28.102 GET /Development/images/index_07.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 w3svc1 172.16.28.102 GET /Development/images/index_08.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 w3svc1 172.16.28.102 GET /Development/script/dhtml.js - 80 - 172
Mozilla/4.0+(compatible;+MSIE+6.0;+windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 w3svc1 172.16.28.102 GET /Development/images/greenArrow.jpg - 80
Mozilla/4.0+(compatible;+MSIE+6.0;+windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 w3svc1 172.16.28.102 GET /Development/images/board_01.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 w3svc1 172.16.28.102 GET /Development/images/board_02.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
```

What time standard is used by IIS as seen in the screenshot?

- A. UTC
- B. GMT
- C. TAI
- D. UT

Answer: A

NEW QUESTION 546

- (Exam Topic 2)

What is the size value of a nibble?

- A. 0.5 kilo byte
- B. 0.5 bit
- C. 0.5 byte
- D. 2 bits

Answer: C

NEW QUESTION 548

- (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 550

- (Exam Topic 2)

Richard is extracting volatile data from a system and uses the command doskey/history. What is he trying to extract?

- A. Events history
- B. Previously typed commands
- C. History of the browser
- D. Passwords used across the system

Answer: B

NEW QUESTION 554

- (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 557

- (Exam Topic 2)

Where are files temporarily written in Unix when printing?

- A. /usr/spool
- B. /var/print
- C. /spool
- D. /var/spool

Answer: D

NEW QUESTION 560

- (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 563

- (Exam Topic 2)

In handling computer-related incidents, which IT role should be responsible for recovery, containment, and prevention to constituents?

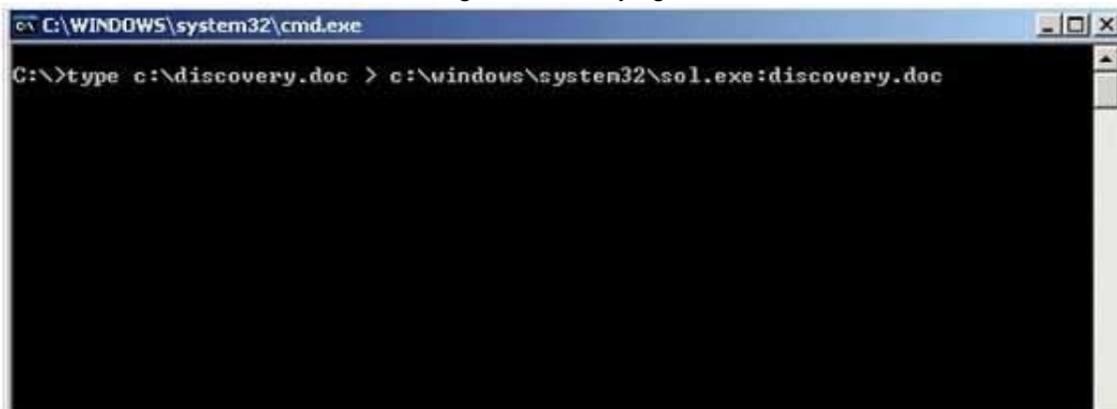
- A. Security Administrator
- B. Network Administrator
- C. Director of Information Technology
- D. Director of Administration

Answer: B

NEW QUESTION 564

- (Exam Topic 2)

What feature of Windows is the following command trying to utilize?



- A. White space
- B. AFS
- C. ADS
- D. Slack file

Answer: C

NEW QUESTION 568

- (Exam Topic 2)

Microsoft Security IDs are available in Windows Registry Editor. The path to locate IDs in Windows 7 is:

- A. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList
- B. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProfileList
- C. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\RegList
- D. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Regedit

Answer: A

NEW QUESTION 573

- (Exam Topic 2)

If you are concerned about a high level of compression but not concerned about any possible data loss, what type of compression would you use?

- A. Lossful compression
- B. Lossy compression
- C. Lossless compression
- D. Time-loss compression

Answer: B

NEW QUESTION 578

- (Exam Topic 2)

What technique used by Encase makes it virtually impossible to tamper with evidence once it has been acquired?

- A. Every byte of the file(s) is given an MD5 hash to match against a master file
- B. Every byte of the file(s) is verified using 32-bit CRC
- C. Every byte of the file(s) is copied to three different hard drives
- D. Every byte of the file(s) is encrypted using three different methods

Answer: B

NEW QUESTION 579

- (Exam Topic 2)

Using Linux to carry out a forensics investigation, what would the following command accomplish? `dd if=/usr/home/partition.image of=/dev/sdb2 bs=4096 conv=notrunc,noerror`

- A. Search for disk errors within an image file
- B. Backup a disk to an image file
- C. Copy a partition to an image file
- D. Restore a disk from an image file

Answer: D

NEW QUESTION 582

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions 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](#)