

Exam Questions 312-49v10

Computer Hacking Forensic Investigator (CHFI-v10)

<https://www.2passeasy.com/dumps/312-49v10/>



NEW QUESTION 1

- (Exam Topic 1)

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

- A. Keep the information of file for later review
- B. Destroy the evidence
- C. Bring the information to the attention of the prosecutor, his or her supervisor or finally to the judge
- D. Present the evidence to the defense attorney

Answer: C

NEW QUESTION 2

- (Exam Topic 1)

What operating system would respond to the following command?

- A. Windows 95
- B. FreeBSD
- C. Windows XP
- D. Mac OS X

Answer: B

NEW QUESTION 3

- (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 4

- (Exam Topic 1)

In a forensic examination of hard drives for digital evidence, what type of user is most likely to have the most file slack to analyze?

- A. one who has NTFS 4 or 5 partitions
- B. one who uses dynamic swap file capability
- C. one who uses hard disk writes on IRQ 13 and 21
- D. one who has lots of allocation units per block or cluster

Answer: D

NEW QUESTION 5

- (Exam Topic 1)

George is performing security analysis for Hammond and Sons LLC. He is testing security vulnerabilities of their wireless network. He plans on remaining as "stealthy" as possible during the scan. Why would a scanner like Nessus is not recommended in this situation?

- A. Nessus is too loud
- B. Nessus cannot perform wireless testing
- C. Nessus is not a network scanner
- D. There are no ways of performing a "stealthy" wireless scan

Answer: A

NEW QUESTION 6

- (Exam Topic 1)

After passing her CEH exam, Carol wants to ensure that her network is completely secure. She implements a DMZ, stateful firewall, NAT, IPSEC, and a packet filtering firewall. Since all security measures were taken, none of the hosts on her network can reach the Internet. Why is that?

- A. Stateful firewalls do not work with packet filtering firewalls
- B. NAT does not work with stateful firewalls
- C. IPSEC does not work with packet filtering firewalls
- D. NAT does not work with IPSEC

Answer: D

NEW QUESTION 7

- (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 8

- (Exam Topic 1)

Chris has been called upon to investigate a hacking incident reported by one of his clients. The company suspects the involvement of an insider accomplice in the attack. Upon reaching the incident scene, Chris secures the physical area, records the scene using visual media. He shuts the system down by pulling the power plug so that he does not disturb the system in any way. He labels all cables and connectors prior to disconnecting any. What do you think would be the next sequence of events?

- A. Connect the target media; prepare the system for acquisition; Secure the evidence; Copy the media
- B. Prepare the system for acquisition; Connect the target media; copy the media; Secure the evidence
- C. Connect the target media; Prepare the system for acquisition; Secure the evidence; Copy the media
- D. Secure the evidence; prepare the system for acquisition; Connect the target media; copy the media

Answer: B

NEW QUESTION 9

- (Exam Topic 1)

When you are running a vulnerability scan on a network and the IDS cuts off your connection, what type of IDS is being used?

- A. Passive IDS
- B. Active IDS
- C. Progressive IDS
- D. NIPS

Answer: B

NEW QUESTION 10

- (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 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 11

- (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 15

- (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 17

- (Exam Topic 1)

When setting up a wireless network with multiple access points, why is it important to set each access point on a different channel?

- A. Multiple access points can be set up on the same channel without any issues
- B. Avoid over-saturation of wireless signals
- C. So that the access points will work on different frequencies
- D. Avoid cross talk

Answer: D

NEW QUESTION 19

- (Exam Topic 1)

Paul's company is in the process of undergoing a complete security audit including logical and physical security testing. After all logical tests were performed; it is now time for the physical round to begin. None of the employees are made aware of this round of testing. The security-auditing firm sends in a technician dressed as an electrician. He waits outside in the lobby for some employees to get to work and follows behind them when they access the restricted areas. After entering the main office, he is able to get into the server room telling the IT manager that there is a problem with the outlets in that room. What type of attack has the technician performed?

- A. Tailgating
- B. Backtrapping
- C. Man trap attack
- D. Fuzzing

Answer: A

NEW QUESTION 24

- (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 27

- (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 32

- (Exam Topic 2)

What technique is used by JPEGs for compression?

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

Answer: C

NEW QUESTION 35

- (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 40

- (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 41

- (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 46

- (Exam Topic 2)

What type of attack sends SYN requests to a target system with spoofed IP addresses?

- A. SYN flood
- B. Ping of death
- C. Cross site scripting
- D. Land

Answer: A

NEW QUESTION 48

- (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 53

- (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 54

- (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 58

- (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 63

- (Exam Topic 1)

What binary coding is used most often for e-mail purposes?

- A. MIME
- B. Uuencode
- C. IMAP
- D. SMTP

Answer: A

NEW QUESTION 66

- (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 67

- (Exam Topic 1)

After undergoing an external IT audit, George realizes his network is vulnerable to DDoS attacks. What countermeasures could he take to prevent DDoS attacks?

- A. Enable direct broadcasts
- B. Disable direct broadcasts
- C. Disable BGP
- D. Enable BGP

Answer: B

NEW QUESTION 71

- (Exam Topic 1)

You are working for a large clothing manufacturer as a computer forensics investigator and are called in to investigate an unusual case of an employee possibly stealing clothing designs from the company and selling them under a different brand name for a different company. What you discover during the course of the investigation is that the clothing designs are actually original products of the employee and the company has no policy against an employee selling his own designs on his own time. The only thing that you can find that the employee is doing wrong is that his clothing design incorporates the same graphic symbol as that of the company with only the wording in the graphic being different. What area of the law is the employee violating?

- A. trademark law
- B. copyright law
- C. printright law
- D. landmark law

Answer: A

NEW QUESTION 75

- (Exam Topic 1)

You have used a newly released forensic investigation tool, which doesn't meet the Daubert Test, during a case. The case has ended-up in court. What argument could the defense make to weaken your case?

- A. The tool hasn't been tested by the International Standards Organization (ISO)
- B. Only the local law enforcement should use the tool
- C. The tool has not been reviewed and accepted by your peers
- D. You are not certified for using the tool

Answer: C

NEW QUESTION 78

- (Exam Topic 1)

You setup SNMP in multiple offices of your company. Your SNMP software manager is not receiving data from other offices like it is for your main office. You suspect that firewall changes are to blame. What ports should you open for SNMP to work through Firewalls? (Choose two.)

- A. 162
- B. 161
- C. 163
- D. 160

Answer: AB

NEW QUESTION 80

- (Exam Topic 1)

If an attacker's computer sends an IPID of 31400 to a zombie computer on an open port in IDLE scanning, what will be the response?

- A. The zombie will not send a response
- B. 31402
- C. 31399
- D. 31401

Answer: D

NEW QUESTION 84

- (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 86

- (Exam Topic 1)

When investigating a network that uses DHCP to assign IP addresses, where would you look to determine which system (MAC address) had a specific IP address at a specific time?

- A. on the individual computer's ARP cache
- B. in the Web Server log files
- C. in the DHCP Server log files
- D. there is no way to determine the specific IP address

Answer: C

NEW QUESTION 90

- (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 93

- (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 96

- (Exam Topic 1)

What information do you need to recover when searching a victim's computer for a crime committed with specific e-mail message?

- A. Internet service provider information
- B. E-mail header
- C. Username and password
- D. Firewall log

Answer: B

NEW QUESTION 97

- (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 101

- (Exam Topic 1)

Printing under a Windows Computer normally requires which one of the following files types to be created?

- A. EME
- B. MEM
- C. EMF
- D. CME

Answer: C

NEW QUESTION 104

- (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 105

- (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 110

- (Exam Topic 1)

One way to identify the presence of hidden partitions on a suspect's hard drive is to:

- A. Add up the total size of all known partitions and compare it to the total size of the hard drive
- B. Examine the FAT and identify hidden partitions by noting an H in the partition Type field
- C. Examine the LILO and note an H in the partition Type field
- D. It is not possible to have hidden partitions on a hard drive

Answer: A

NEW QUESTION 112

- (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 113

- (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 118

- (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 123

- (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 125

- (Exam Topic 1)

You are called by an author who is writing a book and he wants to know how long the copyright for his book will last after he has the book published?

- A. 70 years
- B. the life of the author
- C. the life of the author plus 70 years
- D. copyrights last forever

Answer: C

NEW QUESTION 129

- (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 134

- (Exam Topic 1)

In a computer forensics investigation, what describes the route that evidence takes from the time you find it until the case is closed or goes to court?

- A. rules of evidence
- B. law of probability
- C. chain of custody
- D. policy of separation

Answer: C

NEW QUESTION 135

- (Exam Topic 1)

Study the log given below and answer the following question:

```
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
Precautionary measures to prevent this attack would include writing firewall rules. Of these firewall rules, which among the following would be appropriate?

- A. Disallow UDP53 in from outside to DNS server
- B. Allow UDP53 in from DNS server to outside
- C. Disallow TCP53 in from secondaries or ISP server to DNS server
- D. Block all UDP traffic

Answer: A

NEW QUESTION 136

- (Exam Topic 1)

George is the network administrator of a large Internet company on the west coast. Per corporate policy, none of the employees in the company are allowed to use FTP or SFTP programs without obtaining approval from the IT department. Few managers are using SFTP program on their computers. Before talking to his boss, George wants to have some proof of their activity. George wants to use Ethereal to monitor network traffic, but only SFTP traffic to and from his network. What filter should George use in Ethereal?

- A. src port 23 and dst port 23
- B. udp port 22 and host 172.16.28.1/24
- C. net port 22
- D. src port 22 and dst port 22

Answer: D

NEW QUESTION 138

- (Exam Topic 1)

What does the superblock in Linux define?

- A. filesynames
- B. diskgeometr
- C. location of the firstinode
- D. available space

Answer: C

NEW QUESTION 142

- (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 146

- (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 148

- (Exam Topic 1)

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

- A. Trace the IP address to its origin
- B. Write a report
- C. Determine whether a crime was actually committed
- D. Recover the evidence

Answer: A

NEW QUESTION 152

- (Exam Topic 1)

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

Although they found very few issues, they were able to enumerate the model, OS version, and capabilities for all your Cisco routers with very little effort. Which

feature will you disable to eliminate the ability to enumerate this information on your Cisco routers?

- A. Border Gateway Protocol
- B. Cisco Discovery Protocol
- C. Broadcast System Protocol
- D. Simple Network Management Protocol

Answer: B

NEW QUESTION 153

- (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 157

- (Exam Topic 1)

Which Intrusion Detection System (IDS) usually produces the most false alarms due to the unpredictable behaviors of users and networks?

- A. network-based IDS systems (NIDS)
- B. host-based IDS systems (HIDS)
- C. anomaly detection
- D. signature recognition

Answer: B

NEW QUESTION 162

- (Exam Topic 1)

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

- A. The IP address of the employees' computers
- B. Bank account numbers and the corresponding routing numbers
- C. The employees network usernames and passwords
- D. The MAC address of the employees' computers

Answer: C

NEW QUESTION 166

- (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 169

- (Exam Topic 1)

You work as an IT security auditor hired by a law firm in Boston to test whether you can gain access to sensitive information about the company clients. You have rummaged through their trash and found very little information. You do not want to set off any alarms on their network, so you plan on performing passive foot printing against their Web servers. What tool should you use?

- A. Ping sweep
- B. Nmap
- C. Netcraft
- D. Dig

Answer: C

NEW QUESTION 171

- (Exam Topic 1)

Why is it a good idea to perform a penetration test from the inside?

- A. It is never a good idea to perform a penetration test from the inside
- B. Because 70% of attacks are from inside the organization
- C. To attack a network from a hacker's perspective
- D. It is easier to hack from the inside

Answer: B

NEW QUESTION 172

- (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 175

- (Exam Topic 1)

You are the network administrator for a small bank in Dallas, Texas. To ensure network security, you enact a security policy that requires all users to have 14 character passwords. After giving your users 2 weeks notice, you change the Group Policy to force 14 character passwords. A week later you dump the SAM database from the standalone server and run a password-cracking tool against it. Over 99% of the passwords are broken within an hour. Why were these passwords cracked so Quickly?

- A. Passwords of 14 characters or less are broken up into two 7-character hashes
- B. A password Group Policy change takes at least 3 weeks to completely replicate throughout a network
- C. Networks using Active Directory never use SAM databases so the SAM database pulled was empty
- D. The passwords that were cracked are local accounts on the Domain Controller

Answer: A

NEW QUESTION 176

- (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 177

- (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 182

- (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 184

- (Exam Topic 1)

You are working on a thesis for your doctorate degree in Computer Science. Your thesis is based on HTML, DHTML, and other web-based languages and how they have evolved over the years.

You navigate to archive. org and view the HTML code of news.com. You then navigate to the current news.com website and copy over the source code. While searching through the code, you come across something abnormal: What have you found?

- A. Web bug
- B. CGI code
- C. Trojan.downloader
- D. Blind bug

Answer: A

NEW QUESTION 185

- (Exam Topic 1)

What is the following command trying to accomplish?

- A. Verify that UDP port 445 is open for the 192.168.0.0 network
- B. Verify that TCP port 445 is open for the 192.168.0.0 network
- C. Verify that NETBIOS is running for the 192.168.0.0 network
- D. Verify that UDP port 445 is closed for the 192.168.0.0 network

Answer: A

NEW QUESTION 186

- (Exam Topic 1)

When examining a file with a Hex Editor, what space does the file header occupy?

- A. the last several bytes of the file
- B. the first several bytes of the file
- C. none, file headers are contained in the FAT
- D. one byte at the beginning of the file

Answer: D

NEW QUESTION 190

- (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 195

- (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 199

- (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 203

- (Exam Topic 1)

You are using DriveSpy, a forensic tool and want to copy 150 sectors where the starting sector is 1709 on the primary hard drive. Which of the following formats correctly specifies these sectors?

- A. 0:1000, 150
- B. 0:1709, 150
- C. 1:1709, 150
- D. 0:1709-1858

Answer: B

NEW QUESTION 206

- (Exam Topic 1)

The efforts to obtain information before a trial 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 210

- (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 215

- (Exam Topic 1)

Harold is a web designer who has completed a website for ghttech.net. As part of the maintenance agreement he signed with the client, Harold is performing research online and seeing how much exposure the site has received so far. Harold navigates to google.com and types in the following search. link:www.ghttech.net What will this search produce?

- A. All sites that ghttech.net links to
- B. All sites that link to ghttech.net
- C. All search engines that link to .net domains
- D. Sites that contain the code: link:www.ghttech.net

Answer: B

NEW QUESTION 218

- (Exam Topic 1)

To make sure the evidence you recover and analyze with computer forensics software can be admitted in court, you must test and validate the software. What group is actively providing tools and creating procedures for testing and validating computer forensics software?

- A. Computer Forensics Tools and Validation Committee (CFTVC)
- B. Association of Computer Forensics Software Manufacturers (ACFSM)
- C. National Institute of Standards and Technology (NIST)
- D. Society for Valid Forensics Tools and Testing (SVFTT)

Answer: C

NEW QUESTION 223

- (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 228

- (Exam Topic 1)

Which is a standard procedure to perform during all computer forensics investigations?

- A. with the hard drive removed from the suspect PC, check the date and time in the system's CMOS
- B. with the hard drive in the suspect PC, check the date and time in the File Allocation Table
- C. with the hard drive removed from the suspect PC, check the date and time in the system's RAM
- D. with the hard drive in the suspect PC, check the date and time in the system's CMOS

Answer: A

NEW QUESTION 229

- (Exam Topic 1)

Microsoft Outlook maintains email messages in a proprietary format in what type of file?

- A. .email
- B. .mail
- C. .pst
- D. .doc

Answer: C

NEW QUESTION 230

- (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 233

- (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 238

- (Exam Topic 1)

You are working for a local police department that services a population of 1,000,000 people and you have been given the task of building a computer forensics lab. How many law-enforcement computer investigators should you request to staff the lab?

- A. 8
- B. 1
- C. 4
- D. 2

Answer: C

NEW QUESTION 240

- (Exam Topic 1)

The police believe that Melvin Matthew has been obtaining unauthorized access to computers belonging to numerous computer software and computer operating systems manufacturers, cellular telephone manufacturers, Internet Service Providers and Educational Institutions. They also suspect that he has been stealing, copying and misappropriating proprietary computer software belonging to the several victim companies. What is preventing the police from breaking down the suspects door and searching his home and seizing all of his computer equipment if they have not yet obtained a warrant?

- A. The Fourth Amendment
- B. The USA patriot Act
- C. The Good Samaritan Laws
- D. The Federal Rules of Evidence

Answer: A

NEW QUESTION 244

- (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 249

- (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 253

- (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 256

- (Exam Topic 1)

The newer Macintosh Operating System is based on:

- A. OS/2
- B. BSD Unix
- C. Linux
- D. Microsoft Windows

Answer: B

NEW QUESTION 260

- (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 261

- (Exam Topic 1)

What type of file is represented by a colon (:) with a name following it in the Master File Table of NTFS disk?

- A. A compressed file
- B. A Data stream file
- C. An encrypted file
- D. A reserved file

Answer: B

NEW QUESTION 262

- (Exam Topic 1)

You work as a penetration tester for Hammond Security Consultants. You are currently working on a contract for the state government of California. Your next step is to initiate a DoS attack on their network. Why would you want to initiate a DoS attack on a system you are testing?

- A. Show outdated equipment so it can be replaced
- B. List weak points on their network
- C. Use attack as a launching point to penetrate deeper into the network
- D. Demonstrate that no system can be protected against DoS attacks

Answer: B

NEW QUESTION 263

- (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 264

- (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 267

- (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 269

- (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 272

- (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 276

- (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 280

- (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 284

- (Exam Topic 1)

An Expert witness give an opinion if:

- A. The Opinion, inferences or conclusions depend on special knowledge, skill or training not within the ordinary experience of lay jurors
- B. To define the issues of the case for determination by the finder of fact
- C. To stimulate discussion between the consulting expert and the expert witness
- D. To deter the witness from expanding the scope of his or her investigation beyond the requirements of the case

Answer: A

NEW QUESTION 287

- (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 292

- (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 296

- (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 298

- (Exam Topic 4)

This law sets the rules for commercial email, establishes requirements for commercial messages, gives recipients the right to have you stop emailing them, and spells out tough penalties for violations.

- A. The CAN-SPAM act
- B. Federal Spam act
- C. Telemarketing act
- D. European Anti-Spam act

Answer: A

NEW QUESTION 302

- (Exam Topic 4)

You are a forensic investigator who is analyzing a hard drive that was recently collected as evidence. You have been unsuccessful at locating any meaningful evidence within the file system and suspect a drive wiping utility may have been used. You have reviewed the keys within the software hive of the Windows registry and did not find any drive wiping utilities. How can you verify that drive wiping software was used on the hard drive?

- A. Document in your report that you suspect a drive wiping utility was used, but no evidence was found
- B. Check the list of installed programs
- C. Load various drive wiping utilities offline, and export previous run reports
- D. Look for distinct repeating patterns on the hard drive at the bit level

Answer: D

NEW QUESTION 304

- (Exam Topic 4)

"No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court" - this principle is advocated by which of the following?

- A. The Association of Chief Police Officers (ACPO) Principles of Digital Evidence
- B. Locard's exchange principle
- C. Scientific Working Group on Imaging Technology (SWGIT)
- D. FBI Cyber Division

Answer: A

NEW QUESTION 307

- (Exam Topic 4)

An investigator is examining a file to identify any potentially malicious content. To avoid code execution and still be able to uncover hidden indicators of

compromise (IOC), which type of examination should the investigator perform:

- A. Threat hunting
- B. Threat analysis
- C. Static analysis
- D. Dynamic analysis

Answer: B

NEW QUESTION 312

- (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 315

- (Exam Topic 4)

Storage location of Recycle Bin for NTFS file systems (Windows Vista and later) is located at:

- A. Drive:\\$ Recycl
- B. Bin
- C. Drive\ARECYCIE.BIN
- D. Drive:\RECYCLER
- E. Drive:\RECYCLED

Answer: C

NEW QUESTION 320

- (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 321

- (Exam Topic 4)

Which OWASP IoT vulnerability talks about security flaws such as lack of firmware validation, lack of secure delivery, and lack of anti-rollback mechanisms on IoT 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 326

- (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 329

- (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 332

- (Exam Topic 4)

Which of the following methods of mobile device data acquisition captures all the data present on the device, as well as all deleted data and access to unallocated space?

- A. Manual acquisition
- B. Logical acquisition
- C. Direct acquisition
- D. Physical acquisition

Answer: D

NEW QUESTION 337

- (Exam Topic 4)

In a Filesystem Hierarchy Standard (FHS), which of the following directories contains the binary files required for working?

- A. /sbin
- B. /proc
- C. /mm
- D. /media

Answer: A

NEW QUESTION 340

- (Exam Topic 4)

Which of the following malware targets Android mobile devices and installs a backdoor that remotely installs applications from an attacker-controlled server?

- A. Felix
- B. XcodeGhost
- C. xHelper
- D. Unflod

Answer: C

NEW QUESTION 344

- (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 348

- (Exam Topic 4)

Which of the following statements pertaining to First Response is true?

- A. First Response is a part of the investigation phase
- B. First Response is a part of the post-investigation phase
- C. First Response is a part of the pre-investigation phase
- D. First Response is neither a part of pre-investigation phase nor a part of investigation phase
- E. It only involves attending to a crime scene first and taking measures that assist forensic investigators in executing their tasks in the investigation phase more efficiently

Answer: A

NEW QUESTION 350

- (Exam Topic 4)

Ronald, a forensic investigator, has been hired by a financial services organization to investigate an attack on their MySQL database server, which is hosted on a Windows machine named WIN-DTRAI83202X. Ronald wants to retrieve information on the changes that have been made to the database. Which of the following files should Ronald examine for this task?

- A. relay-log.info
- B. WIN-DTRAI83202Xrelay-bin.index

- C. WIN-DTRAI83202Xslow.log
- D. WIN-DTRAI83202X-bin.nnnnnn

Answer: C

NEW QUESTION 354

- (Exam Topic 4)

What happens to the header of the file once it is deleted from the Windows OS file systems?

- A. The OS replaces the first letter of a deleted file name with a hex byte code: E5h
- B. The OS replaces the entire hex byte coding of the file.
- C. The hex byte coding of the file remains the same, but the file location differs
- D. The OS replaces the second letter of a deleted file name with a hex byte code: Eh5

Answer: A

NEW QUESTION 355

- (Exam Topic 4)

What is the extension used by Windows OS for shortcut files present on the machine?

- A. .log
- B. .pf
- C. .lnk
- D. .dat

Answer: C

NEW QUESTION 356

- (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 360

- (Exam Topic 4)

Which of the following is the most effective tool for acquiring volatile data from a Windows-based system?

- A. Coreography
- B. Datagrab
- C. Ethereal
- D. Helix

Answer: D

NEW QUESTION 364

- (Exam Topic 4)

Which of the following directory contains the binary files or executables required for system maintenance and administrative tasks on a Linux system?

- A. /sbin
- B. /bin
- C. /usr
- D. /lib

Answer: A

NEW QUESTION 368

- (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 371

- (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 375

- (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 378

- (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 382

- (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 384

- (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 385

- (Exam Topic 4)

Chloe is a forensic examiner who is currently cracking hashed passwords for a crucial mission and hopefully solve the case. She is using a lookup table used for recovering a plain text password from cipher text; it contains word list and brute-force list along with their computed hash values. Chloe Is also using a graphical generator that supports SHA1.

* a. What password technique is being used?

* b. What tool is Chloe using?

- A. Dictionary attack
- B. Cisco PIX
- C. Cain & Able
- D. Rten
- E. Brute-force
- F. MScache
- G. Rainbow Tables
- H. Winrtgen

Answer: D

NEW QUESTION 390

- (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 395

- (Exam Topic 4)

An EC2 instance storing critical data of a company got infected with malware. The forensics team took the EBS volume snapshot of the affected Instance to perform further analysis and collected other data of evidentiary value. What should be their next step?

- A. They should pause the running instance
- B. They should keep the instance running as it stores critical data
- C. They should terminate all instances connected via the same VPC
- D. They should terminate the instance after taking necessary backup

Answer: D

NEW QUESTION 396

- (Exam Topic 4)

Which of the following attacks refers to unintentional download of malicious software via the Internet? Here, an attacker exploits flaws in browser software to install malware merely by the user visiting the malicious website.

- A. Malvertising
- B. Internet relay chats
- C. Drive-by downloads
- D. Phishing

Answer: C

NEW QUESTION 398

- (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 399

- (Exam Topic 4)

A computer forensics Investigator or forensic analyst is a specially trained professional who works with law enforcement as well as private businesses to retrieve information from computers and other types of data storage devices. For this, the analyst should have an excellent working knowledge of all aspects of the computer. Which of the following is not a duty of the analyst during a criminal investigation?

- A. To create an investigation report
- B. To fill the chain of custody
- C. To recover data from suspect devices
- D. To enforce the security of all devices and software in the scene

Answer: D

NEW QUESTION 403

- (Exam Topic 4)

Debbie has obtained a warrant to search a known pedophile's 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 old
- E. had a cracked screen, and did not have batteries
- F. Therefore, it could not have been used in a crime.

Answer: A

NEW QUESTION 404

- (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 409

- (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 414

- (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 416

- (Exam Topic 3)

Which of the following Perl scripts will help an investigator to access the executable image of a process?

- A. Lspd.pl
- B. Lpsi.pl
- C. Lspm.pl
- D. Lspi.pl

Answer: D

NEW QUESTION 421

- (Exam Topic 3)

You are assigned a task to examine the log files pertaining to MyISAM storage engine. While examining, you are asked to perform a recovery operation on a MyISAM log file. Which among the following MySQL Utilities allow you to do so?

- A. mysqldump
- B. myisamaccess
- C. myisamlog
- D. myisamchk

Answer: C

NEW QUESTION 423

- (Exam Topic 3)

Bob has encountered a system crash and has lost vital data stored on the hard drive of his Windows computer. He has no cloud storage or backup hard drives. He wants to recover all the data, which includes his personal photos, music, documents, videos, official emails, etc. Which of the following tools shall resolve Bob's purpose?

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

Answer: B

NEW QUESTION 428

- (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 432

- (Exam Topic 3)

Tasklist command displays a list of applications and services with their Process ID (PID) for all tasks running on either a local or a remote computer. Which of the following tasklist commands provides information about the listed processes, including the image name, PID, name, and number of the session for the process?

- A. tasklist /p
- B. tasklist /v
- C. tasklist /u
- D. tasklist /s

Answer: B

NEW QUESTION 437

- (Exam Topic 3)

Which of the following processes is part of the dynamic malware analysis?

- A. Process Monitoring
- B. Malware disassembly
- C. Searching for the strings
- D. File fingerprinting

Answer: A

NEW QUESTION 438

- (Exam Topic 3)

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

- A. Adjacent memory locations
- B. Adjacent bit blocks
- C. Adjacent buffer locations
- D. Adjacent string locations

Answer: A

NEW QUESTION 443

- (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 444

- (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 449

- (Exam Topic 3)

Gary, a computer technician, is facing allegations of abusing children online by befriending them and sending them illicit adult images from his office computer. What type of investigation does this case require?

- A. Administrative Investigation
- B. Criminal Investigation
- C. Both Criminal and Administrative Investigation
- D. Civil Investigation

Answer: B

NEW QUESTION 452

- (Exam Topic 3)

Shane, a forensic specialist, is investigating an ongoing attack on a MySQL database server hosted on a Windows machine with SID "WIN-ABCDE12345F." Which of the following log file will help Shane in tracking all the client connections and activities performed on the database server?

- A. WIN-ABCDE12345F.err
- B. WIN-ABCDE12345F-bin.n
- C. WIN-ABCDE12345F.pid
- D. WIN-ABCDE12345F.log

Answer: D

NEW QUESTION 455

- (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 457

- (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 460

- (Exam Topic 3)

Joshua is analyzing an MSSQL database for finding the attack evidence and other details, where should he look for the database logs?

- A. Model.log
- B. Model.txt
- C. Model.ldf
- D. Model.lgf

Answer: C

NEW QUESTION 464

- (Exam Topic 3)

What does the 56.58.152.114(445) denote in a Cisco router log?

Jun 19 23:25:46.125 EST: %SEC-4-IPACCESSLOGP: list internet-inbound denied udp 67.124.115.35(8084)
-> 56.58.152.114(445), 1 packet

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

Answer: D

NEW QUESTION 466

- (Exam Topic 3)

Which of these Windows utility help you to repair logical file system errors?

- A. Resource Monitor
- B. Disk cleanup
- C. Disk defragmenter
- D. CHKDSK

Answer: D

NEW QUESTION 471

- (Exam Topic 3)

An International Mobile Equipment Identifier (IMEI) is a 15-digit number that indicates the manufacturer, model type, and country of approval for GSM devices. The first eight digits of an IMEI number that provide information about the model and origin of the mobile device is also known as:

- A. Type Allocation Code (TAC)
- B. Integrated Circuit Code (ICC)
- C. Manufacturer Identification Code (MIC)

D. Device Origin Code (DOC)

Answer: A

NEW QUESTION 475

- (Exam Topic 3)

What document does the screenshot represent?



The screenshot shows a form for evidence collection. It has several fields with folder icons: 'Laboratory or Agency Name', 'Case Number', 'Received from (Name and Title)', 'Address and Telephone Number', 'Location from where Evidence Obtained', 'Reason Evidence Was Obtained', and 'Date and Time Evidence Was Obtained'. Below these fields is a table with three columns: 'Item Number', 'Quantity', and 'Description of Item'.

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 480

- (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 485

- (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 487

- (Exam Topic 3)

In which cloud crime do attackers try to compromise the security of the cloud environment in order to steal data or inject a malware?

- A. Cloud as an Object
- B. Cloud as a Tool
- C. Cloud as an Application
- D. Cloud as a Subject

Answer: D

NEW QUESTION 491

- (Exam Topic 3)

Which of the following tool is used to locate IP addresses?

- A. SmartWhois
- B. Deep Log Analyzer

- C. Towelroot
- D. XRY LOGICAL

Answer: A

NEW QUESTION 492

- (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 496

- (Exam Topic 3)

Which of the following web browser uses the Extensible Storage Engine (ESE) database format to store browsing records, including history, cache, and cookies?

- A. Safari
- B. Mozilla Firefox
- C. Microsoft Edge
- D. Google Chrome

Answer: C

NEW QUESTION 498

- (Exam Topic 3)

During forensics investigations, investigators tend to collect the system time at first and compare it with UTC. What does the abbreviation UTC stand for?

- A. Coordinated Universal Time
- B. Universal Computer Time
- C. Universal Time for Computers
- D. Correlated Universal Time

Answer: A

NEW QUESTION 501

- (Exam Topic 3)

Brian needs to acquire data from RAID storage. Which of the following acquisition methods is recommended to retrieve only the data relevant to the investigation?

- A. Static Acquisition
- B. Sparse or Logical Acquisition
- C. Bit-stream disk-to-disk Acquisition
- D. Bit-by-bit Acquisition

Answer: B

NEW QUESTION 504

- (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 509

- (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 512

- (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 516

- (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 518

- (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 519

- (Exam Topic 3)

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

- A. net serv
- B. netmgr
- C. lusmgr
- D. net start

Answer: D

NEW QUESTION 520

- (Exam Topic 3)

Gary is checking for the devices connected to USB ports of a suspect system during an investigation. Select the appropriate tool that will help him document all the connected devices.

- A. DevScan
- B. Devcon
- C. fsutil
- D. Reg.exe

Answer: B

NEW QUESTION 525

- (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 527

- (Exam Topic 3)

Which among the following laws emphasizes the need for each Federal agency to develop, document, and implement an organization-wide program to provide information security for the information systems that support its operations and assets?

- A. FISMA

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

Answer: A

NEW QUESTION 531

- (Exam Topic 3)

companyXYZ has asked you to assess the security of their perimeter email gateway. From your office in New York you craft a specially formatted email message and send it across the Internet to an employee of CompanyXYZ. The employee of CompanyXYZ is aware.

- A. Source code review
- B. Reviewing the firewalls configuration
- C. Data items and vulnerability scanning
- D. Interviewing employees and network engineers

Answer: A

NEW QUESTION 536

- (Exam Topic 3)

What is the investigator trying to view by issuing the command displayed in the following screenshot?

```

Administrator: Command Prompt
C:\WINDOWS\system32>wmic service list brief | more
ExitCode Name ProcessId StartMode State Status
0 AdobeARMservice 2072 Auto Running OK
1077 AdobeFlashPlayerUpdateSvc 0 Manual Stopped OK
1077 AJRouter 0 Manual Stopped OK
1077 ALG 0 Manual Stopped OK
1077 AppIDSvc 0 Manual Stopped OK
0 Appinfo 1128 Manual Running OK
1077 AppMgmt 0 Manual Stopped OK
0 AppReadiness 0 Manual Stopped OK
1077 AppVClient 0 Disabled Stopped OK
0 AppXSvc 0 Manual Stopped OK
0 AudioEndpointBuilder 524 Auto Running OK
0 Audiosrv 1428 Auto Running OK
0 Browser 1128 Manual Running OK
1077 BthHFSrv 0 Manual Stopped OK
1077 bthserv 0 Manual Stopped OK
0 CDPSvc 1136 Auto Running OK
1077 CertPropSvc 0 Manual Stopped OK
0 ClipSVC 5620 Manual Running OK
1077 COMSysApp 0 Manual Stopped OK
0 CoreMessagingRegistrar 1092 Auto Running OK
  
```

- 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 537

- (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 542

- (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 547

- (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 548

- (Exam Topic 3)

An investigator enters the command `sqlcmd -S WIN-CQQMK62867E -e -s"," -E` as part of collecting the primary data file and logs from a database. What does the "WIN-CQQMK62867E" represent?

- A. Name of the Database
- B. Name of SQL Server
- C. Operating system of the system
- D. Network credentials of the database

Answer: B

NEW QUESTION 551

- (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 553

- (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 558

- (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. `lsmod -m`

Answer: B

NEW QUESTION 563

- (Exam Topic 3)

Which of the following tool can reverse machine code to assembly language?

- A. PEiD
- B. RAM Capturer
- C. IDA Pro
- D. Deep Log Analyzer

Answer: C

NEW QUESTION 566

- (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 568

- (Exam Topic 3)

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

- A. DependencyWalker
- B. SysAnalyzer
- C. PEiD
- D. ResourcesExtract

Answer: A

NEW QUESTION 569

- (Exam Topic 3)

Which of the following components within the android architecture stack take care of displaying windows owned by different applications?

- A. Media Framework
- B. Surface Manager
- C. Resource Manager
- D. Application Framework

Answer: D

NEW QUESTION 574

- (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 577

- (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 581

- (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 582

- (Exam Topic 3)

During an investigation, Noel found the following SIM card from the suspect's mobile. What does the code 89 44 represent?



- A. Issuer Identifier Number and TAC

- B. Industry Identifier and Country code
- C. Individual Account Identification Number and Country Code
- D. TAC and Industry Identifier

Answer: B

NEW QUESTION 583

- (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 584

- (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 585

- (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 586

- (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 588

- (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 592

- (Exam Topic 3)

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

- A. Status of users connected to the internet
- B. Net status of computer usage
- C. Information about network connections
- D. Status of network hardware

Answer: C

NEW QUESTION 597

- (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 600

- (Exam Topic 3)

What is the role of Alloc.c in Apache core?

- A. It handles allocation of resource pools
- B. It is useful for reading and handling of the configuration files
- C. It takes care of all the data exchange and socket connections between the client and the server
- D. It handles server start-ups and timeouts

Answer: A

NEW QUESTION 605

- (Exam Topic 3)

Robert, a cloud architect, received a huge bill from the cloud service provider, which usually doesn't happen. After analyzing the bill, he found that the cloud resource consumption was very high. He then examined the cloud server and discovered that a malicious code was running on the server, which was generating huge but harmless traffic from the server. This means that the server has been compromised by an attacker with the sole intention to hurt the cloud customer financially. Which attack is described in the above scenario?

- A. XSS Attack
- B. DDoS Attack (Distributed Denial of Service)
- C. Man-in-the-cloud Attack
- D. EDoS Attack (Economic Denial of Service)

Answer: B

NEW QUESTION 609

- (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 612

- (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 616

- (Exam Topic 3)

What value of the "Boot Record Signature" is used to indicate that the boot-loader exists?

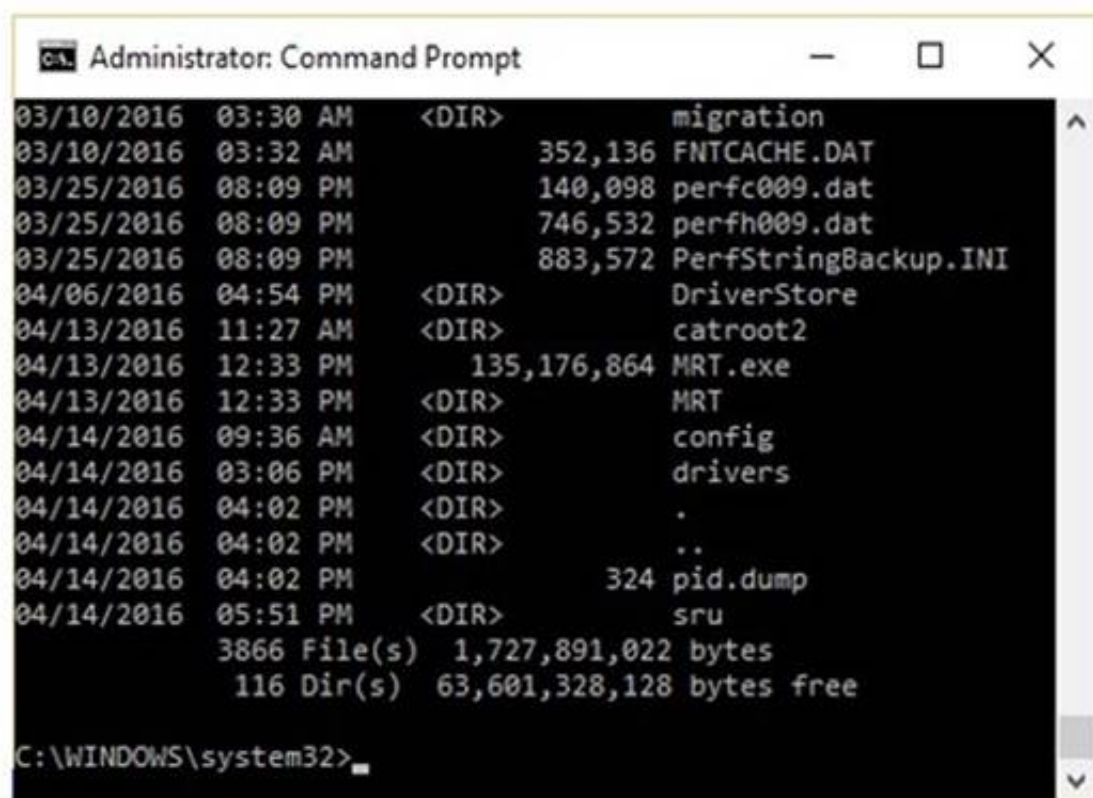
- A. AA55
- B. 00AA
- C. AA00
- D. A100

Answer: A

NEW QUESTION 620

- (Exam Topic 3)

The given image displays information about date and time of installation of the OS along with service packs, patches, and sub-directories. What command or tool did the investigator use to view this output?



```

Administrator: Command Prompt
03/10/2016 03:30 AM <DIR> migration
03/10/2016 03:32 AM 352,136 FNTCACHE.DAT
03/25/2016 08:09 PM 140,098 perfc009.dat
03/25/2016 08:09 PM 746,532 perfh009.dat
03/25/2016 08:09 PM 883,572 PerfStringBackup.INI
04/06/2016 04:54 PM <DIR> DriverStore
04/13/2016 11:27 AM <DIR> catroot2
04/13/2016 12:33 PM 135,176,864 MRT.exe
04/13/2016 12:33 PM <DIR> MRT
04/14/2016 09:36 AM <DIR> config
04/14/2016 03:06 PM <DIR> drivers
04/14/2016 04:02 PM <DIR> .
04/14/2016 04:02 PM <DIR> ..
04/14/2016 04:02 PM 324 pid.dump
04/14/2016 05:51 PM <DIR> sru
3866 File(s) 1,727,891,022 bytes
116 Dir(s) 63,601,328,128 bytes free

C:\WINDOWS\system32>
  
```

- A. dir /o:d
- B. dir /o:s
- C. dir /o:e
- D. dir /o:n

Answer: A

NEW QUESTION 625

- (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 627

- (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 629

- (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 630

- (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 631

- (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 633

- (Exam Topic 3)

Which of the following is a federal law enacted in the US to control the ways that financial institutions deal with the private information of individuals?

- A. SOX
- B. HIPAA 1996
- C. GLBA
- D. PCI DSS

Answer: C

NEW QUESTION 634

- (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 636

- (Exam Topic 3)

Which of the following tools is not a data acquisition hardware tool?

- A. UltraKit
- B. Atola Insight Forensic
- C. F-Response Imager
- D. Triage-Responder

Answer: C

NEW QUESTION 641

- (Exam Topic 3)

Which of the following is NOT an anti-forensics technique?

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

Answer: A

NEW QUESTION 645

- (Exam Topic 3)

Korey, a data mining specialist in a knowledge processing firm DataHub.com, reported his CISO that he has lost certain sensitive data stored on his laptop. The CISO wants his forensics investigation team to find if the data loss was accident or intentional. In which of the following category this case will fall?

- A. Civil Investigation
- B. Administrative Investigation
- C. Both Civil and Criminal Investigations
- D. Criminal Investigation

Answer: B

NEW QUESTION 646

- (Exam Topic 3)

Which of the following is a responsibility of the first responder?

- A. Determine the severity of the incident
- B. Collect as much information about the incident as possible
- C. Share the collected information to determine the root cause
- D. Document the findings

Answer: B

NEW QUESTION 648

- (Exam Topic 3)

Lynne receives the following email:

Dear lynne@gmail.com! We are sorry to inform you that your ID has been temporarily frozen due to incorrect or missing information saved at 2016/11/10 20:40:24

You have 24 hours to fix this problem or risk to be closed permanently! To proceed Please Connect >> My Apple ID

Thank You The link to My Apple ID shows <http://byggarbetsplatsen.se/backup/signon/> What type of attack is this?

- A. Mail Bombing
- B. Phishing
- C. Email Spamming
- D. Email Spoofing

Answer: B

NEW QUESTION 649

- (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 652

- (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 657

- (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 661

- (Exam Topic 3)

Identify the file system that uses \$Bitmap file to keep track of all used and unused clusters on a volume.

- A. NTFS
- B. FAT
- C. EXT
- D. FAT32

Answer: A

NEW QUESTION 666

- (Exam Topic 3)

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

- A. Adjacent buffer locations
- B. Adjacent string locations
- C. Adjacent bit blocks
- D. Adjacent memory locations

Answer: D

NEW QUESTION 669

- (Exam Topic 3)
> NMAP -sn 192.168.11.200-215 The NMAP command above performs which of the following?

- A. A trace sweep
- B. A port scan
- C. A ping scan
- D. An operating system detect

Answer: C

NEW QUESTION 674

- (Exam Topic 3)
Examination of a computer by a technically unauthorized person will almost always result in:

- A. Rendering any evidence found inadmissible in a court of law
- B. Completely accurate results of the examination
- C. The chain of custody being fully maintained
- D. Rendering any evidence found admissible in a court of law

Answer: A

NEW QUESTION 678

- (Exam Topic 3)
Which of the following Windows-based tool displays who is logged onto a computer, either locally or remotely?

- A. Tokenmon
- B. PSLoggedon
- C. TCPView
- D. Process Monitor

Answer: B

NEW QUESTION 683

- (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 684

- (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 685

- (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 688

- (Exam Topic 3)
Select the tool appropriate for finding the dynamically linked lists of an application or malware.

- A. SysAnalyzer
- B. ResourcesExtract
- C. PEiD
- D. Dependency Walker

Answer: D

NEW QUESTION 691

- (Exam Topic 3)

Which of these rootkit detection techniques function by comparing a snapshot of the file system, boot records, or memory with a known and trusted baseline?

- A. Signature-Based Detection
- B. Integrity-Based Detection
- C. Cross View-Based Detection
- D. Heuristic/Behavior-Based Detection

Answer: B

NEW QUESTION 692

- (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 694

- (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 698

- (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 699

- (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 701

- (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 704

- (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 706

- (Exam Topic 2)

What does the part of the log, "% SEC-6-IPACCESSLOGP", extracted from a Cisco router represent?

- A. The system was not able to process the packet because there was not enough room for all of the desired IP header options
- B. Immediate action required messages
- C. Some packet-matching logs were missed because the access list log messages were rate limited, or no access list log buffers were available
- D. A packet matching the log criteria for the given access list has been detected (TCP or UDP)

Answer: D

NEW QUESTION 708

- (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 712

- (Exam Topic 2)

Jacob is a computer forensics investigator with over 10 years experience in investigations and has written over 50 articles on computer forensics. He has been called upon as a qualified witness to testify the accuracy and integrity of the technical log files gathered in an investigation into computer fraud. What is the term used for Jacob testimony in this case?

- A. Justification
- B. Authentication
- C. Reiteration
- D. Certification

Answer: B

NEW QUESTION 714

- (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 151EfCEh032241
    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@somewhereelse.com>
MIME-version: 1.0
```

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

Answer: C

NEW QUESTION 715

- (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 719

- (Exam Topic 2)

What type of analysis helps to identify the time and sequence of events in an investigation?

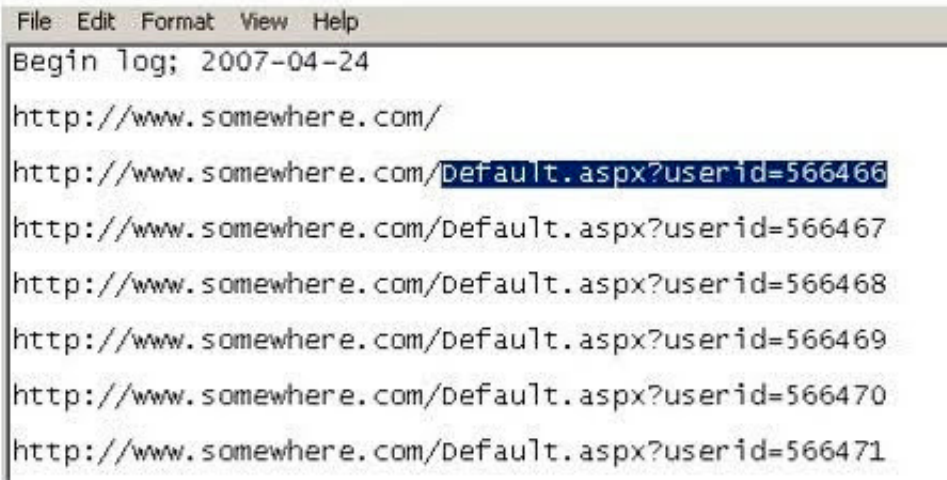
- A. Time-based
- B. Functional
- C. Relational
- D. Temporal

Answer: D

NEW QUESTION 721

- (Exam Topic 2)

Using Internet logging software to investigate a case of malicious use of computers, the investigator comes across some entries that appear odd.



```
File Edit Format View Help
Begin log; 2007-04-24
http://www.somewhere.com/
http://www.somewhere.com/default.aspx?userid=566466
http://www.somewhere.com/default.aspx?userid=566467
http://www.somewhere.com/default.aspx?userid=566468
http://www.somewhere.com/default.aspx?userid=566469
http://www.somewhere.com/default.aspx?userid=566470
http://www.somewhere.com/default.aspx?userid=566471
```

From the log, the investigator can see where the person in question went on the Internet. From the log, it appears that the user was manually typing in different user ID numbers. What technique this user was trying?

- A. Parameter tampering
- B. Cross site scripting
- C. SQL injection
- D. Cookie Poisoning

Answer: A

NEW QUESTION 726

- (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 731

- (Exam Topic 2)

Harold is a computer forensics investigator working for a consulting firm out of Atlanta Georgia. Harold is called upon to help with a corporate espionage case in Miami Florida. Harold assists in the investigation by pulling all the data from the computers allegedly used in the illegal activities. He finds that two suspects in the company were stealing sensitive corporate information and selling it to competing companies. From the email and instant messenger logs recovered, Harold has discovered that the two employees notified the buyers by writing symbols on the back of specific stop signs. This way, the buyers knew when and where to meet with the alleged suspects to buy the stolen material. What type of steganography did these two suspects use?

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

Answer: B

NEW QUESTION 732

- (Exam Topic 2)

Which of the following files stores information about a local Google Drive installation such as User email ID, Local Sync Root Path, and Client version installed?

- A. filecache.db
- B. config.db
- C. sigstore.db
- D. Sync_config.db

Answer: D

NEW QUESTION 736

- (Exam Topic 2)

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

- A. Xplico
- B. Colasoft's Capsa
- C. FileSalvage
- D. DriveSpy

Answer: C

NEW QUESTION 739

- (Exam Topic 2)

How will you categorize a cybercrime that took place within a CSP's cloud environment?

- A. Cloud as a Subject
- B. Cloud as a Tool
- C. Cloud as an Audit
- D. Cloud as an Object

Answer: D

NEW QUESTION 742

- (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 746

- (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 751

- (Exam Topic 2)

What will the following Linux command accomplish? `dd if=/dev/mem of=/home/sam/mem.bin bs=1024`

- A. Copy the master boot record to a file
- B. Copy the contents of the system folder to a file
- C. Copy the running memory to a file
- D. Copy the memory dump file to an image file

Answer: C

NEW QUESTION 752

- (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 755

- (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 758

- (Exam Topic 2)

- A. 202
- B. 404
- C. 606
- D. 999

Answer: B

NEW QUESTION 760

- (Exam Topic 2)

Which of the following is NOT a part of pre-investigation phase?

- A. Building forensics workstation
- B. Gathering information about the incident
- C. Gathering evidence data
- D. Creating an investigation team

Answer: C

NEW QUESTION 762

- (Exam Topic 2)

On an Active Directory network using NTLM authentication, where on the domain controllers are the passwords stored?

- A. SAM
- B. AMS

- C. Shadow file
- D. Password.conf

Answer: A

NEW QUESTION 763

- (Exam Topic 2)

What encryption technology is used on Blackberry devices Password Keeper?

- A. 3DES
- B. AES
- C. Blowfish
- D. RC5

Answer: B

NEW QUESTION 766

- (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 768

- (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 772

- (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 773

- (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 777

- (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 781

- (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 783

- (Exam Topic 2)

While searching through a computer under investigation, you discover numerous files that appear to have had the first letter of the file name replaced by the hex code byte 5h. What does this indicate on the computer?

- A. The files have been marked as hidden
- B. The files have been marked for deletion
- C. The files are corrupt and cannot be recovered
- D. The files have been marked as read-only

Answer: B

NEW QUESTION 786

- (Exam Topic 2)

Which of the following techniques can be used to beat steganography?

- A. Encryption
- B. Steganalysis
- C. Decryption
- D. Cryptanalysis

Answer: B

NEW QUESTION 790

- (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 794

- (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 796

- (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 797

- (Exam Topic 2)

What feature of Decryption Collection allows an investigator to crack a password as quickly as possible?

- A. Cracks every password in 10 minutes
- B. Distribute processing over 16 or fewer computers
- C. Support for Encrypted File System
- D. Support for MD5 hash verification

Answer: B

NEW QUESTION 801

- (Exam Topic 2)

Which of the following tool enables a user to reset his/her lost admin password in a Windows system?

- A. Advanced Office Password Recovery
- B. Active@ Password Changer
- C. Smartkey Password Recovery Bundle Standard
- D. Passware Kit Forensic

Answer: B

NEW QUESTION 802

- (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 804

- (Exam Topic 2)

Which of the following files gives information about the client sync sessions in Google Drive on Windows?

- A. sync_log.log
- B. Sync_log.log
- C. sync.log
- D. Sync.log

Answer: B

NEW QUESTION 809

- (Exam Topic 2)

Which among the following is an act passed by the U.S. Congress in 2002 to protect investors from the possibility of fraudulent accounting activities by corporations?

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

Answer: C

NEW QUESTION 812

- (Exam Topic 2)

Which file is a sequence of bytes organized into blocks understandable by the system's linker?

- A. executable file
- B. source file
- C. Object file
- D. None of these

Answer: C

NEW QUESTION 815

- (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 819

- (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

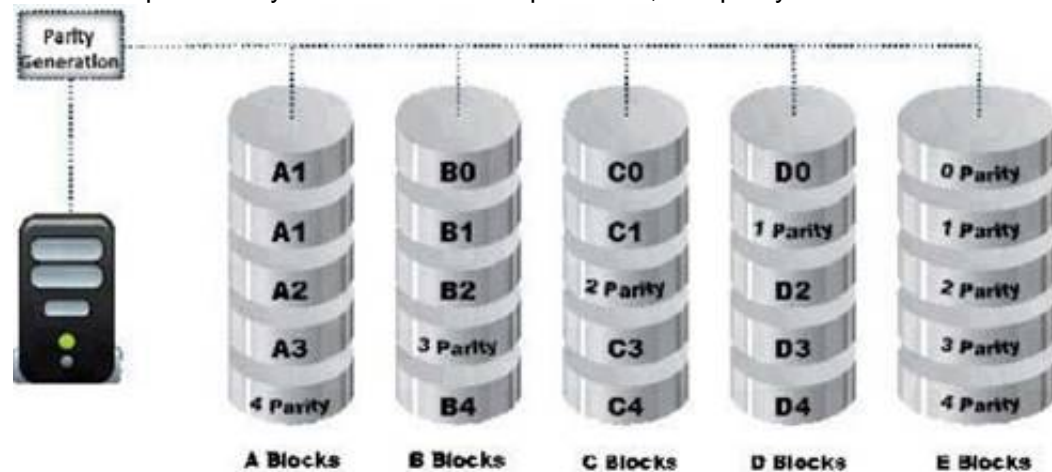
- B. Net config
- C. Net share
- D. Net use

Answer: D

NEW QUESTION 823

- (Exam Topic 2)

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



What RAID level is represented here?

- A. RAID Level 0
- B. RAID Level 5
- C. RAID Level 3
- D. RAID Level 1

Answer: B

NEW QUESTION 825

- (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 826

- (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 830

- (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 834

- (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 837

- (Exam Topic 2)

Why would a company issue a dongle with the software they sell?

- A. To provide source code protection
- B. To provide wireless functionality with the software
- C. To provide copyright protection
- D. To ensure that keyloggers cannot be used

Answer: C

NEW QUESTION 838

- (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 840

- (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 843

- (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 847

- (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 848

- (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 852

- (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 857

- (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 861

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

Answer: D

NEW QUESTION 865

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 312-49v10 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 312-49v10 Product From:

<https://www.2passeasy.com/dumps/312-49v10/>

Money Back Guarantee

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