EC-Council

Exam Questions 312-49v10

Computer Hacking Forensic Investigator (CHFI-v10)

NEW QUESTION 1
- (Exam Topic 1)
It takes mismanaged case/s to ruin your professional reputation as a computer forensics examiner?

A. by law, three
B. quite a few
C. only one
D. at least two

Answer: C

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

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

Answer: A

NEW QUESTION 3
- (Exam Topic 1)
John is using Firewalk to test the security of his Cisco PIX firewall. He is also utilizing a sniffer located on a subnet that resides deep inside his network. After analyzing the sniffer log files, he does not see any of the traffic produced by Firewalk. Why is that?

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

Answer: D

NEW QUESTION 4
- (Exam Topic 1)
George is performing security analysis for Hammond and Sons LLC. He is testing security vulnerabilities of their wireless network. He plans on remaining as "stealthy" as possible during the scan. Why would a scanner like Nessus is not recommended in this situation?

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

Answer: A

NEW QUESTION 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)
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 7
- (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 8
- (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 9
- (Exam Topic 1)
The objective of this act was to protect consumers' personal financial information held by financial institutions and their service providers.

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

Answer: A

NEW QUESTION 10
- (Exam Topic 1)
When you are running a vulnerability scan on a network and the IDS cuts off your connection, what type of IDS is being used?

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

Answer: B

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

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

Answer: C

NEW QUESTION 14
- (Exam Topic 1)
When reviewing web logs, you see an entry for resource not found in the HTTP status code filed. What is the actual error code that you would see in the log for resource not found?

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

Answer: B

NEW QUESTION 18
- (Exam Topic 1)
You are employed directly by an attorney to help investigate an alleged sexual harassment case at a large pharmaceutical manufacture. While at the corporate office of the company, the CEO demands to know the status of the investigation. What prevents you from discussing the case with the CEO?

A. the attorney-work-product rule
B. Good manners
C. Trade secrets
D. ISO 17799

Answer: A

NEW QUESTION 22
- (Exam Topic 1)
Paul's company is in the process of undergoing a complete security audit including logical and physical security testing. After all logical tests were performed; it is now time for the physical round to begin. None of the employees are made aware of this round of testing. The security-auditing firm sends in a technician dressed as an electrician. He waits outside in the lobby for some employees to get to work and follows behind them when they access the restricted areas. After entering the main office, he is able to get into the server room telling the IT manager that there is a problem with the outlets in that room. What type of attack has the technician performed?

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

Answer: A

NEW QUESTION 24
- (Exam Topic 2)
How many times can data be written to a DVD+R disk?

A. Twice
B. Once
C. Zero
D. Infinite

Answer: B

NEW QUESTION 29
- (Exam Topic 2)
Which of the following Registry components include offsets to other cells as well as the LastWrite time for the key?

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

Answer: C

NEW QUESTION 30
- (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 33
- (Exam Topic 2)
What will the following command accomplish? dd if=/dev/xxx of=mbr.backup bs=512 count=1

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

Answer: A

NEW QUESTION 38
- (Exam Topic 2)
Which of the following commands shows you the names of all open shared files on a server and the number of file locks on each file?

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

Answer: B

NEW QUESTION 41

- (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 44
- (Exam Topic 2)
Amber, a black hat hacker, has embedded a malware into a small enticing advertisement and posted it on a popular ad-network that displays across various websites. What is she doing?

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

Answer: D

NEW QUESTION 49
- (Exam Topic 1)
From the following spam mail header, identify the host IP that sent this spam? From jie02@netvigator.com jie02@netvigator.com Tue Nov 27 17:27:11 2001
Received: from viruswall.ie.cuhk.edu.hk (viruswall [137.189.96.52]) by eng.ie.cuhk.edu.hk (8.11.6/8.11.6) with ESMTP id
fAR9RAP23061 for ; Tue, 27 Nov 2001 17:27:10 +0800 (HKT)
Received: from mydomain.com (pcd249020.netvigator.com [203.218.39.20]) by viruswall.ie.cuhk.edu.hk (8.12.1/8.12.1)
with SMTP id fAR9QXwZ018431 for ; Tue, 27 Nov 2001 17:26:36 +0800 (HKT)
Message-Id: >200111270926.fAR9QXwZ018431@viruswall.ie.cuhk.edu.hk From: "china hotel web"
To: "Shlam"
Subject: SHANGHAI (HILTON HOTEL) PACKAGE
Date: Tue, 27 Nov 2001 17:25:58 +0800 MIME-Version: 1.0
X- Priority: 3 X-MSMail- Priority: Normal
Reply-To: "china hotel web"

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

Answer: C

NEW QUESTION 53
- (Exam Topic 1)
Lance wants to place a honeypot on his network. Which of the following would be your recommendations?

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

Answer: D

NEW QUESTION 56
- (Exam Topic 1)
After undergoing an external IT audit, George realizes his network is vulnerable to DDoS attacks. What countermeasures could he take to prevent DDoS attacks?

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

Answer: B

NEW QUESTION 60
- (Exam Topic 1)
You are working for a large clothing manufacturer as a computer forensics investigator and are called in to investigate an unusual case of an employee possibly stealing clothing designs from the company and selling them under a different brand name for a different company. What you discover during the course of the investigation is that the clothing designs are actually original products of the employee and the company has no policy against an employee selling his own designs on his own time. The only thing that you can find that the employee is doing wrong is that his clothing design incorporates the same graphic symbol as that of the company with only the wording in the graphic being different. What area of the law is the employee violating?

A. trademark law
B. copyright law
C. printright law
D. brandmark law

Answer: A

NEW QUESTION 63
- (Exam Topic 1)
You have used a newly released forensic investigation tool, which doesn't meet the Daubert Test, during a case. The case has ended-up in court. What argument could the defense make to weaken your case?

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

Answer: C

NEW QUESTION 65
- (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 69
- (Exam Topic 1)
What information do you need to recover when searching a victim’s computer for a crime committed with specific e-mail message?

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

Answer: B

NEW QUESTION 70
- (Exam Topic 1)
If you plan to startup a suspect's computer, you must modify the to ensure that you do not contaminate or alter data on the suspect's hard drive by booting to the hard drive.

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

Answer: C

NEW QUESTION 71
- (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 73
- (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 75
- (Exam Topic 1)
You should make at least how many bit-stream copies of a suspect drive?

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

Answer: B

NEW QUESTION 77
- (Exam Topic 1)
What does the superblock in Linux define?

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

Answer: C

NEW QUESTION 79
- (Exam Topic 1)
What does the acronym POST mean as it relates to a PC?

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

Answer: B

NEW QUESTION 82
- (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 87
- (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 89
- (Exam Topic 1)
During the course of an investigation, you locate evidence that may prove the innocence of the suspect of the investigation. You must maintain an unbiased opinion and be objective in your entire fact finding process. Therefore, you report this evidence. This type of evidence is known as:

A. Inculpatory evidence
B. Mandatory evidence
C. Exculpatory evidence
D. Terrible evidence

Answer: C

NEW QUESTION 90
- (Exam Topic 1)
James is testing the ability of his routers to withstand DoS attacks. James sends ICMP ECHO requests to the broadcast address of his network. What type of DoS attack is James testing against his network?

A. Smurf
B. Trinoo
C. Fraggle
D. SYN flood

Answer: A

NEW QUESTION 95
- (Exam Topic 1)
Why is it a good idea to perform a penetration test from the inside?

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

Answer: B

NEW QUESTION 98
- (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 103
- (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 105
- (Exam Topic 1)
What is the following command trying to accomplish?

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

Answer: A

NEW QUESTION 109
- (Exam Topic 1)
Why should you note all cable connections for a computer you want to seize as evidence?

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

Answer: A

NEW QUESTION 110
- (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 113
- (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 116
- (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 121
- (Exam Topic 1)
With Regard to using an Antivirus scanner during a computer forensics investigation, You should:

A. Scan the suspect hard drive before beginning an investigation
B. Never run a scan on your forensics workstation because it could change your systems configuration
C. Scan your forensics workstation at intervals of no more than once every five minutes during an investigation
D. Scan your Forensics workstation before beginning an investigation

Answer: D

NEW QUESTION 126
- (Exam Topic 1)
A law enforcement officer may only search for and seize criminal evidence with , which are facts or circumstances that would lead a reasonable person to believe a crime has been committed or is about to be committed, evidence of the specific crime exists and the evidence of the specific crime exists at the place to be searched.

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

Answer: C

NEW QUESTION 130
- (Exam Topic 1)
Larry is an IT consultant who works for corporations and government agencies. Larry plans on shutting down the city's network using BGP devices and zombies? What type of Penetration Testing is Larry planning to carry out?

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

Answer: B

NEW QUESTION 134
- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 135
- (Exam Topic 1)
The MD5 program is used to:

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

Answer: D

NEW QUESTION 139
- (Exam Topic 1)
To make sure the evidence you recover and analyze with computer forensics software can be admitted in court, you must test and validate the software. What group is actively providing tools and creating procedures for testing and validating computer forensics software?

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

Answer: C

NEW QUESTION 144
- (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 145
- (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 150
- (Exam Topic 1)
Which is a standard procedure to perform during all computer forensics investigations?

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

Answer: A

NEW QUESTION 153
- (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 154
- (Exam Topic 1)
Microsoft Outlook maintains email messages in a proprietary format in what type of file?

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

Answer: C

NEW QUESTION 157
- (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 161
- (Exam Topic 1)
John and Hillary works at the same department in the company. John wants to find out Hillary's network password so he can take a look at her documents on the file server. He enables Lophtcrack program to sniffing mode. John sends Hillary an email with a link to Error! Reference source not found. What information will he be able to gather from this?

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

Answer: A

NEW QUESTION 163
- (Exam Topic 1)
Which response organization tracks hoaxes as well as viruses?

A. NIPC
B. FEDCIRC
C. CERT
D. CIAC

Answer: D

NEW QUESTION 168
- (Exam Topic 1)
When performing a forensics analysis, what device is used to prevent the system from recording data on an evidence disk?

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

Answer: A

NEW QUESTION 173
- (Exam Topic 1)
When using Windows acquisitions tools to acquire digital evidence, it is important to use a well-tested hardware write-blocking device to:

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

Answer: D

NEW QUESTION 175
- (Exam Topic 1)
What is the name of the Standard Linux Command that is also available as windows application that can be used to create bit-stream images?

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

Answer: D

NEW QUESTION 178
- (Exam Topic 1)
You are assigned to work in the computer forensics lab of a state police agency. While working on a high profile criminal case, you have followed every applicable procedure, however your boss is still concerned that the defense attorney might question whether evidence has been changed while at the lab. What can you do to prove that the evidence is the same as it was when it first entered the lab?

A. make an MD5 hash of the evidence and compare it with the original MD5 hash that was taken when the evidence first entered the lab
B. make an MD5 hash of the evidence and compare it to the standard database developed by NIST
C. there is no reason to worry about this possible claim because state labs are certified
D. sign a statement attesting that the evidence is the same as it was when it entered the lab

Answer: A

NEW QUESTION 180
- (Exam Topic 1)
Bill is the accounting manager for Grummon and Sons LLC in Chicago. On a regular basis, he needs to send PDF documents containing sensitive information through E-mail to his customers.
Bill protects the PDF documents with a password and sends them to their intended recipients. Why PDF passwords do not offer maximum protection?

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

Answer: A

NEW QUESTION 181
- (Exam Topic 1)
Which of the following refers to the data that might still exist in a cluster even though the original file has been overwritten by another file?

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

Answer: D

NEW QUESTION 185
- (Exam Topic 1)
This is original file structure database that Microsoft originally designed for floppy disks. It is written to the outermost track of a disk and contains information about each file stored on the drive.

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

Answer: C

NEW QUESTION 189
- (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 191
- (Exam Topic 1)
What header field in the TCP/IP protocol stack involves the hacker exploit known as the Ping of Death?

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

Answer: B

NEW QUESTION 196
- (Exam Topic 1)
An Expert witness give an opinion if:

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

Answer: A

NEW QUESTION 198
- (Exam Topic 4)
During a forensic investigation, a large number of files were collected. The investigator needs to evaluate ownership and accountability of those files. Therefore, he begins to Identify attributes such as "author name," "organization name." "network name," or any additional supporting data that is meant for the owner's Identification purpose. Which term describes these attributes?

A. Data header
B. Data index
C. Metabase
D. Metadata

Answer: D

NEW QUESTION 199
- (Exam Topic 4)
When Investigating a system, the forensics analyst discovers that malicious scripts were Injected Into benign and trusted websites. The attacker used a web application to send malicious code. In the form of a browser side script, to a different end-user. What attack was performed here?

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

Answer: C

NEW QUESTION 203
- (Exam Topic 4)
According to RFC 3227, which of the following is considered as the most volatile item on a typical system?

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

Answer: A

NEW QUESTION 206
- (Exam Topic 4)
This is a statement, other than one made by the declarant while testifying at the trial or hearing, offered in evidence to prove the truth of the matter asserted. Which among the following is suitable for the above statement?

A. Testimony by the accused
B. Limited admissibility
C. Hearsay rule
D. Rule 1001

Answer: C

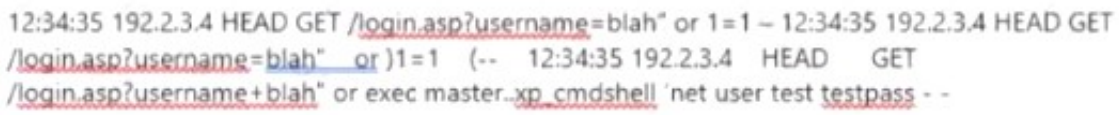
NEW QUESTION 208
- (Exam Topic 4)
During an Investigation. Noel found a SIM card from the suspect's mobile. The ICCID on the card is 8944245252001451548.
What does the first four digits (89 and 44) In the ICCID represent?

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 213
- (Exam Topic 4)

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



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

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

Answer: D

NEW QUESTION 214
- (Exam Topic 4)
Consider a scenario where a forensic investigator is performing malware analysis on a memory dump acquired from a victims computer. The investigator uses Volatility Framework to analyze RAM contents; which plugin helps investigator to identify hidden processes or injected code/DLL in the memory dump?

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

Answer: D

NEW QUESTION 218
- (Exam Topic 4)
Which of the following statements is true with respect to SSDs (solid-state drives)?

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

Answer: D

NEW QUESTION 221
- (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 223
- (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)|>)/Ix. 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 228
- (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 229

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

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

Answer: A

NEW QUESTION 234
- (Exam Topic 4)
Which of the following statements pertaining to First Response is true?

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

Answer: A

NEW QUESTION 235
- (Exam Topic 4)
Ronald, a forensic investigator, has been hired by a financial services organization to Investigate an attack on their MySQL database server, which Is hosted on a Windows machine named WIN-DTRAI83202X. Ronald wants to retrieve information on the changes that have been made to the database. Which of the following files should Ronald examine for this task?

A. relay-log.info
B. WIN-DTRAl83202Xrelay-bin.index
C. WIN-DTRAI83202Xslow.log
D. WIN-DTRAI83202X-bin.nnnnnn

Answer: C

NEW QUESTION 240
- (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 244
- (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 248
- (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 249
- (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 254
- (Exam Topic 4)
Assume there Is a file named myflle.txt In C: drive that contains hidden data streams. Which of the following commands would you Issue to display the contents of a data stream?

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

Answer: A

NEW QUESTION 256
- (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. Iocal/sha re/Trash
C. Drive:\RECYCLER\
D. DriveARECYCLED

Answer: C

NEW QUESTION 257
- (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 261
- (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 262
- (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 266
- (Exam Topic 4)
When installed on a Windows machine, which port does the Tor browser use to establish a network connection via Tor nodes?

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

Answer: C

NEW QUESTION 267
- (Exam Topic 4)
Chloe is a forensic examiner who is currently cracking hashed passwords for a crucial mission and hopefully solve the case. She is using a lookup table used for recovering a plain text password from cipher text; it contains word list and brute-force list along with their computed hash values. Chloe Is also using a graphical generator that supports SHA1.
* a. What password technique is being used?
* b. What tool is Chloe using?

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

Answer: D

NEW QUESTION 268
- (Exam Topic 4)
Edgar is part of the FBI's forensic media and malware analysis team; he Is analyzing a current malware and Is conducting a thorough examination of the suspect system, network, and other connected devices. Edgar's approach Is to execute the malware code to know how It Interacts with the host system and Its Impacts on It. He is also using a virtual machine and a sandbox environment.
What type of malware analysis is Edgar performing?

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

Answer: D

NEW QUESTION 269
- (Exam Topic 4)
Consider a scenario where the perpetrator of a dark web crime has unInstalled Tor browser from their computer after committing the crime. The computer has been seized by law enforcement so they can Investigate It for artifacts of Tor browser usage. Which of the following should the Investigators examine to establish the use of Tor browser on the suspect machine?

A. Swap files
B. Files in Recycle Bin
C. Security logs
D. Prefetch files

Answer: A

NEW QUESTION 271
- (Exam Topic 4)
SO/IEC 17025 is an accreditation for which of the following:

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

Answer: C

NEW QUESTION 275
- (Exam Topic 4)
Which of the following attacks refers to unintentional download of malicious software via the Internet? Here, an attacker exploits flaws in browser software to install malware merely by the user visiting the malicious website.

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

Answer: C

NEW QUESTION 278

- (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 Wlreshark 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 283
- (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 287
- (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 292
- (Exam Topic 4)
Place the following In order of volatility from most volatile to the least volatile.

A. Registers and cache, routing tables, temporary file systems, disk storage, archival media
B. Register and cache, temporary file systems, routing tables, disk storage, archival media
C. Registers and cache, routing tables, temporary file systems, archival media, disk storage
D. Archival media, temporary file systems, disk storage, archival media, register and cache

Answer: B

NEW QUESTION 297
- (Exam Topic 4)
In which loT attack does the attacker use multiple forged identities to create a strong illusion of traffic congestion, affecting communication between neighboring nodes and networks?

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

Answer: D

NEW QUESTION 298
- (Exam Topic 4)
Steve received a mail that seemed to have come from her bank. The mail has instructions for Steve to click on a link and provide information to avoid the suspension of her account. The link in the mail redirected her to a form asking for details such as name, phone number, date of birth, credit card number or PIN, CW code, SNNs, and email address. On a closer look, Steve realized that the URL of the form in not the same as that of her bank's. Identify the type of external attack performed by the attacker In the above scenario?

A. Aphishing
B. Espionage
C. Taiigating
D. Brute-force

Answer: A

NEW QUESTION 301
- (Exam Topic 4)
To understand the impact of a malicious program after the booting process and to collect recent information from the disk partition, an Investigator should evaluate

the content of the:

A. MBR
B. GRUB
C. UEFI
D. BIOS

Answer: A

NEW QUESTION 303
- (Exam Topic 3)
In a computer that has Dropbox client installed, which of the following files related to the Dropbox client store information about local Dropbox installation and the Dropbox user account, along with email IDs linked with the account?

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

Answer: A

NEW QUESTION 308
- (Exam Topic 3)
Which of the following standard represents a legal precedent regarding the admissibility of scientific examinations or experiments in legal cases?

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

Answer: C

NEW QUESTION 310
- (Exam Topic 3)
Which principle states that “anyone or anything, entering a crime scene takes something of the scene with them, and leaves something of themselves behind when they leave”?

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

Answer: A

NEW QUESTION 313
- (Exam Topic 3)
Tasklist command displays a list of applications and services with their Process ID (PID) for all tasks running on either a local or a remote computer. Which of the following tasklist commands provides information about the listed processes, including the image name, PID, name, and number of the session for the process?

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

Answer: B

NEW QUESTION 316
- (Exam Topic 3)
Select the data that a virtual memory would store in a Windows-based system.

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

Answer: D

NEW QUESTION 320
- (Exam Topic 3)
Which of the following file system uses Master File Table (MFT) database to store information about every file and directory on a volume?

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

Answer: D

NEW QUESTION 321
- (Exam Topic 3)
What technique is used by JPEGs for compression?

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

Answer: C

NEW QUESTION 325
- (Exam Topic 3)
Buffer overflow vulnerability of a web application occurs when it fails to guard its buffer properly and allows writing beyond its maximum size. Thus, it overwrites the . There are multiple forms of buffer overflow, including a Heap Buffer Overflow and a Format String Attack.

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

Answer: A

NEW QUESTION 327
- (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 330
- (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 334
- (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 335
- (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 338
- (Exam Topic 3)
What is cold boot (hard boot)?

A. It is the process of restarting a computer that is already in sleep mode
B. It is the process of shutting down a computer from a powered-on or on state

C. It is the process of restarting a computer that is already turned on through the operating system
D. It is the process of starting a computer from a powered-down or off state

Answer: D

NEW QUESTION 341
- (Exam Topic 3)
Joshua is analyzing an MSSQL database for finding the attack evidence and other details, where should he look for the database logs?

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

Answer: C

NEW QUESTION 342
- (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

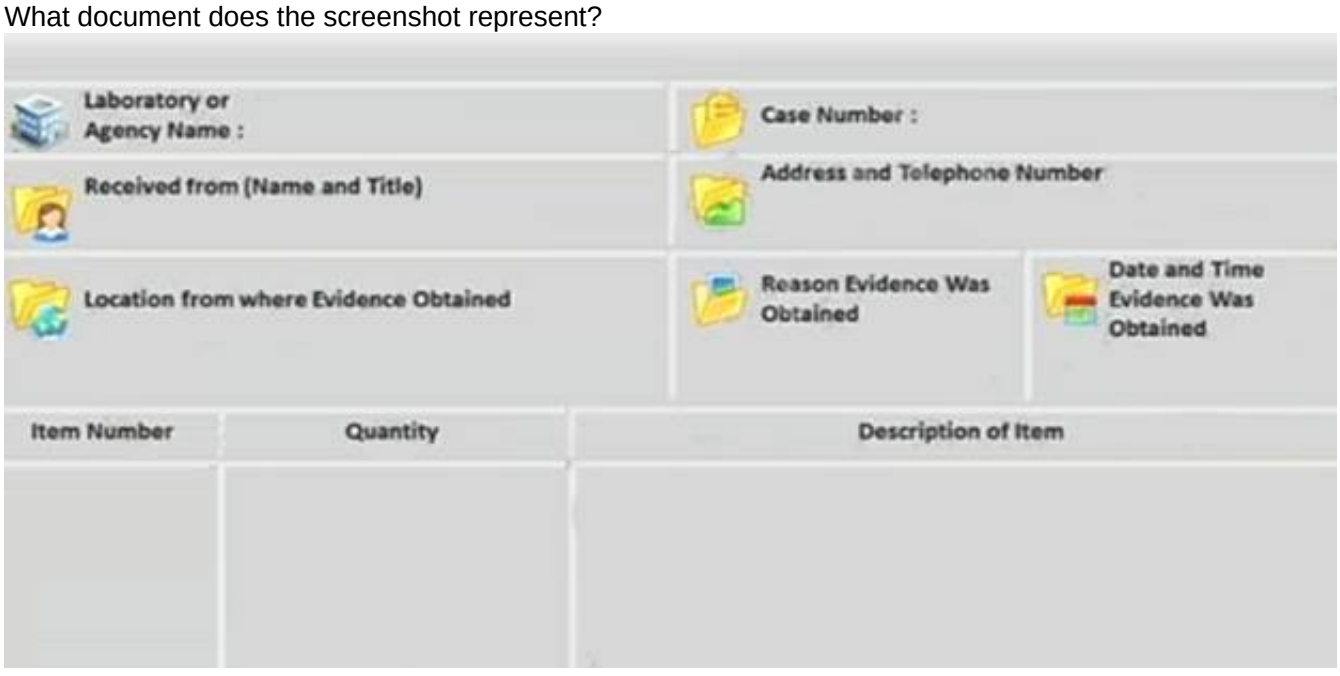
Answer: A

NEW QUESTION 344
- (Exam Topic 3)
An International Mobile Equipment Identifier (IMEI) is a 15-digit number that indicates the manufacturer, model type, and country of approval for GSM devices. The first eight digits of an IMEI number that provide information about the model and origin of the mobile device is also known as:

A. Type Allocation Code (TAC)
B. Integrated Circuit Code (ICC)
C. Manufacturer Identification Code (MIC)
D. Device Origin Code (DOC)

Answer: A

NEW QUESTION 346
- (Exam Topic 3)
What document does the screenshot represent?



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

Answer: D

NEW QUESTION 350
- (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 355
- (Exam Topic 3)
Which of the following tool is used to locate IP addresses?

A. SmartWhois
B. Deep Log Analyzer
C. Towelroot
D. XRY LOGICAL

Answer: A

NEW QUESTION 356
- (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 358
- (Exam Topic 3)
Which program uses different techniques to conceal a malware's code, thereby making it difficult for security mechanisms to detect or remove it?

A. Dropper
B. Packer
C. Injector
D. Obfuscator

Answer: D

NEW QUESTION 361
- (Exam Topic 3)
What malware analysis operation can the investigator perform using the jv16 tool?

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

Answer: D

NEW QUESTION 363
- (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 366
- (Exam Topic 3)
Which type of attack is possible when attackers know some credible information about the victim's password, such as the password length, algorithms involved, or the strings and characters used in its creation?

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

Answer: A

NEW QUESTION 371
- (Exam Topic 3)

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

A. Email spamming
B. Phishing
C. Email spoofing
D. Mail bombing

Answer: D

NEW QUESTION 376
- (Exam Topic 3)
Which of the following is a tool to reset Windows admin password?

A. R-Studio
B. Windows Password Recovery Bootdisk
C. Windows Data Recovery Software
D. TestDisk for Windows

Answer: B

NEW QUESTION 377
- (Exam Topic 3)
What is the name of the first reserved sector in File allocation table?

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

Answer: C

NEW QUESTION 379
- (Exam Topic 3)
An investigator enters the command sqlcmd -S WIN-CQQMK62867E -e -s"," -E as part of collecting the primary data file and logs from a database. What does the "WIN-CQQMK62867E" represent?

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

Answer: B

NEW QUESTION 380
- (Exam Topic 3)
MAC filtering is a security access control methodology, where a is assigned to each network card to determine access to the network.

A. 48-bit address
B. 24-bit address
C. 16-bit address
D. 32-bit address

Answer: A

NEW QUESTION 384
- (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 386
- (Exam Topic 3)
Which command can provide the investigators with details of all the loaded modules on a Linux-based system?

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

Answer: B

NEW QUESTION 388
- (Exam Topic 3)
Which of the following tool can reverse machine code to assembly language?

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

Answer: C

NEW QUESTION 391
- (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 394
- (Exam Topic 3)
Consider that you are investigating a machine running an Windows OS released prior to Windows Vista. You are trying to gather information about the deleted files by examining the master database file named INFO2 located at C:\Recycler\<USER SID>\. You read an entry named "Dd5.exe". What does Dd5.exe mean?

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

Answer: B

NEW QUESTION 399
- (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 402
- (Exam Topic 3)
During an investigation, Noel found the following SIM card from the suspect's mobile. What does the code 89 44 represent?

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

Answer: B

NEW QUESTION 405
- (Exam Topic 3)
Which of the following setups should a tester choose to analyze malware behavior?

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

Answer: D

NEW QUESTION 409
- (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 414
- (Exam Topic 3)
What do you call the process in which an attacker uses magnetic field over the digital media device to delete any previously stored data?

A. Disk deletion
B. Disk cleaning
C. Disk degaussing
D. Disk magnetization

Answer: C

NEW QUESTION 419
- (Exam Topic 3)
Which among the following search warrants allows the first responder to search and seize the victim’s computer components such as hardware, software, storage devices, and documentation?

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

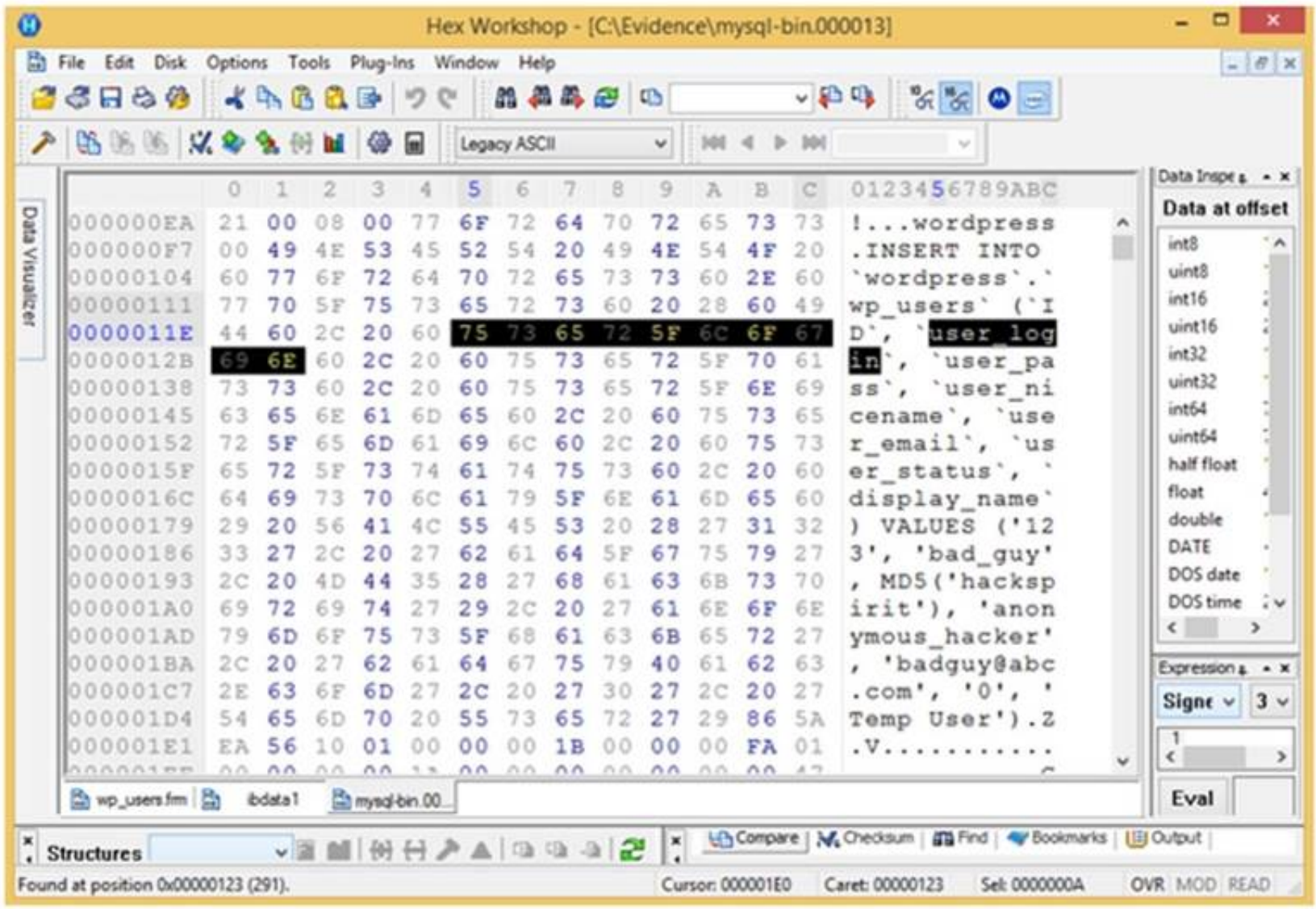
Answer: C

NEW QUESTION 421
- (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 426
- (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 427
- (Exam Topic 3)
Which of the following statements is true regarding SMTP Server?

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

Answer: C

NEW QUESTION 432
- (Exam Topic 3)
What is the role of Alloc.c in Apache core?

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

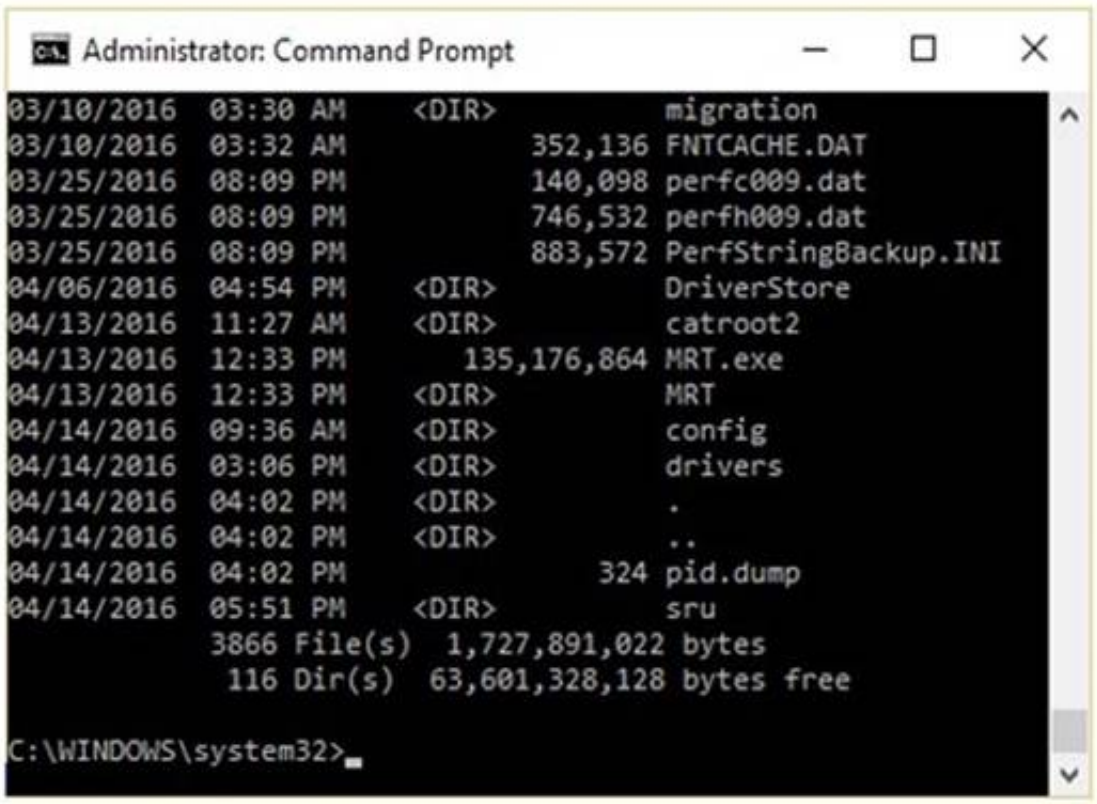
Answer: A

NEW QUESTION 436
- (Exam Topic 3)
You are working as an independent computer forensics investigator and received a call from a systems administrator for a local school system requesting your assistance. One of the students at the local high school is suspected of downloading inappropriate images from the Internet to a PC in the Computer Lab. When you arrive at the school, the systems administrator hands you a hard drive and tells you that he made a "simple backup copy" of the hard drive in the PC and put it on this drive and requests that you examine the drive for evidence of the suspected images. You inform him that a "simple backup copy" will not provide deleted files or recover file fragments. What type of copy do you need to make to ensure that the evidence found is complete and admissible in future proceeding?

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

Answer: C

NEW QUESTION 438
- (Exam Topic 3)
The given image displays information about date and time of installation of the OS along with service packs, patches, and sub-directories. What command or tool did the investigator use to view this output?



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

Answer: A

NEW QUESTION 440
- (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 441
- (Exam Topic 3)
The MAC attributes are timestamps that refer to a time at which the file was last modified or last accessed or originally created. Which of the following file systems store MAC attributes in Coordinated Universal Time (UTC) format?

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

Answer: B

NEW QUESTION 443
- (Exam Topic 3)
Event correlation is the process of finding relevance between the events that produce a final result. What type of correlation will help an organization to correlate events across a set of servers, systems, routers and network?

A. Same-platform correlation
B. Network-platform correlation
C. Cross-platform correlation
D. Multiple-platform correlation

Answer: C

NEW QUESTION 447
- (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 451
- (Exam Topic 3)
Which of the following techniques delete the files permanently?

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

Answer: B

NEW QUESTION 453
- (Exam Topic 3)
As a part of the investigation, Caroline, a forensic expert, was assigned the task to examine the transaction logs pertaining to a database named Transfers. She used SQL Server Management Studio to collect the active transaction log files of the database. Caroline wants to extract detailed information on the logs, including AllocUnitId, page id, slot id, etc. Which of the following commands does she need to execute in order to extract the desired information?

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

Answer: D

NEW QUESTION 455
- (Exam Topic 3)
Which of these ISO standards define the file system for optical storage media, such as CD-ROM and DVD-ROM?

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

Answer: A

NEW QUESTION 460
- (Exam Topic 3)
Which of the following statements is TRUE about SQL Server error logs?

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

Answer: B

NEW QUESTION 464
- (Exam Topic 3)
In both pharming and phishing attacks an attacker can create websites that look similar to legitimate sites with the intent of collecting personal identifiable information from its victims. What is the difference between pharming and phishing attacks?

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

Answer: B

NEW QUESTION 468
- (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 471
- (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 474
- (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 475
- (Exam Topic 2)
Billy, a computer forensics expert, has recovered a large number of DBX files during the forensic investigation of a laptop. Which of the following email clients can he use to analyze the DBX files?

A. Microsoft Outlook
B. Eudora
C. Mozilla Thunderbird
D. Microsoft Outlook Express

Answer: D

NEW QUESTION 480
- (Exam Topic 2)
When a router receives an update for its routing table, what is the metric value change to that path?

A. Increased by 2
B. Decreased by 1
C. Increased by 1
D. Decreased by 2

Answer: C

NEW QUESTION 481
- (Exam Topic 2)
After attending a CEH security seminar, you make a list of changes you would like to perform on your network to increase its security. One of the first things you change is to switch the RestrictAnonymous setting from 0 to 1 on your servers. This, as you were told, would prevent anonymous users from establishing a null session on the server. Using Userinfo tool mentioned at the seminar, you succeed in establishing a null session with one of the servers. Why is that?

A. RestrictAnonymous must be set to "10" for complete security
B. RestrictAnonymous must be set to "3" for complete security
C. RestrictAnonymous must be set to "2" for complete security
D. There is no way to always prevent an anonymous null session from establishing

Answer: C

NEW QUESTION 486
- (Exam Topic 2)
How will you categorize a cybercrime that took place within a CSP’s cloud environment?

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

Answer: D

NEW QUESTION 488
- (Exam Topic 2)
What will the following Linux command accomplish? dd if=/dev/mem of=/home/sam/mem.bin bs=1024

A. Copy the master boot record to a file
B. Copy the contents of the system folder to a file
C. Copy the running memory to a file

D. Copy the memory dump file to an image file

Answer: C

NEW QUESTION 489
- (Exam Topic 2)
Which program is the bootloader when Windows XP starts up?

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

Answer: B

NEW QUESTION 494
- (Exam Topic 2)

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

Answer: B

NEW QUESTION 498
- (Exam Topic 2)
On an Active Directory network using NTLM authentication, where on the domain controllers are the passwords stored?

A. SAM
B. AMS
C. Shadow file
D. Password.conf

Answer: A

NEW QUESTION 499
- (Exam Topic 2)
Davidson Trucking is a small transportation company that has three local offices in Detroit Michigan. Ten female employees that work for the company have gone to an attorney reporting that male employees repeatedly harassed them and that management did nothing to stop the problem. Davidson has employee policies that outline all company guidelines, including awareness on harassment and how it will not be tolerated. When the case is brought to court, whom should the prosecuting attorney call upon for not upholding company policy?

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

Answer: C

NEW QUESTION 501
- (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 503
- (Exam Topic 2)
Which of the following techniques can be used to beat steganography?

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

Answer: B

NEW QUESTION 508

- (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 511
- (Exam Topic 2)
Smith, a network administrator with a large MNC, was the first to arrive at a suspected crime scene involving criminal use of compromised computers. What should be his first response while maintaining the integrity of evidence?

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

Answer: A

NEW QUESTION 514
- (Exam Topic 2)
What feature of Decryption Collection allows an investigator to crack a password as quickly as possible?

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

Answer: B

NEW QUESTION 515
- (Exam Topic 2)
When investigating a wireless attack, what information can be obtained from the DHCP logs?

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

Answer: C

NEW QUESTION 516
- (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 517
- (Exam Topic 2)
Why would you need to find out the gateway of a device when investigating a wireless attack?

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

Answer: D

NEW QUESTION 518
- (Exam Topic 2)
The surface of a hard disk consists of several concentric rings known as tracks; each of these tracks has smaller partitions called disk blocks. What is the size of each block?

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

Answer: B

NEW QUESTION 520
- (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

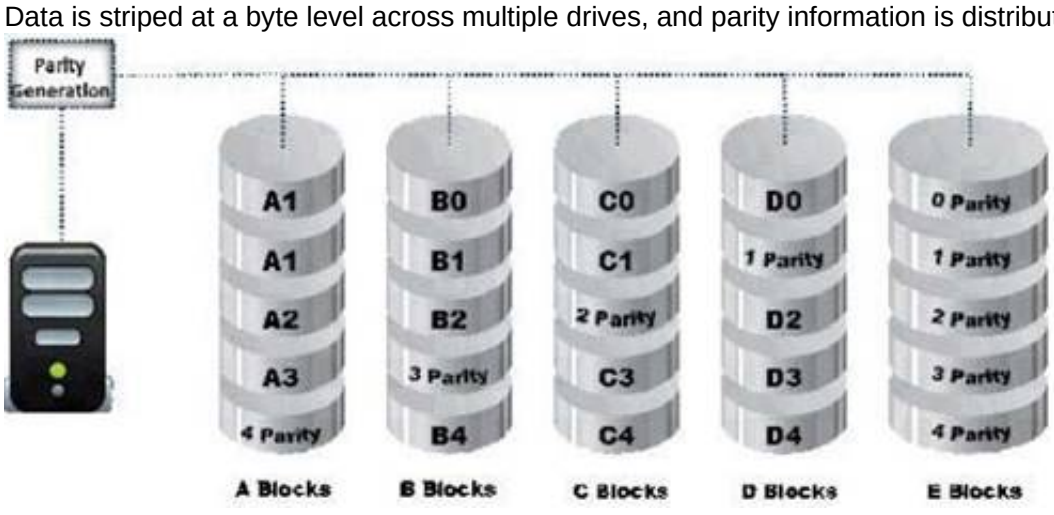
Answer: D

NEW QUESTION 524
- (Exam Topic 2)
You have been given the task to investigate web attacks on a Windows-based server. Which of the following commands will you use to look at the sessions the machine has opened with other systems?

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

Answer: D

NEW QUESTION 525
- (Exam Topic 2)
Data is striped at a byte level across multiple drives, and parity information is distributed among all member drives.



What RAID level is represented here?

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

Answer: B

NEW QUESTION 528
- (Exam Topic 2)
What hashing method is used to password protect Blackberry devices?

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

Answer: D

NEW QUESTION 533
- (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 537
- (Exam Topic 2)
A small law firm located in the Midwest has possibly been breached by a computer hacker looking to obtain information on their clientele. The law firm does not

have any on-site IT employees, but wants to search for evidence of the breach themselves to prevent any possible media attention. Why would this not be recommended?

A. Searching for evidence themselves would not have any ill effects
B. Searching could possibly crash the machine or device
C. Searching creates cache files, which would hinder the investigation
D. Searching can change date/time stamps

Answer: D

NEW QUESTION 539
- (Exam Topic 2)
Why would a company issue a dongle with the software they sell?

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

Answer: C

NEW QUESTION 540
- (Exam Topic 2)
What layer of the OSI model do TCP and UDP utilize?

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

Answer: C

NEW QUESTION 543
- (Exam Topic 2)
Which forensic investigating concept trails the whole incident from how the attack began to how the victim was affected?

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

Answer: B

NEW QUESTION 547
- (Exam Topic 2)
Which among the following search warrants allows the first responder to get the victim’s computer information such as service records, billing records, and subscriber information from the service provider?

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

Answer: B

NEW QUESTION 551
- (Exam Topic 2)
Which of the following commands shows you all of the network services running on Windows-based servers?

A. Netstart
B. Net Session
C. Net use
D. Net config

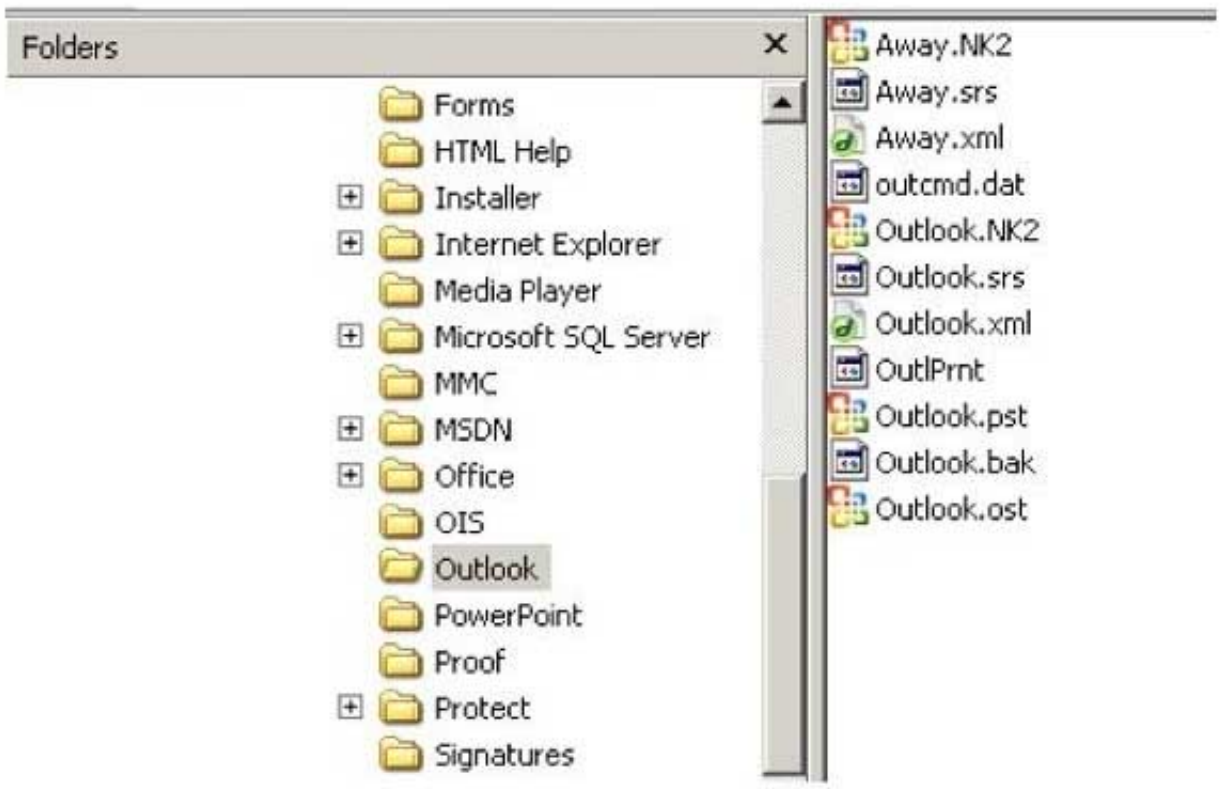
Answer: A

NEW QUESTION 553
- (Exam Topic 2)
When should an MD5 hash check be performed when processing evidence?

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

Answer: C

NEW QUESTION 558
- (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 560
- (Exam Topic 2)
Which network attack is described by the following statement? "At least five Russian major banks came under a continuous hacker attack, although online client services were not disrupted. The attack came from a wide-scale botnet involving at least 24,000 computers, located in 30 countries."

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

Answer: D

NEW QUESTION 563
- (Exam Topic 2)
What is the slave device connected to the secondary IDE controller on a Linux OS referred to?

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

Answer: B

NEW QUESTION 568
- (Exam Topic 2)
Which of the following files stores information about local Dropbox installation and account, email IDs linked with the account, current version/build for the local application, the host_id, and local path information?

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

Answer: C

NEW QUESTION 573
- (Exam Topic 2)
Jason discovered a file named $RIYG6VR.doc in the C:\$Recycle.Bin\<USER SID>\ while analyzing a hard disk image for the deleted data. What inferences can he make from the file name?

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

D. It is a deleted doc file

Answer: D

NEW QUESTION 576
- (Exam Topic 2)
Why should you never power on a computer that you need to acquire digital evidence from?

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

Answer: A

NEW QUESTION 581
- (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 586
- (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 589
- (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 594
- (Exam Topic 2)
What file is processed at the end of a Windows XP boot to initialize the logon dialog box?

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

Answer: A

NEW QUESTION 596
- (Exam Topic 2)
Paul is a computer forensics investigator working for Tyler & Company Consultants. Paul has been called upon to help investigate a computer hacking ring broken up by the local police. Paul begins to inventory the
PCs found in the hackers hideout. Paul then comes across a PDA left by them that is attached to a number of different peripheral devices. What is the first step that Paul must take with the PDA to ensure the integrity of the investigation?

A. Place PDA, including all devices, in an antistatic bag
B. Unplug all connected devices
C. Power off all devices if currently on
D. Photograph and document the peripheral devices

Answer: D

NEW QUESTION 599

- (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 600
- (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 605
- (Exam Topic 2)
Which of the following tool creates a bit-by-bit image of an evidence media?

A. Recuva
B. FileMerlin
C. AccessData FTK Imager
D. Xplico

Answer: C

NEW QUESTION 609
- (Exam Topic 2)
Madison is on trial for allegedly breaking into her university internal network. The police raided her dorm room and seized all of her computer equipment. Madison lawyer is trying to convince the judge that the
seizure was unfounded and baseless. Under which US Amendment is Madison lawyer trying to prove the police violated?

A. The 10th Amendment
B. The 5th Amendment
C. The 1st Amendment
D. The 4th Amendment

Answer: D

NEW QUESTION 612
- (Exam Topic 2)
The following is a log file screenshot from a default installation of IIS 6.0.

```
#Software: Microsoft Internet Information Services 6.0
#Version: 1.0
#Date: 2007-01-22 15:42:36
#Fields: date time s-sitename s-ip cs-method cs-uri-stem cs-uri-query s-port cs-user
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /index.html - 80 - 172.16.28.80
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /Development/index.asp - 80 - 172.16.28
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /Development/css/olcstyle.css - 80 - 17
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /favicon.ico - 80 - 172.16.28.80 Avant+
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /Development/css/dhtml_horiz.css - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /Development/images/index_01.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /Development/images/index_02.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /Development/images/index_03.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /Development/images/index_04.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /Development/images/index_06.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /Development/images/index_07.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /Development/images/index_08.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /Development/script/dhtml.js - 80 - 172
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /Development/images/greenArraw.jpg - 80
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /Development/images/board_01.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /Development/images/board_02.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
```

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

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

Answer: A

NEW QUESTION 617
- (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 620
- (Exam Topic 2)
Files stored in the Recycle Bin in its physical location are renamed as Dxy.ext, where “x” represents the _____.

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

Answer: A

NEW QUESTION 625
- (Exam Topic 2)
Heather, a computer forensics investigator, is assisting a group of investigators working on a large computer fraud case involving over 20 people. These 20 people, working in different offices, allegedly siphoned off money from many different client accounts. Heather responsibility is to find out how the accused people communicated between each other. She has searched their email and their computers and has not found any useful evidence. Heather then finds some possibly useful evidence under the desk of one of the accused.
In an envelope she finds a piece of plastic with numerous holes cut out of it. Heather then finds the same exact piece of plastic with holes at many of the other accused peoples desks. Heather believes that the 20 people involved in the case were using a cipher to send secret messages in between each other. What type of cipher was used by the accused in this case?

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

Answer: A

NEW QUESTION 629
- (Exam Topic 2)
Why is it still possible to recover files that have been emptied from the Recycle Bin on a Windows computer?

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

Answer: A

NEW QUESTION 632
- (Exam Topic 2)
Watson, a forensic investigator, is examining a copy of an ISO file stored in CDFS format. What type of evidence is this?

A. Data from a CD copied using Windows
B. Data from a CD copied using Mac-based system
C. Data from a DVD copied using Windows system
D. Data from a CD copied using Linux system

Answer: A

NEW QUESTION 633
- (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 638
- (Exam Topic 2)
Before performing a logical or physical search of a drive in Encase, what must be added to the program?

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

Answer: B

NEW QUESTION 641
- (Exam Topic 2)
Microsoft Security IDs are available in Windows Registry Editor. The path to locate IDs in Windows 7 is:

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

Answer: A

NEW QUESTION 646
.....

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