

EC-Council

Exam Questions 312-49v10

Computer Hacking Forensic Investigator (CHFI-v10)



NEW QUESTION 1

- (Exam Topic 1)

You are the security analyst working for a private company out of France. Your current assignment is to obtain credit card information from a Swiss bank owned by that company. After initial reconnaissance, you discover that the bank security defenses are very strong and would take too long to penetrate. You decide to get the information by monitoring the traffic between the bank and one of its subsidiaries in London. After monitoring some of the traffic, you see a lot of FTP packets traveling back and forth. You want to sniff the traffic and extract usernames and passwords. What tool could you use to get this information?

- A. Airsnort
- B. Snort
- C. Ettercap
- D. RaidSniff

Answer: C

NEW QUESTION 2

- (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 3

- (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 4

- (Exam Topic 1)

What will the following URL produce in an unpatched IIS Web Server? `http://www.thetargetsite.com/scripts/..%co%af../..%co%af../windows/system32/cmd.exe?/c+dir+c:\`

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

Answer: A

NEW QUESTION 5

- (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 6

- (Exam Topic 1)

John is using Firewalk to test the security of his Cisco PIX firewall. He is also utilizing a sniffer located on a subnet that resides deep inside his network. After analyzing the sniffer log files, he does not see any of the traffic produced by Firewalk. Why is that?

- A. Firewalk cannot pass through Cisco firewalls
- B. Firewalk sets all packets with a TTL of zero
- C. Firewalk cannot be detected by network sniffers
- D. Firewalk sets all packets with a TTL of one

Answer: D

NEW QUESTION 7

- (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 8

- (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 9

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 10

- (Exam Topic 1)

The objective of this act was to protect consumers' personal financial information held by financial institutions and their service providers.

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

Answer: A

NEW QUESTION 10

- (Exam Topic 1)

Terri works for a security consulting firm that is currently performing a penetration test on First National Bank in Tokyo. Terri's duties include bypassing firewalls and switches to gain access to the network. Terri sends an IP packet to one of the company's switches with ACK bit and the source address of her machine set. What is Terri trying to accomplish by sending this IP packet?

- A. Trick the switch into thinking it already has a session with Terri's computer
- B. Poison the switch's MAC address table by flooding it with ACK bits
- C. Crash the switch with a DoS attack since switches cannot send ACK bits
- D. Enable tunneling feature on the switch

Answer: A

NEW QUESTION 13

- (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 15

- (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 17

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 19

- (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 23

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 27

- (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 29

- (Exam Topic 2)

Which of the following file contains the traces of the applications installed, run, or uninstalled from a system?

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

Answer: A

NEW QUESTION 32

- (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 37

- (Exam Topic 2)

Amber, a black hat hacker, has embedded a malware into a small enticing advertisement and posted it on a popular ad-network that displays across various websites. What is she doing?

- A. Click-jacking
- B. Compromising a legitimate site
- C. Spearphishing
- D. Malvertising

Answer: D

NEW QUESTION 38

- (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 39

- (Exam Topic 1)

From the following spam mail header, identify the host IP that sent this spam? From jie02@netvigator.com jie02@netvigator.com Tue Nov 27 17:27:11 2001
Received: from viruswall.ie.cuhk.edu.hk (viruswall [137.189.96.52]) by eng.ie.cuhk.edu.hk (8.11.6/8.11.6) with ESMTP id fAR9RAP23061 for ; Tue, 27 Nov 2001 17:27:10 +0800 (HKT)
Received: from mydomain.com (pcd249020.netvigator.com [203.218.39.20]) by viruswall.ie.cuhk.edu.hk (8.12.1/8.12.1) with SMTP id fAR9QXwZ018431 for ; Tue, 27 Nov 2001 17:26:36 +0800 (HKT)
Message-Id: >200111270926.fAR9QXwZ018431@viruswall.ie.cuhk.edu.hk From: "china hotel web"
To: "Shlam"
Subject: SHANGHAI (HILTON HOTEL) PACKAGE
Date: Tue, 27 Nov 2001 17:25:58 +0800 MIME-Version: 1.0
X- Priority: 3 X-MSMail- Priority: Normal
Reply-To: "china hotel web"

- A. 137.189.96.52
- B. 8.12.1.0
- C. 203.218.39.20
- D. 203.218.39.50

Answer: C

NEW QUESTION 41

- (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 44

- (Exam Topic 1)

Lance wants to place a honeypot on his network. Which of the following would be your recommendations?

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

Answer: D

NEW QUESTION 45

- (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 total has not been reviewed and accepted by your peers
- D. You are not certified for using the tool

Answer: C

NEW QUESTION 48

- (Exam Topic 1)

In a FAT32 system, a 123 KB file will use how many sectors?

- A. 34
- B. 25
- C. 11
- D. 56

Answer: B

NEW QUESTION 52

- (Exam Topic 1)

You are a security analyst performing reconnaissance on a company you will be carrying out a penetration test for. You conduct a search for IT jobs on Dice.com and find the following information for an open position: 7+ years experience in Windows Server environment 5+ years experience in Exchange 2000/2003 environment Experience with Cisco Pix Firewall, Linksys 1376 router, Oracle 11i and MYOB v3.4 Accounting software are required MCSA desired, MCSE, CEH preferred No Unix/Linux Experience needed What is this information posted on the job website considered?

- A. Social engineering exploit
- B. Competitive exploit
- C. Information vulnerability
- D. Trade secret

Answer: C

NEW QUESTION 56

- (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 59

- (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 63

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 67

- (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 68

- (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 70

- (Exam Topic 1)

What should you do when approached by a reporter about a case that you are working on or have worked on?

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

Answer: A

NEW QUESTION 74

- (Exam Topic 1)

Item 2If you come across a sheepdip machine at your client site, what would you infer?

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

Answer: C

NEW QUESTION 78

- (Exam Topic 1)

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 81

- (Exam Topic 1)

When examining a hard disk without a write-blocker, you should not start windows because Windows will write data to the:

- A. Recycle Bin
- B. MSDOS.sys
- C. BIOS
- D. Case files

Answer: A

NEW QUESTION 84

- (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 85

- (Exam Topic 1)

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

- A. forensic duplication of hard drive
- B. analysis of volatile data

- C. comparison of MD5 checksums
- D. review of SIDs in the Registry

Answer: C

NEW QUESTION 90

- (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_pwd[12509]: (login) session opened for user simple by (uid=0)
Apr 26 06:44:36 victim7 PAM_pwd[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 92

- (Exam Topic 1)

You should make at least how many bit-stream copies of a suspect drive?

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

Answer: B

NEW QUESTION 96

- (Exam Topic 1)

Jessica works as systems administrator for a large electronics firm. She wants to scan her network quickly to detect live hosts by using ICMP ECHO Requests. What type of scan is Jessica going to perform?

- A. Tracert
- B. Smurf scan
- C. Ping trace
- D. ICMP ping sweep

Answer: D

NEW QUESTION 99

- (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 103

- (Exam Topic 1)

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

- A. 10
- B. 25
- C. 110
- D. 135

Answer: B

NEW QUESTION 107

- (Exam Topic 1)

What does the acronym POST mean as it relates to a PC?

- A. Primary Operations Short Test
- B. PowerOn Self Test
- C. Pre Operational Situation Test
- D. Primary Operating System Test

Answer: B

NEW QUESTION 112

- (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 114

- (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 118

- (Exam Topic 1)

How many sectors will a 125 KB file use in a FAT32 file system?

- A. 32
- B. 16
- C. 256
- D. 25

Answer: C

NEW QUESTION 122

- (Exam Topic 1)

The rule of thumb when shutting down a system is to pull the power plug. However, it has certain drawbacks. Which of the following would that be?

- A. Any data not yet flushed to the system will be lost
- B. All running processes will be lost
- C. The /tmp directory will be flushed
- D. Power interruption will corrupt the pagefile

Answer: A

NEW QUESTION 124

- (Exam Topic 1)

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

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

Answer: D

NEW QUESTION 128

- (Exam Topic 1)

Kimberly is studying to be an IT security analyst at a vocational school in her town. The school offers many different programming as well as networking

languages. What networking protocol language should she learn that routers utilize?

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

Answer: D

NEW QUESTION 130

- (Exam Topic 1)

You have compromised a lower-level administrator account on an Active Directory network of a small company in Dallas, Texas. You discover Domain Controllers through enumeration. You connect to one of the Domain Controllers on port 389 using ldp.exe. What are you trying to accomplish here?

- A. Poison the DNS records with false records
- B. Enumerate MX and A records from DNS
- C. Establish a remote connection to the Domain Controller
- D. Enumerate domain user accounts and built-in groups

Answer: D

NEW QUESTION 134

- (Exam Topic 1)

The offset in a hexadecimal code is:

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

Answer: B

NEW QUESTION 138

- (Exam Topic 1)

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

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

Answer: D

NEW QUESTION 141

- (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 145

- (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 146

- (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 151

- (Exam Topic 1)

What file structure database would you expect to find on floppy disks?

- A. NTFS
- B. FAT32
- C. FAT16
- D. FAT12

Answer: D

NEW QUESTION 154

- (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 156

- (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 161

- (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 165

- (Exam Topic 1)

When examining the log files from a Windows IIS Web Server, how often is a new log file created?

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

Answer: A

NEW QUESTION 168

- (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 172

- (Exam Topic 1)

A law enforcement officer may only search for and seize criminal evidence with , which are facts or circumstances that would lead a reasonable person to believe a crime has been committed or is about to be committed, evidence of the specific crime exists and the evidence of the specific crime exists at the place to be searched.

- A. Mere Suspicion
- B. A preponderance of the evidence
- C. Probable cause
- D. Beyond a reasonable doubt

Answer: C

NEW QUESTION 173

- (Exam Topic 1)

You are working as an investigator for a corporation and you have just received instructions from your manager to assist in the collection of 15 hard drives that are part of an ongoing investigation.

Your job is to complete the required evidence custody forms to properly document each piece of evidence as it is collected by other members of your team. Your manager instructs you to complete one multi-evidence form for the entire case and a single-evidence form for each hard drive. How will these forms be stored to help preserve the chain of custody of the case?

- A. All forms should be placed in an approved secure container because they are now primary evidence in the case.
- B. The multi-evidence form should be placed in the report file and the single-evidence forms should be kept with each hard drive in an approved secure container.
- C. The multi-evidence form should be placed in an approved secure container with the hard drives and the single-evidence forms should be placed in the report file.
- D. All forms should be placed in the report file because they are now primary evidence in the case.

Answer: B

NEW QUESTION 177

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 182

- (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 185

- (Exam Topic 1)

Which of the following should a computer forensics lab used for investigations have?

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

Answer: B

NEW QUESTION 186

- (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 187

- (Exam Topic 1)

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

- A. bench warrant
- B. wire tap
- C. subpoena
- D. search warrant

Answer: D

NEW QUESTION 190

- (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 191

- (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 195

- (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 197

- (Exam Topic 1)

John and Hillary works at the same department in the company. John wants to find out Hillary's network password so he can take a look at her documents on the file server. He enables Lophcrack program to sniffing mode. John sends Hillary an email with a link to Error! Reference source not found. What information will he be able to gather from this?

- A. Hillary network username and password hash
- B. The SID of Hillary network account
- C. The SAM file from Hillary computer
- D. The network shares that Hillary has permissions

Answer: A

NEW QUESTION 200

- (Exam Topic 1)

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

- A. a write-blocker
- B. a protocol analyzer
- C. a firewall
- D. a disk editor

Answer: A

NEW QUESTION 203

- (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 208

- (Exam Topic 1)

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

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

Answer: D

NEW QUESTION 210

- (Exam Topic 1)

What will the following command produce on a website login page? SELECT email, passwd, login_id, full_name FROM members WHERE email = 'someone@somehwere.com'; DROP TABLE members; --'

- A. Deletes the entire members table
- B. Inserts the Error! Reference source not found.email address into the members table
- C. Retrieves the password for the first user in the members table
- D. This command will not produce anything since the syntax is incorrect

Answer: A

NEW QUESTION 214

- (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 215

- (Exam Topic 1)

Bob has been trying to penetrate a remote production system for the past two weeks. This time however, he is able to get into the system. He was able to use the System for a period of three weeks. However, law enforcement agencies were recoding his every activity and this was later presented as evidence. The organization had used a Virtual Environment to trap Bob. What is a Virtual Environment?

- A. A Honeypot that traps hackers
- B. A system Using Trojaned commands
- C. An environment set up after the user logs in
- D. An environment set up before a user logs in

Answer: A

NEW QUESTION 220

- (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 222

- (Exam Topic 1)

Office documents (Word, Excel, PowerPoint) contain a code that allows tracking the MAC, or unique identifier, of the machine that created the document. What is that code called?

- A. the Microsoft Virtual Machine Identifier
- B. the Personal Application Protocol
- C. the Globally Unique ID
- D. the Individual ASCII String

Answer: C

NEW QUESTION 223

- (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 225

- (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 229

- (Exam Topic 1)

You are carrying out the last round of testing for your new website before it goes live. The website has many dynamic pages and connects to a SQL backend that accesses your product inventory in a database. You come across a web security site that recommends inputting the following code into a search field on web pages to check for vulnerabilities: When you type this and click on search, you receive a pop-up window that says: "This is a test."

What is the result of this test?

- A. Your website is vulnerable to CSS
- B. Your website is not vulnerable
- C. Your website is vulnerable to SQL injection
- D. Your website is vulnerable to web bugs

Answer: A

NEW QUESTION 231

- (Exam Topic 1)

Sectors in hard disks typically contain how many bytes?

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

Answer: B

NEW QUESTION 233

- (Exam Topic 1)

One technique for hiding information is to change the file extension from the correct one to one that might not be noticed by an investigator. For example, changing a .jpg extension to a .doc extension so that a picture file appears to be a document. What can an investigator examine to verify that a file has the correct extension?

- A. the File Allocation Table
- B. the file header
- C. the file footer
- D. the sector map

Answer: B

NEW QUESTION 237

- (Exam Topic 1)

Before you are called to testify as an expert, what must an attorney do first?

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

Answer: D

NEW QUESTION 238

- (Exam Topic 1)

As a CHF1 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 fee that you charge
- D. The friendship of local law enforcement officers

Answer: B

NEW QUESTION 239

- (Exam Topic 1)

What header field in the TCP/IP protocol stack involves the hacker exploit known as the Ping of Death?

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

Answer: B

NEW QUESTION 241

- (Exam Topic 1)

Kyle is performing the final testing of an application he developed for the accounting department. His last round of testing is to ensure that the program is as secure as possible. Kyle runs the following command. What is he testing at this point?

```
#include <stdio.h>
#include <string.h>
int main(int argc, char
*argv[]) { char buffer[10]; if (argc < 2) { printf (stderr, "USAGE: %s string\n", argv[0]); return 1; } strcpy(buffer, argv[1]); return 0; }
```

- A. Buffer overflow
- B. SQL injection
- C. Format string bug
- D. Kernel injection

Answer: A

NEW QUESTION 245

- (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 250

- (Exam Topic 4)

What command-line tool enables forensic Investigator to establish communication between an Android device and a forensic workstation in order to perform data acquisition from the device?

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

Answer: C

NEW QUESTION 254

- (Exam Topic 4)

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

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

Answer: C

NEW QUESTION 259

- (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 264

- (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 269

- (Exam Topic 4)

According to RFC 3227, which of the following is considered as the most volatile item on a typical system?

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

Answer: A

NEW QUESTION 271

- (Exam Topic 4)

To which phase of the computer forensics investigation process does "planning and budgeting of a forensics lab" belong?

- A. Post-investigation phase
- B. Reporting phase
- C. Pre-investigation phase
- D. Investigation phase

Answer: C

NEW QUESTION 272

- (Exam Topic 4)

During an investigation, Noel found a SIM card from the suspect's mobile. The ICCID on the card is 8944245252001451548. What does the first four digits (89 and 44) in the ICCID represent?

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

Answer: C

NEW QUESTION 274

- (Exam Topic 4)

Which of the following tools will allow a forensic investigator to acquire the memory dump of a suspect machine so that it may be investigated on a forensic workstation to collect evidentiary data like processes and Tor browser artifacts?

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

Answer: C

NEW QUESTION 277

- (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 282

- (Exam Topic 4)

An investigator seized a notebook device installed with a Microsoft Windows OS. Which type of files would support an investigation of the data size and structure in the device?

- A. Ext2 and Ext4
- B. APFS and HFS

- C. HFS and GNUC
- D. NTFSandFAT

Answer: D

NEW QUESTION 285

- (Exam Topic 4)

Which of the following statements is true with respect to SSDs (solid-state drives)?

- A. Like HDD
- B. SSDs also have moving parts
- C. SSDs cannot store non-volatile data
- D. SSDs contain tracks, clusters, and sectors to store data
- E. Faster data access, lower power usage, and higher reliability are some of the major advantages of SSDs over HDDs

Answer: D

NEW QUESTION 287

- (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 291

- (Exam Topic 4)

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

- A. Ibdatab1
- B. Application data files (ADF)
- C. Transaction log data files (LDF)
- D. Primary data files (MDF)

Answer: C

NEW QUESTION 296

- (Exam Topic 4)

On NTFS file system, which of the following tools can a forensic investigator use in order to identify timestomping of evidence files?

- A. wbStego
- B. Exiv2
- C. analyzeMFT
- D. Timestomp

Answer: D

NEW QUESTION 300

- (Exam Topic 4)

Web browsers can store relevant information from user activities. Forensic investigators may retrieve files, lists, access history, cookies, among other digital footprints. Which tool can contribute to this task?

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

Answer: B

NEW QUESTION 303

- (Exam Topic 4)

Simona has written a regular expression for the detection of web application-specific attack attempt that reads as `/((\%3C)|<K(\%2F)|V)*[a-zA-Z0-9!*(\%3E)]>/lx`. Which of the following does the part `(\%3E)]>` look for?

- A. Alphanumeric string or its hex equivalent
- B. Opening angle bracket or its hex equivalent
- C. Closing angle bracket or its hex equivalent
- D. Forward slash for a closing tag or its hex equivalent

Answer: D

NEW QUESTION 305

- (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 309

- (Exam Topic 4)

An investigator needs to perform data acquisition from a storage media without altering its contents to maintain the Integrity of the content. The approach adopted by the Investigator relies upon the capacity of enabling read-only access to the storage media. Which tool should the Investigator Integrate Into his/her procedures to accomplish this task?

- A. BitLocker
- B. Data duplication tool
- C. Backup tool
- D. Write blocker

Answer: D

NEW QUESTION 313

- (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 317

- (Exam Topic 4)

Rule 1002 of Federal Rules of Evidence (US) talks about

- A. Admissibility of original
- B. Admissibility of duplicates
- C. Requirement of original
- D. Admissibility of other evidence of contents

Answer: C

NEW QUESTION 321

- (Exam Topic 4)

A file requires 10 KB space to be saved on a hard disk partition. An entire cluster of 32 KB has been allocated for this file. The remaining, unused space of 22 KB on this cluster will be identified as .

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

Answer: D

NEW QUESTION 325

- (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 326

- (Exam Topic 4)

A call detail record (CDR) provides metadata about calls made over a phone service. From the following data fields, which one is not contained in a CDR.

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

Answer: C

NEW QUESTION 330

- (Exam Topic 4)

Maria has executed a suspicious executable file in a controlled environment and wants to see if the file adds/modifies any registry value after execution via Windows Event Viewer. Which of the following event ID should she look for in this scenario?

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

Answer: A

NEW QUESTION 335

- (Exam Topic 4)

Derrick, a forensic specialist, was investigating an active computer that was executing various processes. Derrick wanted to check whether this system was used in an incident that occurred earlier. He started inspecting and gathering the contents of RAM, cache, and DLLs to identify incident signatures. Identify the data acquisition method employed by Derrick in the above scenario.

- A. Dead data acquisition
- B. Static data acquisition
- C. Non-volatile data acquisition
- D. Live data acquisition

Answer: C

NEW QUESTION 337

- (Exam Topic 4)

Cybercriminals sometimes use compromised computers to commit other crimes, which may involve using computers or networks to spread malware or illegal information. Which type of cybercrime stops users from using a device or network, or prevents a company from providing a software service to its customers?

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

Answer: C

NEW QUESTION 340

- (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 341

- (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 345

- (Exam Topic 4)

Which of the following directories 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 350

- (Exam Topic 4)

Fill In the missing Master Boot Record component.

- * 1. Master boot code
- * 2. Partition table
- * 3. _____

- A. Boot loader
- B. Signature word
- C. Volume boot record
- D. Disk signature

Answer: A

NEW QUESTION 351

- (Exam Topic 4)

Assume there is a file named myfile.txt in C: drive that contains hidden data streams. Which of the following commands would you issue to display the contents of a data stream?

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

Answer: A

NEW QUESTION 356

- (Exam Topic 4)

Brian has the job of analyzing malware for a software security company. Brian has setup a virtual environment that includes virtual machines running various versions of OSes. Additionally, Brian has setup separated virtual networks within this environment. The virtual environment does not connect to the company's intranet nor does it connect to the external Internet. With everything setup, Brian now received an executable file from a client that has undergone a cyberattack. Brian ran the executable file in the virtual environment to see what it would do. What type of analysis did Brian perform?

- A. Static malware analysis
- B. Status malware analysis
- C. Dynamic malware analysis
- D. Static OS analysis

Answer: C

NEW QUESTION 358

- (Exam Topic 4)

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

- A. Drive:\\$Recycle.Bin\
- B. local/sha re/Trash
- C. Drive:\RECYCLER\
- D. DriveARECYCLED

Answer: C

NEW QUESTION 359

- (Exam Topic 4)

"To ensure that the digital evidence is collected, preserved, examined, or transferred in a manner safeguarding the accuracy and reliability of the evidence, law enforcement, and forensics organizations must establish and maintain an effective quality system" is a principle established by:

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

Answer: B

NEW QUESTION 361

- (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 365

- (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 369

- (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 373

- (Exam Topic 4)

During an Investigation, the first responders stored mobile devices In specific containers to provide network Isolation. All the following are examples of such pieces of equipment, except for:

- A. Wireless StrongHold bag
- B. VirtualBox
- C. Faraday bag
- D. RF shield box

Answer: D

NEW QUESTION 377

- (Exam Topic 4)

Which layer in the IoT architecture is comprised of hardware parts such as sensors, RFID tags, and devices that play an important role in data collection?

- A. Middleware layer
- B. Edge technology layer
- C. Application layer
- D. Access gateway layer

Answer: B

NEW QUESTION 381

- (Exam Topic 4)

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

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

Answer: D

NEW QUESTION 383

- (Exam Topic 4)

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

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

Answer: C

NEW QUESTION 384

- (Exam Topic 4)

A breach resulted from a malware attack that evaded detection and compromised the machine memory without installing any software or accessing the hard drive. What technique did the adversaries use to deliver the attack?

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

Answer: A

NEW QUESTION 387

- (Exam Topic 4)

When installed on a Windows machine, which port does the Tor browser use to establish a network connection via Tor nodes?

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

Answer: C

NEW QUESTION 392

- (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 396

- (Exam Topic 4)

Edgar is part of the FBI's forensic media and malware analysis team; he is analyzing a current malware and is conducting a thorough examination of the suspect system, network, and other connected devices. Edgar's approach is to execute the malware code to know how it interacts with the host system and its impacts on it. He is also using a virtual machine and a sandbox environment.

What type of malware analysis is Edgar performing?

- A. Malware disassembly
- B. VirusTotal analysis
- C. Static analysis
- D. Dynamic malware analysis/behavioral analysis

Answer: D

NEW QUESTION 400

- (Exam Topic 4)

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

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

Answer: C

NEW QUESTION 403

- (Exam Topic 4)

Identify the location of Recycle Bin on a Windows 7 machine that uses NTFS file system to store and retrieve files on the hard disk.

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

Answer: A

NEW QUESTION 406

- (Exam Topic 4)

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

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

Answer: A

NEW QUESTION 410

- (Exam Topic 4)

allows a forensic investigator to identify the missing links during investigation.

- A. Evidence preservation
- B. Chain of custody
- C. Evidence reconstruction
- D. Exhibit numbering

Answer: C

NEW QUESTION 412

- (Exam Topic 4)

In which IoT attack does the attacker use multiple forged identities to create a strong illusion of traffic congestion, affecting communication between neighboring nodes and networks?

- A. Replay attack
- B. Jamming attack
- C. Blueborne attack
- D. Sybil attack

Answer: D

NEW QUESTION 413

- (Exam Topic 4)

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

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

Answer: A

NEW QUESTION 417

- (Exam Topic 4)

In forensics, are used to view stored or deleted data from both files and disk sectors.

- A. Hash algorithms
- B. SIEM tools
- C. Host interfaces
- D. Hex editors

Answer: D

NEW QUESTION 418

- (Exam Topic 4)

Choose the layer in iOS architecture that provides frameworks for iOS app development?

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

Answer: C

NEW QUESTION 419

- (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 420

- (Exam Topic 3)

In a computer that has Dropbox client installed, which of the following files related to the Dropbox client store information about local Dropbox installation and the Dropbox user account, along with email IDs linked with the account?

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

Answer: A

NEW QUESTION 423

- (Exam Topic 3)

Which of the following standard represents a legal precedent regarding the admissibility of scientific examinations or experiments in legal cases?

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

Answer: C

NEW QUESTION 428

- (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 431

- (Exam Topic 3)

Smith, an employee of a reputed forensic investigation firm, has been hired by a private organization to investigate a laptop that is suspected to be involved in the hacking of the organization's DC server. Smith wants to find all the values typed into the Run box in the Start menu. Which of the following registry keys will Smith check to find the above information?

- A. TypedURLs key
- B. MountedDevices key
- C. UserAssist Key
- D. RunMRU key

Answer: D

NEW QUESTION 436

- (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 438

- (Exam Topic 3)

Which cloud model allows an investigator to acquire the instance of a virtual machine and initiate the forensics examination process?

- A. PaaS model
- B. IaaS model
- C. SaaS model
- D. SecaaS model

Answer: B

NEW QUESTION 441

- (Exam Topic 3)

Which of the following file system uses Master File Table (MFT) database to store information about every file and directory on a volume?

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

Answer: D

NEW QUESTION 442

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 444

- (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 448

- (Exam Topic 3)

An investigator has found certain details after analysis of a mobile device. What can reveal the manufacturer information?

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

Answer: B

NEW QUESTION 453

- (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 454

- (Exam Topic 3)

BMP (Bitmap) is a standard file format for computers running the Windows operating system. BMP images can range from black and white (1 bit per pixel) up to 24 bit color (16.7 million colors). Each bitmap file contains a header, the RGBQUAD array, information header, and image data. Which of the following element specifies the dimensions, compression type, and color format for the bitmap?

- A. Information header
- B. Image data
- C. The RGBQUAD array
- D. Header

Answer: A

NEW QUESTION 459

- (Exam Topic 3)

Hard disk data addressing is a method of allotting addresses to each of data on a hard disk.

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

Answer: A

NEW QUESTION 462

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 464

- (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 469

- (Exam Topic 3)

In which implementation of RAID will the image of a Hardware RAID volume be different from the image taken separately from the disks?

- A. RAID 1
- B. The images will always be identical because data is mirrored for redundancy
- C. RAID 0
- D. It will always be different

Answer: D

NEW QUESTION 473

- (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 475

- (Exam Topic 3)

Amber, a black hat hacker, has embedded malware into a small enticing advertisement and posted it on a popular ad-network that displays across various websites. What is she doing?

- A. Malvertising
- B. Compromising a legitimate site
- C. Click-jacking
- D. Spearphishing

Answer: A

NEW QUESTION 478

- (Exam Topic 3)

Which among the following U.S. laws requires financial institutions—companies that offer consumers financial products or services such as loans, financial or investment advice, or insurance—to protect their customers' information against security threats?

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

Answer: C

NEW QUESTION 482

- (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 484

- (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 485

- (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 489

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 491

- (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 493

- (Exam Topic 3)

Where should the investigator look for the Edge browser's browsing records, including history, cache, and cookies?

- A. ESE Database
- B. Virtual Memory
- C. Sparse files
- D. Slack Space

Answer: A

NEW QUESTION 495

- (Exam Topic 3)

Which type of attack is possible when attackers know some credible information about the victim's password, such as the password length, algorithms involved, or the strings and characters used in its creation?

- A. Rule-Based Attack
- B. Brute-Forcing Attack
- C. Dictionary Attack
- D. Hybrid Password Guessing Attack

Answer: A

NEW QUESTION 497

- (Exam Topic 3)

Which of the following network attacks refers to sending huge volumes of email to an address in an attempt to overflow the mailbox or overwhelm the server where the email address is hosted so as to cause a denial-of-service attack?

- A. Email spamming
- B. Phishing
- C. Email spoofing

D. Mail bombing

Answer: D

NEW QUESTION 500

- (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 503

- (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.

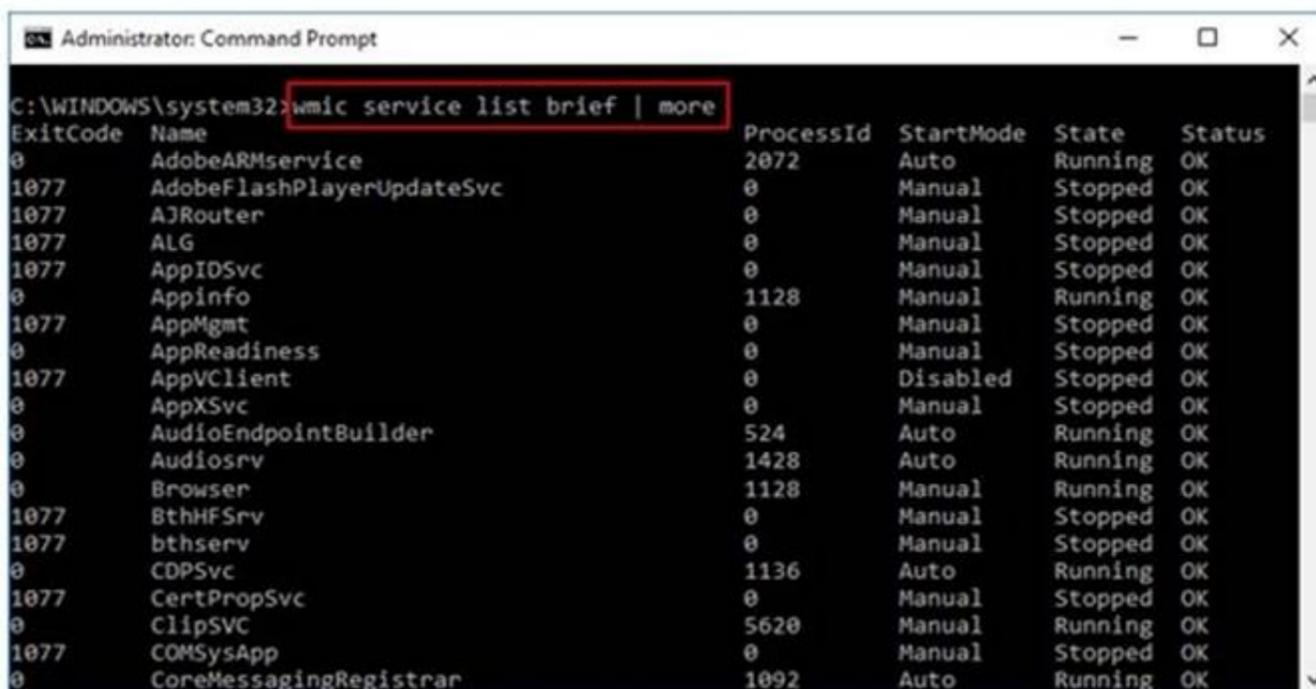
- A. Source code review
- B. Reviewing the firewalls configuration
- C. Data items and vulnerability scanning
- D. Interviewing employees and network engineers

Answer: A

NEW QUESTION 507

- (Exam Topic 3)

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



- A. List of services stopped
- B. List of services closed recently
- C. List of services recently started
- D. List of services installed

Answer: D

NEW QUESTION 509

- (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 512

- (Exam Topic 3)

In which registry does the system store the Microsoft security IDs?

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

Answer: D

NEW QUESTION 514

- (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 515

- (Exam Topic 3)

You are asked to build a forensic lab and your manager has specifically informed you to use copper for lining the walls, ceilings, and floor. What is the main purpose of lining the walls, ceilings, and floor with copper?

- A. To control the room temperature
- B. To strengthen the walls, ceilings, and floor
- C. To avoid electromagnetic emanations
- D. To make the lab sound proof

Answer: D

NEW QUESTION 519

- (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 521

- (Exam Topic 3)

A Linux system is undergoing investigation. In which directory should the investigators look for its current state data if the system is in powered on state?

- A. /auth
- B. /proc
- C. /var/log/debug
- D. /var/spool/cron/

Answer: B

NEW QUESTION 525

- (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 530

- (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. `ls of -m`

Answer: B

NEW QUESTION 531

- (Exam Topic 3)

Which of the following ISO standard defines file systems and protocol for exchanging data between optical disks?

- A. ISO 9660
- B. ISO/IEC 13940
- C. ISO 9060
- D. IEC 3490

Answer: A

NEW QUESTION 536

- (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 538

- (Exam Topic 3)

POP3 is an Internet protocol, which is used to retrieve emails from a mail server. Through which port does an email client connect with a POP3 server?

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

Answer: A

NEW QUESTION 543

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 548

- (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 552

- (Exam Topic 3)

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

- A. A virtual system with internet connection
- B. A normal system without internet connect
- C. A normal system with internet connection

D. A virtual system with network simulation for internet connection

Answer: D

NEW QUESTION 556

- (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 561

- (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 563

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 568

- (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 569

- (Exam Topic 3)

Which command line tool is used to determine active network connections?

- A. netsh
- B. nbstat
- C. nslookup
- D. netstat

Answer: D

NEW QUESTION 574

- (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 579

- (Exam Topic 3)

One technique for hiding information is to change the file extension from the correct one to the one that might not be noticed by an investigator. For example,

changing a .jpg extension to a .doc extension so that a picture file appears to be a document. What can an investigator examine to verify that a file has the correct extension?

- A. The file header
- B. The File Allocation Table
- C. The file footer
- D. The sector map

Answer: A

NEW QUESTION 580

- (Exam Topic 3)

Which of the following statements is true regarding SMTP Server?

- A. SMTP Server breaks the recipient's address into Recipient's name and his/her designation before passing it to the DNS Server
- B. SMTP Server breaks the recipient's address into Recipient's name and recipient's address before passing it to the DNS Server
- C. SMTP Server breaks the recipient's address into Recipient's name and domain name before passing it to the DNS Server
- D. SMTP Server breaks the recipient's address into Recipient's name and his/her initial before passing it to the DNS Server

Answer: C

NEW QUESTION 581

- (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 586

- (Exam Topic 3)

James is dealing with a case regarding a cybercrime that has taken place in Arizona, USA. James needs to lawfully seize the evidence from an electronic device without affecting the user's anonymity. Which of the following law should he comply with, before retrieving the evidence?

- A. First Amendment of the U.
- B. Constitution
- C. Fourth Amendment of the U.
- D. Constitution
- E. Third Amendment of the U.
- F. Constitution
- G. Fifth Amendment of the U.
- H. Constitution

Answer: D

NEW QUESTION 590

- (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 591

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 596

- (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 598

- (Exam Topic 3)

What is the capacity of Recycle bin in a system running on Windows Vista?

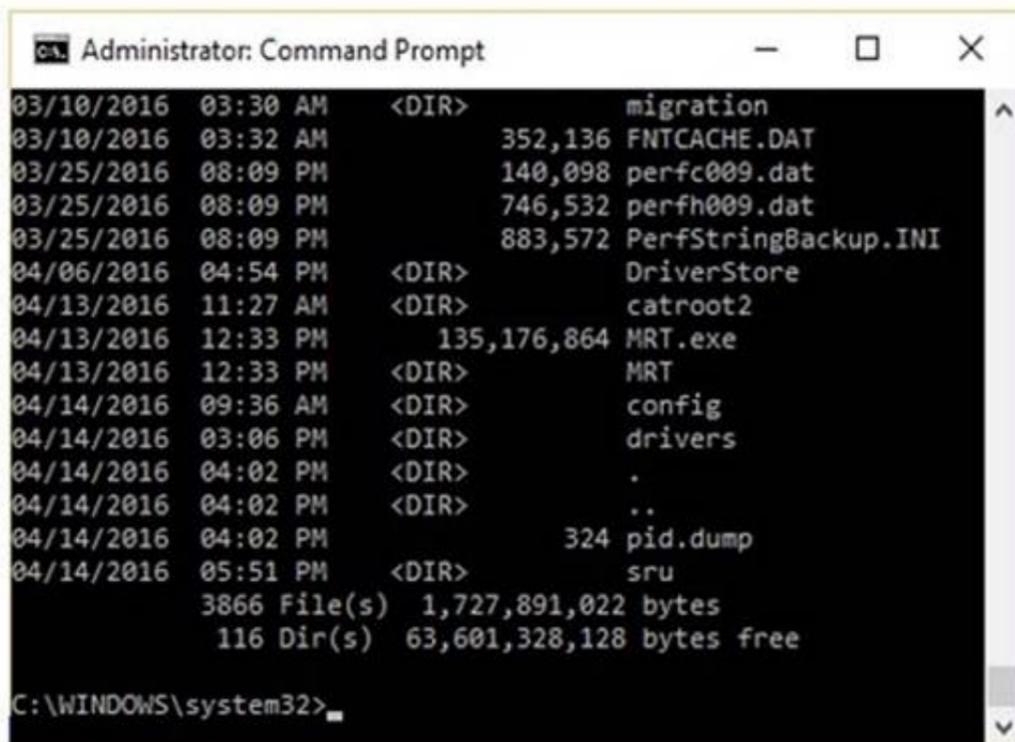
- A. 2.99GB
- B. 3.99GB
- C. Unlimited
- D. 10% of the partition space

Answer: C

NEW QUESTION 601

- (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?



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

Answer: A

NEW QUESTION 606

- (Exam Topic 3)

Which of the following does Microsoft Exchange E-mail Server use for collaboration of various e-mail applications?

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

Answer: B

NEW QUESTION 611

- (Exam Topic 3)

CAN-SPAM act requires that you:

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

D. Don't use true header information

Answer: A

NEW QUESTION 616

- (Exam Topic 3)

The MAC attributes are timestamps that refer to a time at which the file was last modified or last accessed or originally created. Which of the following file systems store MAC attributes in Coordinated Universal Time (UTC) format?

- A. File Allocation Table (FAT)
- B. New Technology File System (NTFS)
- C. Hierarchical File System (HFS)
- D. Global File System (GFS)

Answer: B

NEW QUESTION 621

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 624

- (Exam Topic 3)

Which of the following attack uses HTML tags like <script></script>?

- A. Phishing
- B. XSS attack
- C. SQL injection
- D. Spam

Answer: B

NEW QUESTION 628

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 631

- (Exam Topic 3)

What does the Rule 101 of Federal Rules of Evidence states?

- A. Scope of the Rules, where they can be applied
- B. Purpose of the Rules
- C. Limited Admissibility of the Evidence
- D. Rulings on Evidence

Answer: A

NEW QUESTION 632

- (Exam Topic 3)

Which component in the hard disk moves over the platter to read and write information?

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

Answer: D

NEW QUESTION 635

- (Exam Topic 3)

What does Locard's Exchange Principle state?

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

Answer: C

NEW QUESTION 636

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 640

- (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 642

- (Exam Topic 3)

Which of the following stand true for BIOS Parameter Block?

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

Answer: A

NEW QUESTION 647

- (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 650

- (Exam Topic 3)

While analyzing a hard disk, the investigator finds that the file system does not use UEFI-based interface. Which of the following operating systems is present on the hard disk?

- A. Windows 10
- B. Windows 8
- C. Windows 7
- D. Windows 8.1

Answer: C

NEW QUESTION 651

- (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 655

- (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 660

- (Exam Topic 3)

Which of the following techniques delete the files permanently?

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

Answer: B

NEW QUESTION 663

- (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 665

- (Exam Topic 3)

Which of the following is a part of a Solid-State Drive (SSD)?

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

Answer: C

NEW QUESTION 668

- (Exam Topic 3)

In both pharming and phishing attacks an attacker can create websites that look similar to legitimate sites with the intent of collecting personal identifiable information from its victims. What is the difference between pharming and phishing attacks?

- A. Both pharming and phishing attacks are purely technical and are not considered forms of social engineering
- B. In a pharming attack a victim is redirected to a fake website by modifying their host configuration file or by exploiting vulnerabilities in DN
- C. In a phishing attack an attacker provides the victim with a URL that is either misspelled or looks similar to the actual websites domain name
- D. In a phishing attack a victim is redirected to a fake website by modifying their host configuration file or by exploiting vulnerabilities in DN
- E. In a pharming attack an attacker provides the victim with a URL that is either misspelled or looks very similar to the actual websites domain name
- F. Both pharming and phishing attacks are identical

Answer: B

NEW QUESTION 669

- (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 672

- (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)

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 679

- (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 683

- (Exam Topic 3)

Identify the term that refers to individuals who, by virtue of their knowledge and expertise, express an independent opinion on a matter related to a case based on the information that is provided.

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

Answer: A

NEW QUESTION 684

- (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 686

- (Exam Topic 3)

Which of the following is NOT a physical evidence?

- A. Removable media
- B. Cables
- C. Image file on a hard disk
- D. Publications

Answer: C

NEW QUESTION 690

- (Exam Topic 3)

Which of the following file formats allows the user to compress the acquired data as well as keep it randomly accessible?

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

Answer: B

NEW QUESTION 693

- (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 696

- (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 699

- (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 702

- (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 705

- (Exam Topic 2)

Where is the startup configuration located on a router?

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

Answer: C

NEW QUESTION 707

- (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 711

- (Exam Topic 2)

Depending upon the jurisdictional areas, different laws apply to different incidents. Which of the following law is related to fraud and related activity in connection with computers?

- A. 18 USC §1029
- B. 18 USC §1030
- C. 18 USC §1361

D. 18 USC §1371

Answer: B

NEW QUESTION 716

- (Exam Topic 2)

Stephen is checking an image using Compare Files by The Wizard, and he sees the file signature is shown as FF D8 FF E1. What is the file type of the image?

- A. gif
- B. bmp
- C. jpeg
- D. png

Answer: C

NEW QUESTION 719

- (Exam Topic 2)

Netstat is a tool for collecting information regarding network connections. It provides a simple view of TCP and UDP connections, and their state and network traffic statistics. Which of the following commands shows you the TCP and UDP network connections, listening ports, and the identifiers?

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

Answer: B

NEW QUESTION 724

- (Exam Topic 2)

Adam, a forensic investigator, is investigating an attack on Microsoft Exchange Server of a large organization. As the first step of the investigation, he examined the PRIV.EDB file and found the source from where the mail originated and the name of the file that disappeared upon execution. Now, he wants to examine the MIME stream content. Which of the following files is he going to examine?

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

Answer: A

NEW QUESTION 728

- (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 731

- (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 736

- (Exam Topic 2)

Which program is the bootloader when Windows XP starts up?

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

Answer: B

NEW QUESTION 741

- (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 742

- (Exam Topic 2)

In a virtual test environment, Michael is testing the strength and security of BGP using multiple routers to mimic the backbone of the Internet. This project will help him write his doctoral thesis on "bringing down the Internet". Without sniffing the traffic between the routers, Michael sends millions of RESET packets to the routers in an attempt to shut one or all of them down. After a few hours, one of the routers finally shuts itself down. What will the other routers communicate between themselves?

- A. The change in the routing fabric to bypass the affected router
- B. More RESET packets to the affected router to get it to power back up
- C. RESTART packets to the affected router to get it to power back up
- D. STOP packets to all other routers warning of where the attack originated

Answer: A

NEW QUESTION 745

- (Exam Topic 2)

NTFS has reduced slack space than FAT, thus having lesser potential to hide data in the slack space. This is because:

- A. FAT does not index files
- B. NTFS is a journaling file system
- C. NTFS has lower cluster size space
- D. FAT is an older and inefficient file system

Answer: C

NEW QUESTION 746

- (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 747

- (Exam Topic 2)

A computer forensics investigator is inspecting the firewall logs for a large financial institution that has employees working 24 hours a day, 7 days a week.

```

2007-06-14 23:59:05 192.168.254.1 action=Permit sent=16169 rcvd=180962 src=24.119.129.125 dst=10.120.10.122 src_port=38
2007-06-14 23:59:06 192.168.254.1 action=Deny sent=0 rcvd=12288 src=10.130.9.2 dst=224.0.0.2 src_port=49415 dst_port=49
2007-06-14 23:59:07 192.168.254.1 action=Permit sent=844 rcvd=486 src=24.119.129.125 dst=10.120.10.123 src_port=38660 d
2007-06-14 23:59:07 192.168.254.1 action=Permit sent=549 rcvd=404 src=192.168.254.80 dst=208.188.166.68 src_port=15113
2007-06-14 23:59:07 192.168.254.1 action=Permit sent=549 rcvd=404 src=192.168.254.80 dst=208.188.166.68 src_port=14817
2007-06-14 23:59:07 192.168.254.1 action=Deny sent=0 rcvd=12288 src=10.130.9.3 dst=224.0.0.2 src_port=49415 dst_port=49
2007-06-14 23:59:09 192.168.254.1 action=Permit sent=13795 rcvd=149962 src=70.185.198.122 dst=10.120.10.122 src_port=61
2007-06-14 23:59:09 192.168.254.1 action=Permit sent=690 rcvd=415 src=70.185.198.247 dst=10.120.10.123 src_port=48392 d
2007-06-14 23:59:09 192.168.254.1 action=Permit sent=12219 rcvd=140495 src=70.185.198.122 dst=10.120.10.122 src_port=61
2007-06-14 23:59:09 192.168.254.1 action=Deny sent=0 rcvd=12288 src=10.130.9.2 dst=224.0.0.2 src_port=49415 dst_port=49
2007-06-14 23:59:10 192.168.254.1 action=Deny sent=0 rcvd=12288 src=10.130.9.3 dst=224.0.0.2 src_port=49415 dst_port=49
2007-06-14 18:34:04 192.168.254.1 action=Permit sent=3018 rcvd=34134 src=70.185.198.247 dst=10.120.10.122 src_port=4480
2007-06-14 18:34:05 192.168.254.1 action=Permit sent=799 rcvd=6686 src=70.185.198.247 dst=10.120.10.122 src_port=46244
2007-06-14 18:34:07 192.168.254.1 action=Permit sent=2780 rcvd=18874 src=70.185.198.247 dst=10.120.10.122 src_port=4532
2007-06-14 18:34:07 192.168.254.1 action=Permit sent=2737 rcvd=8922 src=24.119.169.162 dst=10.120.10.122 src_port=2689
2007-06-14 18:34:09 192.168.254.1 action=Permit sent=2094 rcvd=23180 src=70.185.198.247 dst=10.120.10.122 src_port=4685
2007-06-14 18:34:11 192.168.254.1 action=Permit sent=2612 rcvd=68608 src=70.185.198.247 dst=10.120.10.122 src_port=4711
2007-06-14 18:34:12 192.168.254.1 action=Permit sent=4131 rcvd=71135 src=24.119.169.162 dst=10.120.10.122 src_port=1665
2007-06-14 18:34:13 192.168.254.1 action=Permit sent=646 rcvd=1803 src=70.185.198.247 dst=10.120.10.122 src_port=47368
2007-06-14 21:47:29 192.168.254.1 action=Permit sent=729 rcvd=1115 src=70.185.198.247 dst=10.120.10.122 src_port=48136
2007-06-14 21:47:30 192.168.254.1 action=Permit sent=766 rcvd=415 src=70.185.198.122 dst=10.120.10.123 src_port=62212 d
2007-06-14 21:47:35 192.168.254.1 action=Permit sent=5054 rcvd=81725 src=24.119.169.162 dst=10.120.10.122 src_port=7809
2007-06-14 21:47:37 192.168.254.1 action=Permit sent=26196 rcvd=233409 src=24.119.129.125 dst=10.120.10.122 src_port=38
2007-06-14 21:47:40 192.168.254.1 action=Deny sent=0 rcvd=12288 src=10.130.9.2 dst=224.0.0.2 src_port=49415 dst_port=49
2007-06-14 21:47:41 192.168.254.1 action=Permit sent=18121 rcvd=210841 src=216.97.160.253 dst=10.120.10.122 src_port=94
2007-06-14 21:47:42 192.168.254.1 action=Permit sent=3741 rcvd=102596 src=24.119.169.162 dst=10.120.10.122 src_port=579
2007-06-14 21:47:42 192.168.254.1 action=Permit sent=2982 rcvd=24075 src=24.119.169.162 dst=10.120.10.122 src_port=641
2007-06-14 21:47:43 192.168.254.1 action=Permit sent=2197 rcvd=28655 src=24.119.169.162 dst=10.120.10.122 src_port=1690
2007-06-14 21:47:46 192.168.254.1 action=Permit sent=840 rcvd=461 src=24.119.169.162 dst=10.120.10.123 src_port=15185 d
2007-06-14 21:47:49 192.168.254.1 action=Permit sent=3348 rcvd=18192 src=24.119.169.162 dst=10.120.10.122 src_port=4737
2007-06-14 21:47:55 192.168.254.1 action=Permit sent=3780 rcvd=34120 src=24.119.169.162 dst=10.120.10.122 src_port=373
2007-06-14 21:47:57 192.168.254.1 action=Permit sent=3604 rcvd=30265 src=24.119.169.162 dst=10.120.10.122 src_port=6785
2007-06-14 21:47:58 192.168.254.1 action=Permit sent=3406 rcvd=39273 src=24.119.169.162 dst=10.120.10.122 src_port=5781
2007-06-14 21:47:59 192.168.254.1 action=Deny sent=0 rcvd=12288 src=10.130.9.3 dst=224.0.0.2 src_port=49415 dst_port=49
2007-06-14 21:48:04 192.168.254.1 action=Permit sent=549 rcvd=404 src=192.168.254.42 dst=208.188.166.68 src_port=7696 d
2007-06-14 21:48:05 192.168.254.1 action=Deny sent=0 rcvd=12288 src=10.130.9.2 dst=224.0.0.2 src_port=49415 dst_port=49
2007-06-14 21:48:09 192.168.254.1 action=Deny sent=0 rcvd=12288 src=10.130.9.3 dst=224.0.0.2 src_port=49415 dst_port=49
2007-06-14 21:48:09 192.168.254.1 action=Deny sent=0 rcvd=12288 src=10.130.9.2 dst=224.0.0.2 src_port=49415 dst_port=49
2007-06-14 21:48:10 192.168.254.1 action=Permit sent=407 rcvd=0 src=192.168.254.14 dst=204.61.5.130 src_port=260 dst_po
2007-06-14 21:48:13 192.168.254.1 action=Permit sent=1040 rcvd=0 src=192.168.254.14 dst=204.61.5.130 src_port=41216 dst
2007-06-14 21:48:15 192.168.254.1 action=Deny sent=0 rcvd=12288 src=10.130.9.3 dst=224.0.0.2 src_port=49415 dst_port=49
2007-06-14 21:48:16 192.168.254.1 action=Deny sent=0 rcvd=12264 src=10.130.9.3 dst=224.0.0.2 src_port=49415 dst_port=49

```

What can the investigator infer from the screenshot seen below?

- A. A smurf attack has been attempted
- B. A denial of service has been attempted
- C. Network intrusion has occurred
- D. Buffer overflow attempt on the firewall.

Answer: C

NEW QUESTION 749

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 753

- (Exam Topic 2)

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

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

Answer: A

NEW QUESTION 755

- (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 759

- (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 764

- (Exam Topic 2)

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

- A. Rule-based attack
- B. Brute force attack
- C. Syllable attack
- D. Hybrid attack

Answer: A

NEW QUESTION 768

- (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 771

- (Exam Topic 2)

Travis, a computer forensics investigator, is finishing up a case he has been working on for over a month involving copyright infringement and embezzlement. His last task is to prepare an investigative report for the president of the company he has been working for. Travis must submit a hard copy and an electronic copy to this president. In what electronic format should Travis send this report?

- A. TIFF-8
- B. DOC
- C. WPD
- D. PDF

Answer: D

NEW QUESTION 775

- (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 780

- (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 785

- (Exam Topic 2)

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

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

Answer: A

NEW QUESTION 788

- (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 793

- (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 795

- (Exam Topic 2)

When needing to search for a website that is no longer present on the Internet today but was online few years back, what site can be used to view the website collection of pages?

- A. Proxify.net
- B. Dnsstuff.com
- C. Samspace.org
- D. Archive.org

Answer: D

NEW QUESTION 798

- (Exam Topic 2)

What does 254 represent in ICCID 89254021520014515744?

- A. Industry Identifier Prefix
- B. Country Code

- C. Individual Account Identification Number
- D. Issuer Identifier Number

Answer: B

NEW QUESTION 800

- (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?

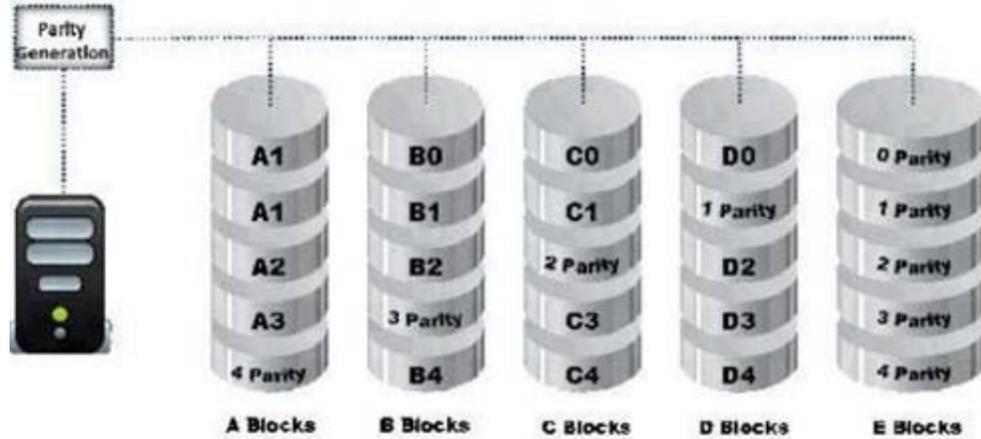
- A. Net sessions
- B. Net config
- C. Net share
- D. Net use

Answer: D

NEW QUESTION 805

- (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 807

- (Exam Topic 2)

What hashing method is used to password protect Blackberry devices?

- A. AES
- B. RC5
- C. MD5
- D. SHA-1

Answer: D

NEW QUESTION 809

- (Exam Topic 2)

Which of the following options will help users to enable or disable the last access time on a system running Windows 10 OS?

- A. wmic service
- B. Reg.exe
- C. fsutil
- D. Devcon

Answer: C

NEW QUESTION 812

- (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 813

- (Exam Topic 2)

What does the 63.78.199.4(161) denotes in a Cisco router log?

Mar 14 22:57:53.425 EST: %SEC-6-IPACCESSLOGP: list internet-inbound denied udp 66.56.16.77(1029) -> 63.78.199.4(161), 1 packet

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

Answer: A

NEW QUESTION 816

- (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 821

- (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 824

- (Exam Topic 2)

Which of the following are small pieces of data sent from a website and stored on the user's computer by the user's web browser to track, validate, and maintain specific user information?

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

Answer: C

NEW QUESTION 828

- (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 833

- (Exam Topic 2)

Which of the following technique creates a replica of an evidence media?

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

Answer: C

NEW QUESTION 835

- (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 838

- (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 842

- (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 845

- (Exam Topic 2)

What type of flash memory card comes in either Type I or Type II and consumes only five percent of the power required by small hard drives?

- A. SD memory
- B. CF memory
- C. MMC memory
- D. SM memory

Answer: B

NEW QUESTION 849

- (Exam Topic 2)

Which of the following tasks DOES NOT come under the investigation phase of a cybercrime forensics investigation case?

- A. Data collection
- B. Secure the evidence
- C. First response
- D. Data analysis

Answer: C

NEW QUESTION 850

- (Exam Topic 2)

Bob works as information security analyst for a big finance company. One day, the anomaly-based intrusion detection system alerted that a volumetric DDOS targeting the main IP of the main web server was occurring. What kind of attack is it?

- A. IDS attack
- B. APT
- C. Web application attack
- D. Network attack

Answer: D

NEW QUESTION 854

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 858

- (Exam Topic 2)

Which of the following is a database in which information about every file and directory on an NT File System (NTFS) volume is stored?

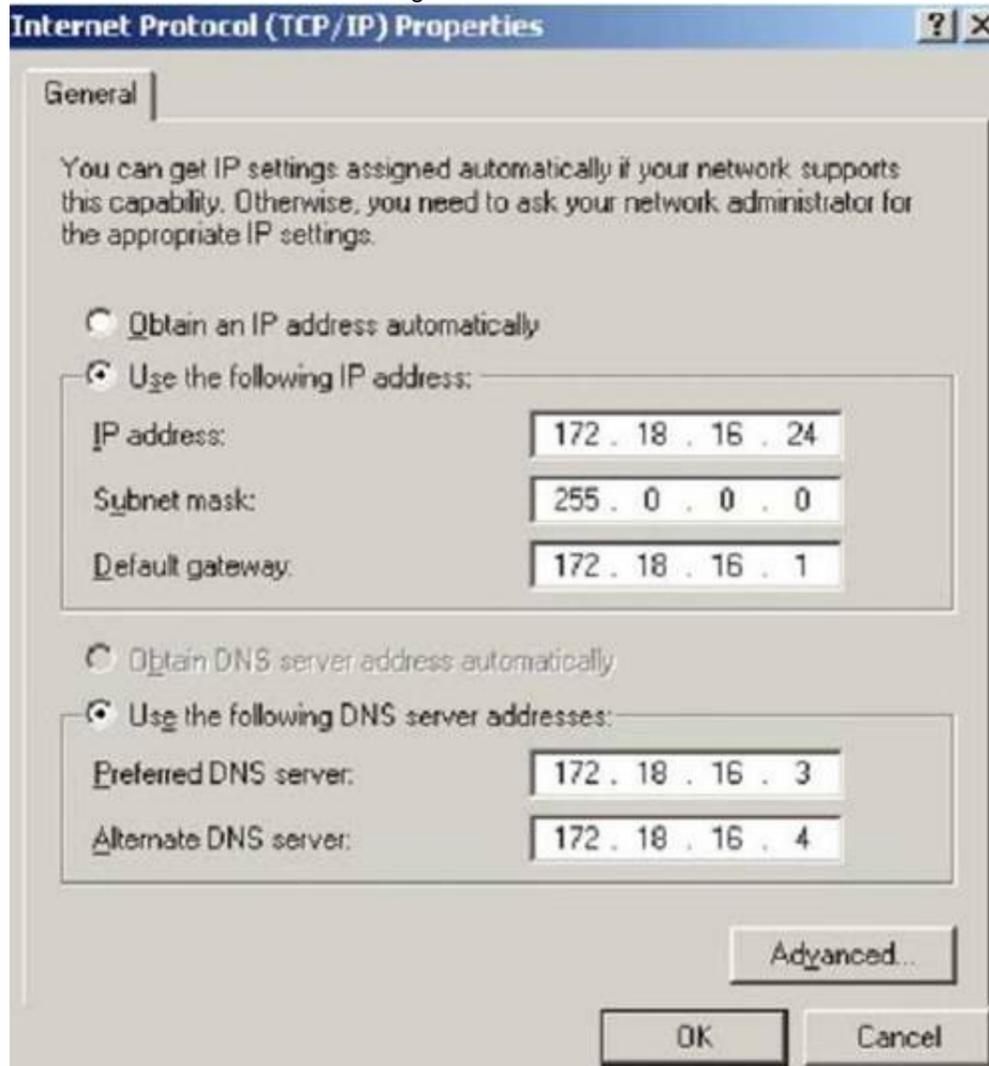
- A. Volume Boot Record
- B. Master Boot Record
- C. GUID Partition Table
- D. Master File Table

Answer: D

NEW QUESTION 859

- (Exam Topic 2)

What is the CIDR from the following screenshot?



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

Answer: D

NEW QUESTION 861

- (Exam Topic 2)

Which of the following Event Correlation Approach checks and compares all the fields systematically and intentionally for positive and negative correlation with each other to determine the correlation across one or multiple fields?

- A. Rule-Based Approach
- B. Automated Field Correlation
- C. Field-Based Approach
- D. Graph-Based Approach

Answer: B

NEW QUESTION 862

- (Exam Topic 2)

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

- A. Slow query log file
- B. General query log file
- C. Binary log
- D. Error log file

Answer: D

NEW QUESTION 867

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 868

- (Exam Topic 2)

Which of the following is a list of recently used programs or opened files?

- A. Most Recently Used (MRU)
- B. Recently Used Programs (RUP)
- C. Master File Table (MFT)
- D. GUID Partition Table (GPT)

Answer: A

NEW QUESTION 871

- (Exam Topic 2)

What is the size value of a nibble?

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

Answer: C

NEW QUESTION 873

- (Exam Topic 2)

Which of the following acts as a network intrusion detection system as well as network intrusion prevention system?

- A. Accunetix
- B. Nikto
- C. Snort
- D. Kismet

Answer: C

NEW QUESTION 874

- (Exam Topic 2)

Which password cracking technique uses details such as length of password, character sets used to construct the password, etc.?

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

Answer: A

NEW QUESTION 875

- (Exam Topic 2)

Files stored in the Recycle Bin in its physical location are renamed as Dxy.ext, where "x" represents the _____.

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

Answer: A

NEW QUESTION 878

- (Exam Topic 2)

A picture file is recovered from a computer under investigation. During the investigation process, the file is enlarged 500% to get a better view of its contents. The picture quality is not degraded at all from this process. What kind of picture is this file. What kind of picture is this file?

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

Answer: B

NEW QUESTION 879

- (Exam Topic 2)

Why is it still possible to recover files that have been emptied from the Recycle Bin on a Windows computer?

- A. The data is still present until the original location of the file is used
- B. The data is moved to the Restore directory and is kept there indefinitely
- C. The data will reside in the L2 cache on a Windows computer until it is manually deleted
- D. It is not possible to recover data that has been emptied from the Recycle Bin

Answer: A

NEW QUESTION 882

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions and Answers in PDF Format

312-49v10 Practice Exam Features:

- * 312-49v10 Questions and Answers Updated Frequently
- * 312-49v10 Practice Questions Verified by Expert Senior Certified Staff
- * 312-49v10 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * 312-49v10 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The 312-49v10 Practice Test Here](#)