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)
What operating system would respond to the following command?

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

Answer: B

NEW QUESTION 3
- (Exam Topic 1)
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 4
- (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 5
- (Exam Topic 1)
Windows identifies which application to open a file with by examining which of the following?

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

Answer: A

NEW QUESTION 6
- (Exam Topic 1)
After passing her CEH exam, Carol wants to ensure that her network is completely secure. She implements a DMZ, stateful firewall, NAT, IPSEC, and a packet filtering firewall. Since all security measures were taken, none of the hosts on her network can reach the Internet. Why is that?

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

Answer: D

NEW QUESTION 7
- (Exam Topic 1)

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

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

Answer: A

NEW QUESTION 8
- (Exam Topic 1)
Chris has been called upon to investigate a hacking incident reported by one of his clients. The company suspects the involvement of an insider accomplice in the attack. Upon reaching the incident scene, Chris secures the physical area, records the scene using visual media. He shuts the system down by pulling the power plug so that he does not disturb the system in any way. He labels all cables and connectors prior to disconnecting any. What do you think would be the next sequence of events?

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

Answer: B

NEW QUESTION 9
- (Exam Topic 1)
What is kept in the following directory? HKLM\SECURITY\Policy\Secrets

A. Cached password hashes for the past 20 users
B. Service account passwords in plain text
C. IAS account names and passwords
D. Local store PKI Kerberos certificates

Answer: B

NEW QUESTION 10
- (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)
Jason is the security administrator of ACMA metal Corporation. One day he notices the company's Oracle database server has been compromised and the customer information along with financial data has been stolen. The financial loss will be in millions of dollars if the database gets into the hands of the competitors. Jason wants to report this crime to the law enforcement agencies immediately.
Which organization coordinates computer crimes investigations throughout the United States?

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

Answer: B

NEW QUESTION 14
- (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 19

- (Exam Topic 1)
When you are running a vulnerability scan on a network and the IDS cuts off your connection, what type of IDS is being used?

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

Answer: B

NEW QUESTION 22

- (Exam Topic 1)
A state department site was recently attacked and all the servers had their disks erased. The incident response team sealed the area and commenced investigation. During evidence collection they came across a zip disks that did not have the standard labeling on it. The incident team ran the disk on an isolated system and found that the system disk was accidentally erased. They decided to call in the FBI for further investigation. Meanwhile, they short listed possible suspects including three summer interns. Where did the incident team go wrong?

A. They examined the actual evidence on an unrelated system
B. They attempted to implicate personnel without proof
C. They tampered with evidence by using it
D. They called in the FBI without correlating with the fingerprint data

Answer: C

NEW QUESTION 26

- (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 29

- (Exam Topic 1)
A packet is sent to a router that does not have the packet destination address in its route table. How will the packet get to its proper destination?

A. Root Internet servers
B. Border Gateway Protocol
C. Gateway of last resort
D. Reverse DNS

Answer: C

NEW QUESTION 31

- (Exam Topic 1)
Michael works for Kimball Construction Company as senior security analyst. As part of yearly security audit, Michael scans his network for vulnerabilities. Using Nmap, Michael conducts XMAS scan and most of the ports scanned do not give a response. In what state are these ports?

A. Closed
B. Open
C. Stealth
D. Filtered

Answer: B

NEW QUESTION 33

- (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 37
- (Exam Topic 1)
Corporate investigations are typically easier than public investigations because:

A. the users have standard corporate equipment and software
B. the investigator does not have to get a warrant
C. the investigator has to get a warrant
D. the users can load whatever they want on their machines

Answer: B

NEW QUESTION 42
- (Exam Topic 1)
When cataloging digital evidence, the primary goal is to

A. Make bit-stream images of all hard drives
B. Preserve evidence integrity
C. Not remove the evidence from the scene
D. Not allow the computer to be turned off

Answer: B

NEW QUESTION 46
- (Exam Topic 1)
What TCP/UDP port does the toolkit program netstat use?

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

Answer: B

NEW QUESTION 51
- (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 52
- (Exam Topic 2)
When making the preliminary investigations in a sexual harassment case, how many investigators are you recommended having?

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

Answer: B

NEW QUESTION 53
- (Exam Topic 2)
What technique is used by JPEGs for compression?

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

Answer: C

NEW QUESTION 54
- (Exam Topic 2)
John is working as a computer forensics investigator for a consulting firm in Canada. He is called to seize a computer at a local web caf purportedly used as a botnet server. John thoroughly scans the computer and finds nothing that would lead him to think the computer was a botnet server. John decides to scan the virtual memory of the computer to possibly find something he had missed. What information will the virtual memory scan produce?

A. It contains the times and dates of when the system was last patched

B. It is not necessary to scan the virtual memory of a computer
C. It contains the times and dates of all the system files
D. Hidden running processes

Answer: D

NEW QUESTION 56
- (Exam Topic 2)
Steven has been given the task of designing a computer forensics lab for the company he works for. He has found documentation on all aspects of how to design a lab except the number of exits needed. How many exits should Steven include in his design for the computer forensics lab?

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

Answer: B

NEW QUESTION 59
- (Exam Topic 2)
What type of attack sends SYN requests to a target system with spoofed IP addresses?

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

Answer: A

NEW QUESTION 64
- (Exam Topic 2)
To check for POP3 traffic using Ethereal, what port should an investigator search by?

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

Answer: C

NEW QUESTION 67
- (Exam Topic 2)
When using an iPod and the host computer is running Windows, what file system will be used?

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

Answer: D

NEW QUESTION 72
- (Exam Topic 2)
Which network attack is described by the following statement?
"At least five Russian major banks came under a continuous hacker attack, although online client services were not disrupted. The attack came from a wide-scale botnet involving at least 24,000 computers, located in 30 countries."

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

Answer: A

NEW QUESTION 74
- (Exam Topic 2)
Which of the following is a record of the characteristics of a file system, including its size, the block size, the empty and the filled blocks and their respective counts, the size and location of the inode tables, the disk block map and usage information, and the size of the block groups?

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

Answer: B

NEW QUESTION 77
- (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 81
- (Exam Topic 1)
What does ICMP Type 3/Code 13 mean?

A. Host Unreachable
B. Administratively Blocked
C. Port Unreachable
D. Protocol Unreachable

Answer: B

NEW QUESTION 86
- (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 90
- (Exam Topic 1)
When investigating a network that uses DHCP to assign IP addresses, where would you look to determine which system (MAC address) had a specific IP address at a specific time?

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

Answer: C

NEW QUESTION 92
- (Exam Topic 1)
The use of warning banners helps a company avoid litigation by overcoming an employee assumed _____. When connecting to the company's intranet, network or Virtual Private Network(VPN) and will allow the company's investigators to monitor, search and retrieve information stored within the network.

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

Answer: D

NEW QUESTION 97
- (Exam Topic 1)
Which of the following is NOT a graphics file?

A. Picture1.tga
B. Picture2.bmp
C. Picture3.nfo
D. Picture4.psd

Answer: C

NEW QUESTION 98
- (Exam Topic 1)
Which part of the Windows Registry contains the user's password file?

A. HKEY_LOCAL_MACHINE

B. HKEY_CURRENT_CONFIGURATION
C. HKEY_USER
D. HKEY_CURRENT_USER

Answer: A

NEW QUESTION 99
- (Exam Topic 1)
Simon is a former employee of Trinitron XML Inc. He feels he was wrongly terminated and wants to hack into his former company's network. Since Simon remembers some of the server names, he attempts to run the axfr and ixfr commands using DIG. What is Simon trying to accomplish here?

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

Answer: C

NEW QUESTION 104
- (Exam Topic 1)
In conducting a computer abuse investigation you become aware that the suspect of the investigation is using ABC Company as his Internet Service Provider (ISP). You contact ISP and request that they provide you assistance with your investigation. What assistance can the ISP provide?

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

Answer: B

NEW QUESTION 106
- (Exam Topic 1)
If a suspect computer is located in an area that may have toxic chemicals, you must:

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

Answer: A

NEW QUESTION 107
- (Exam Topic 1)
You are running through a series of tests on your network to check for any security vulnerabilities.
After normal working hours, you initiate a DoS attack against your external firewall. The firewall Quickly freezes up and becomes unusable. You then initiate an FTP connection from an external IP into your internal network. The connection is successful even though you have FTP blocked at the external firewall. What has happened?

A. The firewall failed-bypass
B. The firewall failed-closed
C. The firewall ACL has been purged
D. The firewall failed-open

Answer: D

NEW QUESTION 108
- (Exam Topic 1)
Melanie was newly assigned to an investigation and asked to make a copy of all the evidence from the compromised system. Melanie did a DOS copy of all the files on the system. What would be the primary reason for you to recommend a disk imaging tool?

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

Answer: C

NEW QUESTION 112
- (Exam Topic 1)
What happens when a file is deleted by a Microsoft operating system using the FAT file system?

A. only the reference to the file is removed from the FAT
B. the file is erased and cannot be recovered
C. a copy of the file is stored and the original file is erased
D. the file is erased but can be recovered

Answer: A

NEW QUESTION 113
- (Exam Topic 1)
Study the log given below and answer the following question:
Apr 24 14:46:46 [4663]: spp_portscan: portscan detected from 194.222.156.169
Apr 24 14:46:46 [4663]: IDS27/FIN Scan: 194.222.156.169:56693 -> 172.16.1.107:482
Apr 24 18:01:05 [4663]: IDS/DNS-version-query: 212.244.97.121:3485 -> 172.16.1.107:53
Apr 24 19:04:01 [4663]: IDS213/ftp-passwd-retrieval: 194.222.156.169:1425 -> 172.16.1.107:21
Apr 25 08:02:41 [5875]: spp_portscan: PORTSCAN DETECTED from 24.9.255.53
Apr 25 02:08:07 [5875]: IDS277/DNS-version-query: 63.226.81.13:4499 -> 172.16.1.107:53
Apr 25 02:08:07 [5875]: IDS277/DNS-version-query: 63.226.81.13:4630 -> 172.16.1.101:53
Apr 25 02:38:17 [5875]: IDS/RPC-rpcinfo-query: 212.251.1.94:642 -> 172.16.1.107:111
Apr 25 19:37:32 [5875]: IDS230/web-cgi-space-wildcard: 198.173.35.164:4221 -> 172.16.1.107:80
Apr 26 05:45:12 [6283]: IDS212/dns-zone-transfer: 38.31.107.87:2291 -> 172.16.1.101:53
Apr 26 06:43:05 [6283]: IDS181/nops-x86: 63.226.81.13:1351 -> 172.16.1.107:53
Apr 26 06:44:25 victim7 PAM_pwdb[12509]: (login) session opened for user simple by (uid=0)
Apr 26 06:44:36 victim7 PAM_pwdb[12521]: (su) session opened for user simon by simple(uid=506) Apr 26 06:45:34 [6283]: IDS175/socks-probe:
24.112.167.35:20 -> 172.16.1.107:1080
Apr 26 06:52:10 [6283]: IDS127/telnet-login-incorrect: 172.16.1.107:23 -> 213.28.22.189:4558
Precautionary measures to prevent this attack would include writing firewall rules. Of these firewall rules, which among the following would be appropriate?

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

Answer: A

NEW QUESTION 116
- (Exam Topic 1)
To preserve digital evidence, an investigator should .

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

Answer: C

NEW QUESTION 118
- (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 119
- (Exam Topic 1)
When investigating a potential e-mail crime, what is your first step in the investigation?

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

Answer: A

NEW QUESTION 122
- (Exam Topic 1)
What are the security risks of running a "repair" installation for Windows XP?

A. Pressing Shift+F10gives the user administrative rights
B. Pressing Shift+F1gives 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 127
- (Exam Topic 1)
Which Intrusion Detection System (IDS) usually produces the most false alarms due to the unpredictable behaviors of users and networks?

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

Answer: B

NEW QUESTION 129
- (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 132
- (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 Florid a. 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 135
- (Exam Topic 1)
Jonathan is a network administrator who is currently testing the internal security of his network. He is attempting to hijack a session, using Ettercap, of a user connected to his Web server. Why will Jonathan not succeed?

A. Only an HTTPS session can be hijacked
B. HTTP protocol does not maintain session
C. Only FTP traffic can be hijacked
D. Only DNS traffic can be hijacked

Answer: B

NEW QUESTION 137
- (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 139
- (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 143
- (Exam Topic 1)
Hackers can gain access to Windows Registry and manipulate user passwords, DNS settings, access rights or others features that they may need in order to accomplish their objectives. One simple method for loading an application at startup is to add an entry (Key) to the following Registry Hive:

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

Answer: D

NEW QUESTION 147
- (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 149
- (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 152
- (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 153
- (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 158
- (Exam Topic 1)
E- mail logs contain which of the following information to help you in your investigation? (Choose four.)

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

Answer: ACDE

NEW QUESTION 163
- (Exam Topic 1)
In Linux, what is the smallest possible shellcode?

A. 24 bytes
B. 8 bytes
C. 800 bytes
D. 80 bytes

Answer: A

NEW QUESTION 165

- (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 166
- (Exam Topic 1)
The efforts to obtain information before a trail by demanding documents, depositions, questioned and answers written under oath, written requests for admissions of fact and examination of the scene is a description of what legal term?

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

Answer: D

NEW QUESTION 169
- (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 171
- (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 173
- (Exam Topic 1)
If you see the files Zer0.tar.gz and copy.tar.gz on a Linux system while doing an investigation, what can you conclude?

A. The system files have been copied by a remote attacker
B. The system administrator has created an incremental backup
C. The system has been compromised using a t0rnrootkit
D. Nothing in particular as these can be operational files

Answer: D

NEW QUESTION 174
- (Exam Topic 1)
During the course of a corporate investigation, you find that an Employee is committing a crime. Can the Employer file a criminal complaint with Police?

A. Yes, and all evidence can be turned over to the police
B. Yes, but only if you turn the evidence over to a federal law enforcement agency
C. No, because the investigation was conducted without following standard police procedures
D. No, because the investigation was conducted without warrant

Answer: A

NEW QUESTION 175
- (Exam Topic 1)
You are a security analyst performing a penetration tests for a company in the Midwest. After some initial reconnaissance, you discover the IP addresses of some Cisco routers used by the company. You type in the following URL that includes the IP address of one of the routers:
http://172.168.4.131/level/99/exec/show/config

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

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

Answer: A

NEW QUESTION 176
- (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 177
- (Exam Topic 1)
You are called in to assist the police in an investigation involving a suspected drug dealer. The suspects house was searched by the police after a warrant was obtained and they located a floppy disk in the suspects bedroom. The disk contains several files, but they appear to be password protected. What are two common methods used by password cracking software that you can use to obtain the password?

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

Answer: B

NEW QUESTION 182
- (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 187
- (Exam Topic 1)
The police believe that Melvin Matthew has been obtaining unauthorized access to computers belonging to numerous computer software and computer operating systems manufacturers, cellular telephone manufacturers, Internet Service Providers and Educational Institutions. They also suspect that he has been stealing, copying and misappropriating proprietary computer software belonging to the several victim companies. What is preventing the police from breaking down the suspects door and searching his home and seizing all of his computer equipment if they have not yet obtained a warrant?

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

Answer: A

NEW QUESTION 189
- (Exam Topic 1)
Diskcopy is:

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

Answer: B

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

NEW QUESTION 191
- (Exam Topic 1)
The refers to handing over the results of private investigations to the authorities because of indications of criminal activity.

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

Answer: D

NEW QUESTION 192
- (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 195
- (Exam Topic 1)
Which federal computer crime law specifically refers to fraud and related activity in connection with access devices like routers?

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

Answer: A

NEW QUESTION 198
- (Exam Topic 1)
What does mactime, an essential part of the coroner's toolkit do?

A. It traverses the file system and produces a listing of all files based on the modification, access and change timestamps
B. It can recover deleted file space and search it for dat
C. However, it does not allow the investigator to preview them
D. The tools scans for i-node information, which is used by other tools in the tool kit
E. It is too specific to the MAC OS and forms a core component of the toolkit

Answer: A

NEW QUESTION 201
- (Exam Topic 1)
Jason has set up a honeypot environment by creating a DMZ that has no physical or logical access to his production network. In this honeypot, he has placed a server running Windows Active Directory. He has also placed a Web server in the DMZ that services a number of web pages that offer visitors a chance to download sensitive information by clicking on a button. A week later, Jason finds in his network logs how an intruder accessed the honeypot and downloaded sensitive information. Jason uses the logs to try and prosecute the intruder for stealing sensitive corporate information. Why will this not be viable?

A. Entrapment
B. Enticement
C. Intruding into a honeypot is not illegal
D. Intruding into a DMZ is not illegal

Answer: A

NEW QUESTION 202
- (Exam Topic 1)
Sectors in hard disks typically contain how many bytes?

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

Answer: B

NEW QUESTION 203
- (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 206
- (Exam Topic 1)
At what layer of the OSI model do routers function on?

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

Answer: B

NEW QUESTION 207
- (Exam Topic 1)
When monitoring for both intrusion and security events between multiple computers, it is essential that the computers' clocks are synchronized. Synchronized time allows an administrator to reconstruct what took place during an attack against multiple computers. Without synchronized time, it is very difficult to determine exactly when specific events took place, and how events interlace. What is the name of the service used to synchronize time among multiple computers?

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

Answer: B

NEW QUESTION 208
- (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 210
- (Exam Topic 4)
Jacob, a cybercrime investigator, joined a forensics team to participate in a criminal case involving digital evidence. After the investigator collected all the evidence and presents it to the court, the judge dropped the case and the defense attorney pressed charges against Jacob and the rest of the forensics team for unlawful search and seizure. What forensics privacy issue was not addressed prior to collecting the evidence?

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

Answer: D

NEW QUESTION 214
- (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 218
- (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 220
- (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 221
- (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 222
- (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 224
- (Exam Topic 4)
Which of the following methods of mobile device data acquisition captures all the data present on the device, as well as all deleted data and access to unallocated space?

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

Answer: D

NEW QUESTION 229
- (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 230
- (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-zO-9\%I*((\%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 233

- (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 234
- (Exam Topic 4)
You are an information security analyst at a large pharmaceutical company. While performing a routine review of audit logs, you have noticed a significant amount of egress traffic to various IP addresses on destination port 22 during off-peak hours. You researched some of the IP addresses and found that many of them are in Eastern Europe. What is the most likely cause of this traffic?

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

Answer: C

NEW QUESTION 236
- (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 241
- (Exam Topic 4)
William is examining a log entry that reads 192.168.0.1 - - [18/Jan/2020:12:42:29 +0000] "GET / HTTP/1.1" 200 1861. Which of the following logs does the log entry belong to?

A. The combined log format of Apache access log
B. The common log format of Apache access log
C. Apache error log
D. IIS log

Answer: A

NEW QUESTION 244
- (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 245
- (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 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 247

- (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 252
- (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 256
- (Exam Topic 4)
Which following forensic tool allows investigator to detect and extract hidden streams on NTFS drive?

A. Stream Detector
B. TimeStomp
C. Autopsy
D. analyzeMFT

Answer: A

NEW QUESTION 259
- (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 262
- (Exam Topic 4)
An investigator wants to extract passwords from SAM and System Files. Which tool can the Investigator use to obtain a list of users, passwords, and their hashes In this case?

A. PWdump7
B. HashKey
C. Nuix
D. FileMerlin

Answer: A

NEW QUESTION 264
- (Exam Topic 4)
Frank, a cloud administrator in his company, needs to take backup of the OS disks of two Azure VMs that store business-critical data. Which type of Azure blob storage can he use for this purpose?

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

Answer: D

NEW QUESTION 269
- (Exam Topic 4)
A cybercriminal is attempting to remove evidence from a Windows computer. He deletes the file evldence1.doc. sending it to Windows Recycle Bin. The cybercriminal then empties the Recycle Bin. After having been removed from the Recycle Bin. what will happen to the data?

A. The data will remain in its original clusters until it is overwritten

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

Answer: A

NEW QUESTION 272
- (Exam Topic 4)
Sally accessed the computer system that holds trade secrets of the company where she Is employed. She knows she accessed It without authorization and all access (authorized and unauthorized) to this computer Is monitored.To cover her tracks. Sally deleted the log entries on this computer. What among the following best describes her action?

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

Answer: B

NEW QUESTION 276
- (Exam Topic 4)
Which layer in the loT 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 278
- (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 279
- (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 282
- (Exam Topic 4)
For the purpose of preserving the evidentiary chain of custody, which of the following labels is not appropriate?

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

Answer: D

NEW QUESTION 285
- (Exam Topic 4)
An EC2 instance storing critical data of a company got infected with malware. The forensics team took the EBS volume snapshot of the affected Instance to perform further analysis and collected other data of evidentiary value. What should be their next step?

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

Answer: D

NEW QUESTION 290
- (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 291
- (Exam Topic 4)
Robert needs to copy an OS disk snapshot of a compromised VM to a storage account in different region for further investigation. Which of the following should he use in this scenario?

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

Answer: D

NEW QUESTION 294
- (Exam Topic 4)
Matthew has been assigned the task of analyzing a suspicious MS Office document via static analysis over an Ubuntu-based forensic machine. He wants to see what type of document It Is. whether It Is encrypted, or contains any flash objects/VBA macros. Which of the following python-based script should he run to get relevant information?

A. oleform.py
B. oleid.py
C. oledir.py
D. pdfid.py

Answer: B

NEW QUESTION 297
- (Exam Topic 4)
An Investigator Is checking a Cisco firewall log that reads as follows:
Aug 21 2019 09:16:44: %ASA-1-106021: Deny ICMP reverse path check from 10.0.0.44 to 10.0.0.33 on Interface outside
What does %ASA-1-106021 denote?

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

Answer: C

NEW QUESTION 302
- (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 tool should Andrew consider deploying in this scenario?

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

Answer: A

NEW QUESTION 303
- (Exam Topic 4)
"In exceptional circumstances, where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to explain his/her actions and the impact of those actions on the evidence, in the court." Which ACPO principle states this?

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

Answer: D

NEW QUESTION 305
- (Exam Topic 4)
Debbie has obtained a warrant to search a known pedophiles house. Debbie went to the house and executed the search warrant to seize digital devices that have been recorded as being used for downloading Illicit Images. She seized all digital devices except a digital camera. Why did she not collect the digital camera?

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

Answer: A

NEW QUESTION 306
- (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 311
- (Exam Topic 4)
Data density of a disk drive is calculated by using

A. Slack space, bit density, and slack density.
B. Track space, bit area, and slack space.
C. Track density, areal density, and slack density.
D. Track density, areal density, and bit density.

Answer: D

NEW QUESTION 312
- (Exam Topic 3)
An investigator is analyzing a checkpoint firewall log and comes across symbols. What type of log is he looking at?

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

Answer: C

NEW QUESTION 317
- (Exam Topic 3)
Which of the following Android libraries are used to render 2D (SGL) or 3D (OpenGL/ES) graphics content to the screen?

A. OpenGL/ES and SGL
B. Surface Manager
C. Media framework
D. WebKit

Answer: A

NEW QUESTION 322
- (Exam Topic 3)
Which list contains the most recent actions performed by a Windows User?

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

Answer: A

NEW QUESTION 327

- (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 330
- (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 334
- (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 339
- (Exam Topic 3)
You need to deploy a new web-based software package for your organization. The package requires three separate servers and needs to be available on the Internet. What is the recommended architecture in terms of server placement?

A. All three servers need to be placed internally
B. A web server and the database server facing the Internet, an application server on the internal network
C. A web server facing the Internet, an application server on the internal network, a database server on the internal network
D. All three servers need to face the Internet so that they can communicate between themselves

Answer: D

NEW QUESTION 343
- (Exam Topic 3)
What system details can an investigator obtain from the NetBIOS name table cache?

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

Answer: C

NEW QUESTION 346
- (Exam Topic 3)
Gary, a computer technician, is facing allegations of abusing children online by befriending them and sending them illicit adult images from his office computer. What type of investigation does this case require?

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

Answer: B

NEW QUESTION 349
- (Exam Topic 3)
Shane, a forensic specialist, is investigating an ongoing attack on a MySQL database server hosted on a Windows machine with SID "WIN-ABCDE12345F."
Which of the following log file will help Shane in tracking all the client connections and activities performed on the database server?

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

Answer: D

NEW QUESTION 352
- (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 357
- (Exam Topic 3)
Raw data acquisition format creates of a data set or suspect drive.

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

Answer: B

NEW QUESTION 359
- (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 360
- (Exam Topic 3)
What does the 56.58.152.114(445) denote in a Cisco router log?
Jun 19 23:25:46.125 EST: %SEC-4-IPACCESSLOGP: list internet-inbound denied udp 67.124.115.35(8084)
-> 56.58.152.114(445), 1 packet

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

Answer: D

NEW QUESTION 363
- (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 366
- (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 368
- (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 369
- (Exam Topic 3)
Which forensic investigation methodology believes that criminals commit crimes solely to benefit their
criminal enterprises?

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

Answer: C

NEW QUESTION 373
- (Exam Topic 3)
What is the purpose of using Obfuscator in malware?

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

Answer: C

NEW QUESTION 374
- (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 377
- (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 379
- (Exam Topic 3)
Which of the following files store the MySQL database data permanently, including the data that had been deleted, helping the forensic investigator in examining the case and finding the culprit?

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

Answer: D

NEW QUESTION 381
- (Exam Topic 3)
An investigator has extracted the device descriptor for a 1GB thumb drive that looks like: Disk&Ven_Best_Buy&Prod_Geek_Squad_U3&Rev_6.15. What does the "Geek_Squad" part represent?

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

Answer: A

NEW QUESTION 386
- (Exam Topic 3)
In a Linux-based system, what does the command "Last -F" display?

A. Login and logout times and dates of the system
B. Last run processes
C. Last functions performed
D. Recently opened files

Answer: A

NEW QUESTION 387
- (Exam Topic 3)
A forensic examiner is examining a Windows system seized from a crime scene. During the examination of a suspect file, he discovered that the file is password protected. He tried guessing the password using the suspect's available information but without any success. Which of the following tool can help the investigator to solve this issue?

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

Answer: A

NEW QUESTION 388
- (Exam Topic 3)
Andie, a network administrator, suspects unusual network services running on a windows system. Which of the following commands should he use to verify unusual network services started on a Windows system?

A. net serv
B. netmgr
C. lusrmgr
D. net start

Answer: D

NEW QUESTION 389
- (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 393
- (Exam Topic 3)
A section of your forensics lab houses several electrical and electronic equipment. Which type of fire extinguisher you must install in this area to contain any fire incident?

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

Answer: C

NEW QUESTION 395
- (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 400
- (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 401
- (Exam Topic 3)
Which of the following statements is incorrect when preserving digital evidence?

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

Answer: B

NEW QUESTION 403
- (Exam Topic 3)
Adam, a forensic analyst, is preparing VMs for analyzing a malware. Which of the following is NOT a best practice?

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

Answer: D

NEW QUESTION 404
- (Exam Topic 3)
Which U.S. law sets the rules for sending emails for commercial purposes, establishes the minimum requirements for commercial messaging, gives the recipients of emails the right to ask the senders to stop emailing them, and spells out the penalties in case the above said rules are violated?

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

Answer: C

NEW QUESTION 407
- (Exam Topic 3)
Which of the following examinations refers to the process of providing the opposing side in a trial the opportunity to question a witness?

A. Cross Examination
B. Direct Examination
C. Indirect Examination
D. Witness Examination

Answer: A

NEW QUESTION 408
- (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 411
- (Exam Topic 3)
Which of the following components within the android architecture stack take care of displaying windows owned by different applications?

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

Answer: D

NEW QUESTION 416
- (Exam Topic 3)
You are a Penetration Tester and are assigned to scan a server. You need to use a scanning technique wherein the TCP Header is split into many packets so that it becomes difficult to detect what the packets are meant for. Which of the below scanning technique will you use?

A. Inverse TCP flag scanning
B. ACK flag scanning
C. TCP Scanning
D. IP Fragment Scanning

Answer: D

NEW QUESTION 417
- (Exam Topic 3)
What is the location of a Protective MBR in a GPT disk layout?

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

Answer: C

NEW QUESTION 422
- (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 425
- (Exam Topic 3)
An attacker has compromised a cloud environment of a company and used the employee information to perform an identity theft attack. Which type of attack is this?

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

Answer: A

NEW QUESTION 430
- (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 435
- (Exam Topic 3)
James, a hacker, identifies a vulnerability in a website. To exploit the vulnerability, he visits the login page and notes down the session ID that is created. He appends this session ID to the login URL and shares the link with a victim. Once the victim logs into the website using the shared URL, James reloads the webpage (containing the URL with the session ID appended) and now, he can browse the active session of the victim. Which attack did James successfully execute?

A. Cross Site Request Forgery
B. Cookie Tampering
C. Parameter Tampering
D. Session Fixation Attack

Answer: D

NEW QUESTION 440
- (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 443
- (Exam Topic 3)
Which layer of iOS architecture should a forensics investigator evaluate to analyze services such as Threading, File Access, Preferences, Networking and high-level features?

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

Answer: D

NEW QUESTION 446
- (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 447
- (Exam Topic 3)
Analyze the hex representation of mysql-bin.000013 file in the screenshot below. Which of the following will be an inference from this analysis?
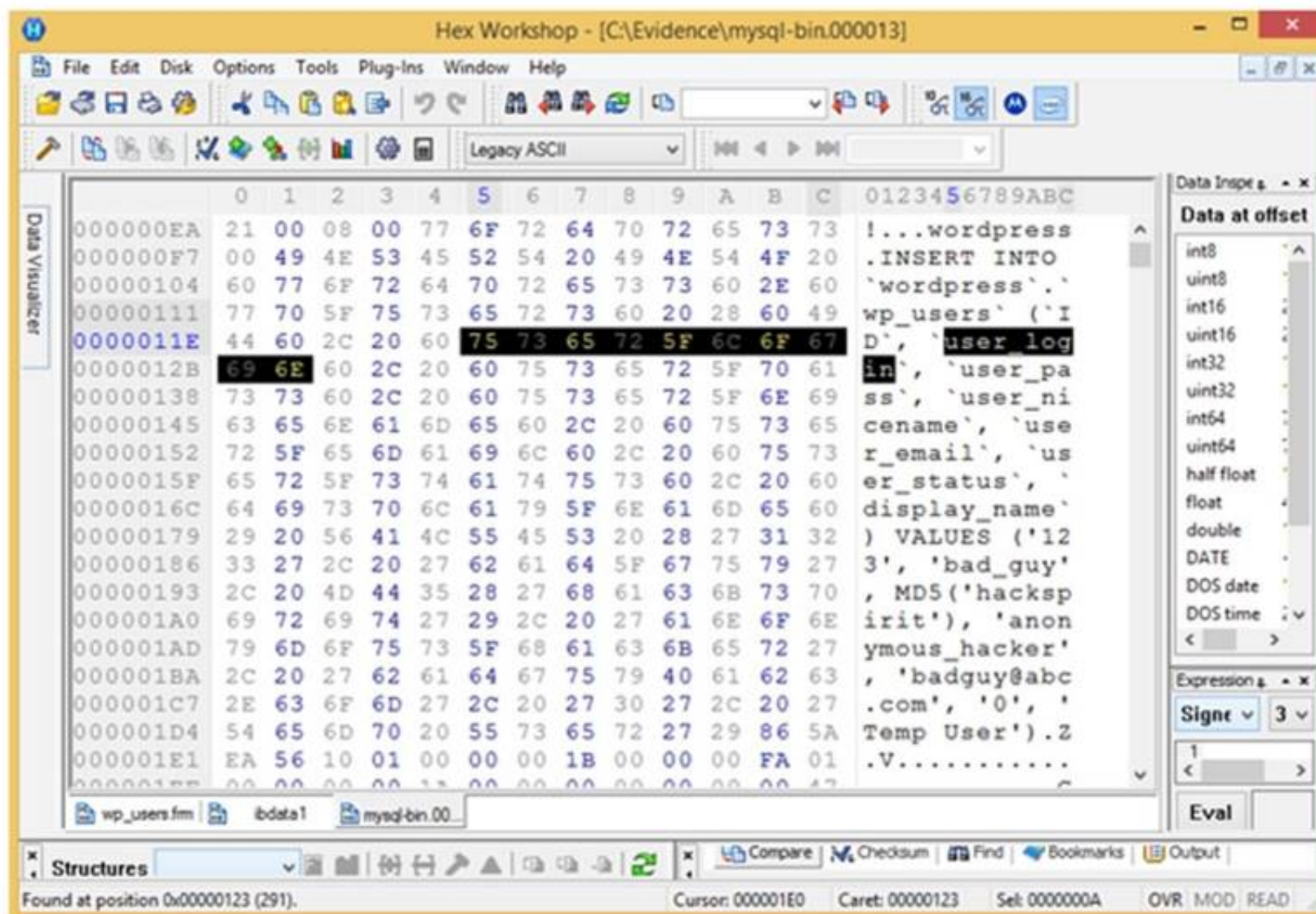
A. A user with username bad_guy has logged into the WordPress web application
B. A WordPress user has been created with the username anonymous_hacker
C. An attacker with name anonymous_hacker has replaced a user bad_guy in the WordPress database
D. A WordPress user has been created with the username bad_guy

Answer: D

NEW QUESTION 450
- (Exam Topic 3)
If the partition size is 4 GB, each cluster will be 32 K. Even if a file needs only 10 K, the entire 32 K will be allocated, resulting in 22 K of .

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

Answer: A

NEW QUESTION 453
- (Exam Topic 3)
Which among the following web application threats is resulted when developers expose various internal implementation objects, such as files, directories, database records, or key-through references?

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

Answer: C

NEW QUESTION 458
- (Exam Topic 3)
What value of the "Boot Record Signature" is used to indicate that the boot-loader exists?

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

Answer: A

NEW QUESTION 461
- (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 466
- (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 470
- (Exam Topic 3)
When analyzing logs, it is important that the clocks of all the network devices are synchronized. Which protocol will help in synchronizing these clocks?

A. UTC
B. PTP
C. Time Protocol
D. NTP

Answer: D

NEW QUESTION 472
- (Exam Topic 3)
Which among the following tools can help a forensic investigator to access the registry files during postmortem analysis?

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

Answer: C

NEW QUESTION 476

- (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 481
- (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 486
- (Exam Topic 3)
Which of the following information is displayed when Netstat is used with -ano switch?
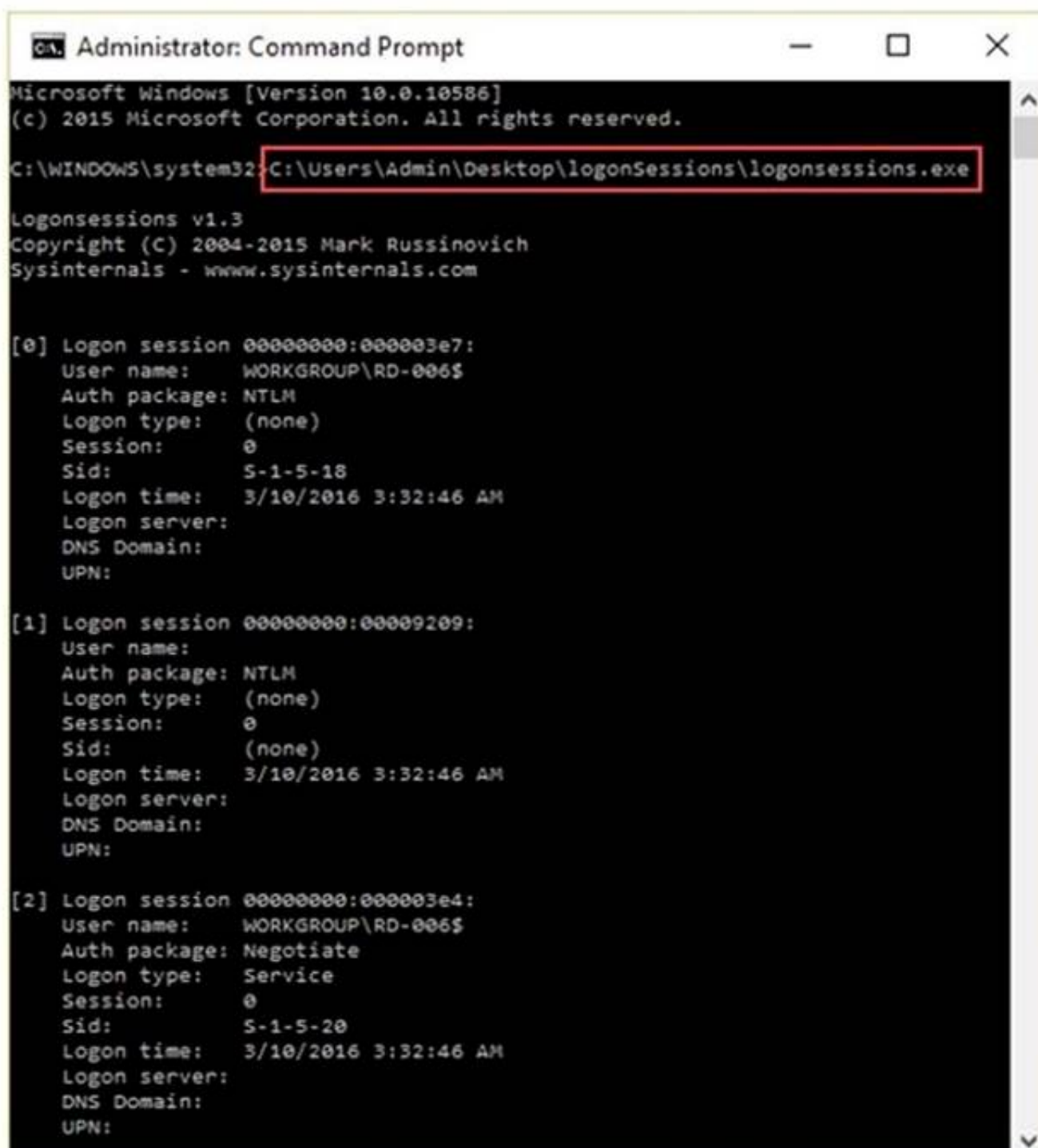
A. Ethernet statistics
B. Contents of IP routing table
C. Details of routing table
D. Details of TCP and UDP connections

Answer: D

NEW QUESTION 489
- (Exam Topic 3)
What is the investigator trying to analyze if the system gives the following image as output?

A. All the logon sessions
B. Currently active logon sessions
C. Inactive logon sessions
D. Details of users who can logon

Answer: B

NEW QUESTION 491
- (Exam Topic 3)
Jim's company regularly performs backups of their critical servers. But the company can't afford to send backup tapes to an off-site vendor for long term storage and archiving. Instead Jim's company keeps the backup tapes in a safe in the office. Jim's company is audited each year, and the results from this year's audit show a risk because backup tapes aren't stored off-site. The Manager of Information Technology has a plan to take the backup tapes home with him and wants to know what two things he can do to secure the backup tapes while in transit?

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

Answer: B

NEW QUESTION 495
- (Exam Topic 3)
Which of the following tools is not a data acquisition hardware tool?

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

Answer: C

NEW QUESTION 499
- (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 503
- (Exam Topic 3)
Which of the following is a responsibility of the first responder?

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

Answer: B

NEW QUESTION 508
- (Exam Topic 3)
Lynne receives the following email:
Dear lynne@gmail.com! We are sorry to inform you that your ID has been temporarily frozen due to incorrect or missing information saved at 2016/11/10 20:40:24
You have 24 hours to fix this problem or risk to be closed permanently! To proceed Please Connect >> My Apple ID
Thank You The link to My Apple ID shows http://byggarbetsplatsen.se/backup/signon/ What type of attack is this?

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

Answer: B

NEW QUESTION 511
- (Exam Topic 3)
Which of the following files contains the traces of the applications installed, run, or uninstalled from a system?

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

Answer: C

NEW QUESTION 513
- (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 515
- (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 520
- (Exam Topic 3)
Which Event Correlation approach assumes and predicts what an attacker can do next after the attack by studying statistics and probability?

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

Answer: B

NEW QUESTION 524
- (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 526
- (Exam Topic 3)
Checkpoint Firewall logs can be viewed through a Check Point Log viewer that uses icons and colors in the log table to represent different security events and their severity. What does the icon in the checkpoint logs represent?

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

Answer: C

NEW QUESTION 527
- (Exam Topic 3)
In Windows, prefetching is done to improve system performance. There are two types of prefetching: boot prefetching and application prefetching. During boot prefetching, what does the Cache Manager do?

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

Answer: C

NEW QUESTION 528
- (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 530
- (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 532
- (Exam Topic 2)
Smith, a forensic examiner, was analyzing a hard disk image to find and acquire deleted sensitive files. He stumbled upon a $Recycle.Bin folder in the root directory of the disk. Identify the operating system in use.

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

Answer: D

NEW QUESTION 536
- (Exam Topic 2)
Annie is searching for certain deleted files on a system running Windows XP OS. Where will she find the files if they were not completely deleted from the system?

A. C: $Recycled.Bin
B. C: \$Recycle.Bin
C. C:\RECYCLER
D. C:\$RECYCLER

Answer: B

NEW QUESTION 541
- (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 542
- (Exam Topic 2)
To which phase of the Computer Forensics Investigation Process does the 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 544
- (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 547

- (Exam Topic 2)
Harold is a computer forensics investigator working for a consulting firm out of Atlanta Georgia. Harold is called upon to help with a corporate espionage case in Miami Florida. Harold assists in the investigation by
pulling all the data from the computers allegedly used in the illegal activities. He finds that two suspects in the company where stealing sensitive corporate information and selling it to competing companies. From the email and instant messenger logs recovered, Harold has discovered that the two employees notified the buyers by writing symbols on the back of specific stop signs. This way, the buyers knew when and where to meet with the alleged suspects to buy the stolen material. What type of steganography did these two suspects use?

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

Answer: B

NEW QUESTION 552
- (Exam Topic 2)
Which of the following is NOT a part of pre-investigation phase?

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

Answer: C

NEW QUESTION 557
- (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 560
- (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 564
- (Exam Topic 2)
A forensics investigator is searching the hard drive of a computer for files that were recently moved to the Recycle Bin. He searches for files in C:\RECYCLED using a command line tool but does not find anything. What is the reason for this?

A. He should search in C:\Windows\System32\RECYCLED folder
B. The Recycle Bin does not exist on the hard drive
C. The files are hidden and he must use switch to view them
D. Only FAT system contains RECYCLED folder and not NTFS

Answer: C

NEW QUESTION 566
- (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 571
- (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 574
- (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 576
- (Exam Topic 2)
All Blackberry email is eventually sent and received through what proprietary RIM-operated mechanism?

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

Answer: A

NEW QUESTION 580
- (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 583
- (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 584
- (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. Samspade.org
D. Archive.org

Answer: D

NEW QUESTION 588
- (Exam Topic 2)
Which US law does the interstate or international transportation and receiving of child pornography fall under?

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

Answer: D

NEW QUESTION 589
- (Exam Topic 2)
Ivanovich, a forensics investigator, is trying to extract complete information about running processes from a system. Where should he look apart from the RAM and virtual memory?

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

Answer: A

NEW QUESTION 590
- (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 593
- (Exam Topic 2)
When carrying out a forensics investigation, why should you never delete a partition on a dynamic disk?

A. All virtual memory will be deleted
B. The wrong partition may be set to active
C. This action can corrupt the disk
D. The computer will be set in a constant reboot state

Answer: C

NEW QUESTION 597
- (Exam Topic 2)
During an investigation, an employee was found to have deleted harassing emails that were sent to someone else. The company was using Microsoft Exchange and had message tracking enabled. Where could the investigator search to find the message tracking log file on the Exchange server?

A. C:\Program Files\Exchsrvr\servername.log
B. D:\Exchsrvr\Message Tracking\servername.log
C. C:\Exchsrvr\Message Tracking\servername.log
D. C:\Program Files\Microsoft Exchange\srvr\servername.log

Answer: A

NEW QUESTION 600
- (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 603
- (Exam Topic 2)
In the following directory listing,
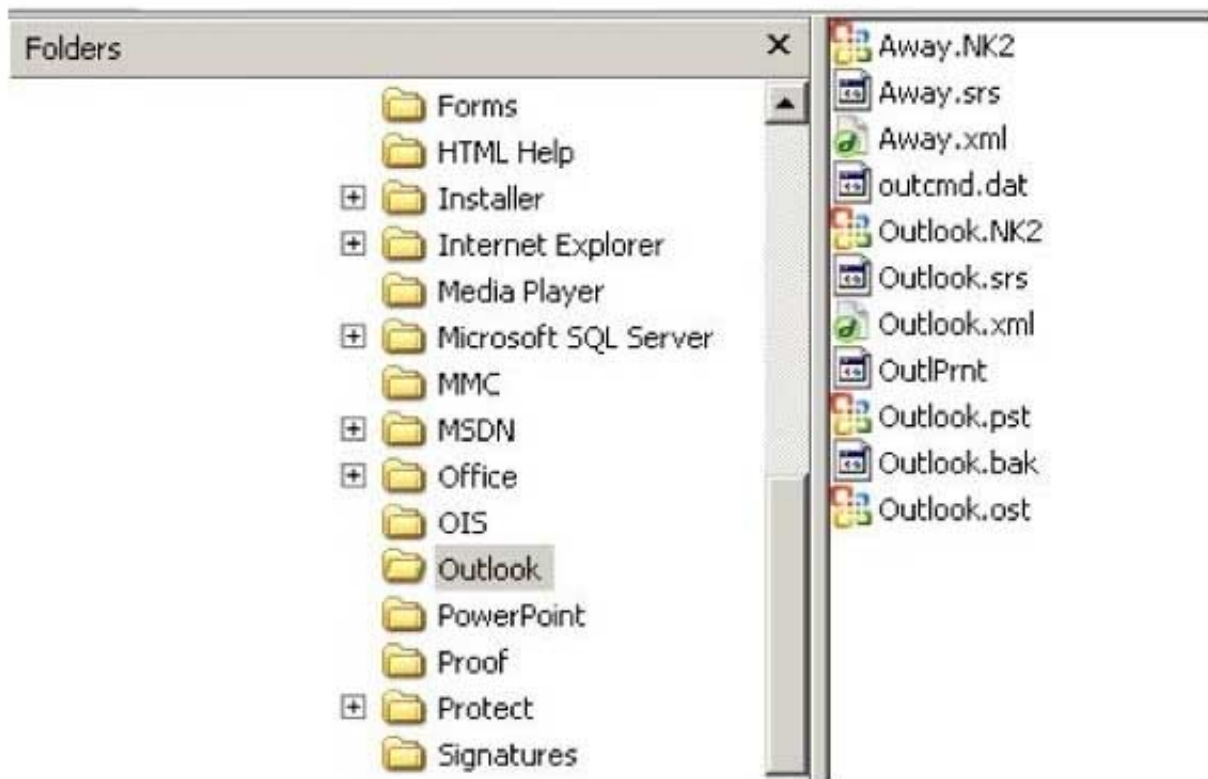
Which file should be used to restore archived email messages for someone using Microsoft Outlook?

A. Outlook bak
B. Outlook ost
C. Outlook NK2
D. Outlook pst

Answer: D

NEW QUESTION 607
- (Exam Topic 2)
Which of the following tool enables data acquisition and duplication?

A. Colasoft's Capsa
B. DriveSpy
C. Wireshark
D. Xplico

Answer: B

NEW QUESTION 608
- (Exam Topic 2)
A forensics investigator needs to copy data from a computer to some type of removable media so he can examine the information at another location. The problem is that the data is around 42GB in size. What type of removable media could the investigator use?

A. Blu-Ray single-layer
B. HD-DVD
C. Blu-Ray dual-layer
D. DVD-18

Answer: C

NEW QUESTION 610
- (Exam Topic 2)
What is the first step taken in an investigation for laboratory forensic staff members?

A. Packaging the electronic evidence
B. Securing and evaluating the electronic crime scene
C. Conducting preliminary interviews
D. Transporting the electronic evidence

Answer: B

NEW QUESTION 615
- (Exam Topic 2)
Where does Encase search to recover NTFS files and folders?

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

Answer: B

NEW QUESTION 616
- (Exam Topic 2)
Which of the following stages in a Linux boot process involve initialization of the system's hardware?

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

Answer: A

NEW QUESTION 621
- (Exam Topic 2)
Wireless access control attacks aim to penetrate a network by evading WLAN access control measures such as AP MAC filters and Wi-Fi port access controls. Which of the following wireless access control attacks allow the attacker to set up a rogue access point outside the corporate perimeter and then lure the employees of the organization to connect to it?

A. Ad hoc associations
B. Client mis-association
C. MAC spoofing
D. Rogue access points

Answer: B

NEW QUESTION 626
- (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 631
- (Exam Topic 2)
What is the default IIS log location?

A. SystemDrive\inetpub\LogFiles
B. %SystemDrive%\inetpub\logs\LogFiles
C. %SystemDrive\logs\LogFiles
D. SystemDrive\logs\LogFiles

Answer: B

NEW QUESTION 634
- (Exam Topic 2)
When marking evidence that has been collected with the aa/ddmmyy/nnnn/zz format, what does the nnn denote?

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

Answer: D

NEW QUESTION 635
- (Exam Topic 2)
What is the CIDR from the following screenshot?
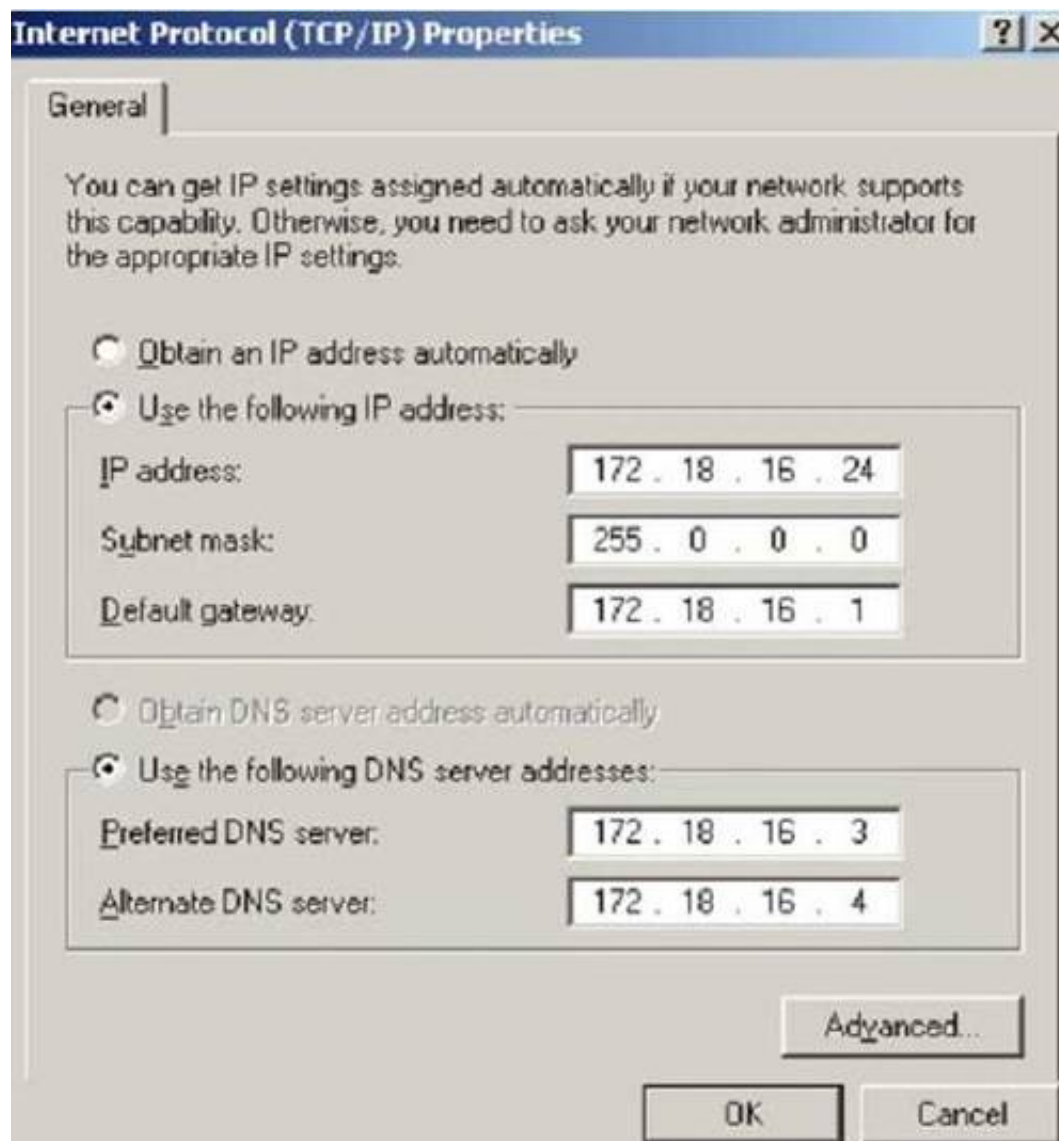
A. /24A./24A./24
B. /32 B./32 B./32
C. /16 C./16 C./16
D. /8D./8D./8

Answer: D

NEW QUESTION 640
- (Exam Topic 2)
Tyler is setting up a wireless network for his business that he runs out of his home. He has followed all the directions from the ISP as well as the wireless router manual. He does not have any encryption set and the SSID is being broadcast. On his laptop, he can pick up the wireless signal for short periods of time, but then the connection drops and the signal goes away.
Eventually the wireless signal shows back up, but drops intermittently. What could be Tyler issue with his home wireless network?

A. Computers on his wired network
B. Satellite television
C. 2.4Ghz Cordless phones
D. CB radio

Answer: C

NEW QUESTION 645
- (Exam Topic 2)
Which of the following tool captures and allows you to interactively browse the traffic on a network?

A. Security Task Manager
B. Wireshark
C. ThumbsDisplay
D. RegScanner

Answer: B

NEW QUESTION 649
- (Exam Topic 2)
An on-site incident response team is called to investigate an alleged case of computer tampering within their company. Before proceeding with the investigation, the CEO informs them that the incident will be classified as low level. How long will the team have to respond to the incident?

A. One working day
B. Two working days
C. Immediately
D. Four hours

Answer: A

NEW QUESTION 650
- (Exam Topic 2)
What must be obtained before an investigation is carried out at a location?

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

Answer: A

NEW QUESTION 655
- (Exam Topic 2)
What is the location of the binary files required for the functioning of the OS in a Linux system?

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

Answer: B

NEW QUESTION 657
- (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 660
- (Exam Topic 2)
The following is a log file screenshot from a default installation of IIS 6.0.

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

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

Answer: A

NEW QUESTION 663
- (Exam Topic 2)
When marking evidence that has been collected with the "aaa/ddmmyy/nnnn/zz" format, what does the "nnnn" denote?

A. The initials of the forensics analyst
B. The sequence number for the parts of the same exhibit

C. The year he evidence was taken
D. The sequential number of the exhibits seized by the analyst

Answer: D

NEW QUESTION 667
- (Exam Topic 2)
Where are files temporarily written in Unix when printing?

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

Answer: D

NEW QUESTION 672
- (Exam Topic 2)
In handling computer-related incidents, which IT role should be responsible for recovery, containment, and prevention to constituents?

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

Answer: B

NEW QUESTION 677
- (Exam Topic 2)
What advantage does the tool Evidor have over the built-in Windows search?

A. It can find deleted files even after they have been physically removed
B. It can find bad sectors on the hard drive
C. It can search slack space
D. It can find files hidden within ADS

Answer: C

NEW QUESTION 682
- (Exam Topic 2)
When investigating a computer forensics case where Microsoft Exchange and Blackberry Enterprise server are used, where would investigator need to search to find email sent from a Blackberry device?
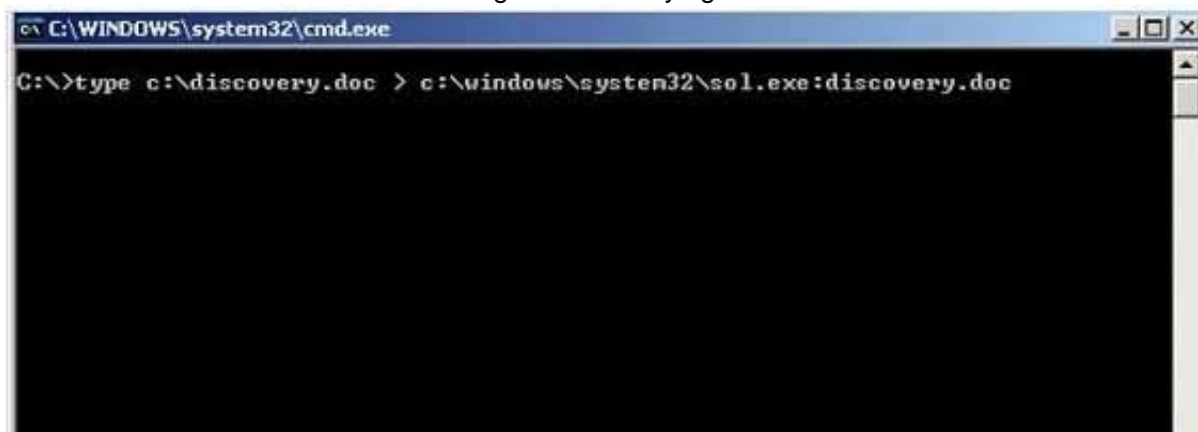
A. RIM Messaging center
B. Blackberry Enterprise server
C. Microsoft Exchange server
D. Blackberry desktop redirector

Answer: C

NEW QUESTION 684
- (Exam Topic 2)
What feature of Windows is the following command trying to utilize?

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

Answer: C

NEW QUESTION 686
- (Exam Topic 2)

How many possible sequence number combinations are there in TCP/IP protocol?

A. 1 billion
B. 320 billion
C. 4 billion
D. 32 million

Answer: C

NEW QUESTION 691
- (Exam Topic 2)
If a PDA is seized in an investigation while the device is turned on, what would be the proper procedure?

A. Keep the device powered on
B. Turn off the device immediately
C. Remove the battery immediately
D. Remove any memory cards immediately

Answer: A

NEW QUESTION 695
- (Exam Topic 2)
While looking through the IIS log file of a web server, you find the following entries:

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

What is evident from this log file?

A. Web bugs
B. Cross site scripting
C. Hidden fields
D. SQL injection is possible

Answer: D

NEW QUESTION 698
- (Exam Topic 2)
If you are concerned about a high level of compression but not concerned about any possible data loss, what type of compression would you use?

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

Answer: B

NEW QUESTION 703
- (Exam Topic 2)
What is the smallest physical storage unit on a hard drive?

A. Track
B. Cluster
C. Sector
D. Platter

Answer: C

NEW QUESTION 708
- (Exam Topic 2)
Paraben Lockdown device uses which operating system to write hard drive data?

A. Mac OS
B. Red Hat
C. Unix
D. Windows

Answer: D

NEW QUESTION 710
......

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

312-49v10 Practice Exam Features:

* 312-49v10 Questions and Answers Updated Frequently

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

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

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

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