Exam Questions 312-49v10

Computer Hacking Forensic Investigator (CHFI-v10)

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

NEW QUESTION 1
- (Exam Topic 1)
You are the security analyst working for a private company out of France. Your current assignment is to obtain credit card information from a Swiss bank owned by that company. After initial reconnaissance, you discover that the bank security defenses are very strong and would take too long to penetrate. You decide to get the information by monitoring the traffic between the bank and one of its subsidiaries in London. After monitoring some of the traffic, you see a lot of FTP packets traveling back and forth. You want to sniff the traffic and extract usernames and passwords. What tool could you use to get this information?

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

Answer: C

NEW QUESTION 2
- (Exam Topic 1)
While working for a prosecutor, what do you think you should do if the evidence you found appears to be exculpatory and is not being released to the defense?

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

Answer: C

NEW QUESTION 3
- (Exam Topic 1)
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 4
- (Exam Topic 1)
In a forensic examination of hard drives for digital evidence, what type of user is most likely to have the most file slack to analyze?

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

Answer: D

NEW QUESTION 5
- (Exam Topic 1)
Law enforcement officers are conducting a legal search for which a valid warrant was obtained.
While conducting the search, officers observe an item of evidence for an unrelated crime that was not included in the warrant. The item was clearly visible to the officers and immediately identified as evidence. What is the term used to describe how this evidence is admissible?

A. Plain view doctrine
B. Corpus delicti
C. Locard Exchange Principle
D. Ex Parte Order

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)
You have completed a forensic investigation case. You would like to destroy the data contained in various disks at the forensics lab due to sensitivity of the case. How would you permanently erase the data on the hard disk?

A. Throw the hard disk into the fire
B. Run the powerful magnets over the hard disk
C. Format the hard disk multiple times using a low level disk utility
D. Overwrite the contents of the hard disk with Junk data

Answer: A

NEW QUESTION 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)
Area density refers to:

A. the amount of data per disk
B. the amount of data per partition
C. the amount of data per square inch
D. the amount of data per platter

Answer: A

NEW QUESTION 10
- (Exam Topic 1)
An employee is attempting to wipe out data stored on a couple of compact discs (CDs) and digital video discs (DVDs) by using a large magnet. You inform him that this method will not be effective in wiping out the data because CDs and DVDs are _____ media used to store large amounts of data and are not affected by the magnet.

A. logical
B. anti-magnetic
C. magnetic
D. optical

Answer: D

NEW QUESTION 12
- (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 16
- (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 18
- (Exam Topic 2)
What stage of the incident handling process involves reporting events?

A. Containment
B. Follow-up
C. Identification
D. Recovery

Answer: C

NEW QUESTION 23
- (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 24
- (Exam Topic 1)
An "idle" system is also referred to as what?

A. PC not connected to the Internet
B. Zombie
C. PC not being used
D. Bot

Answer: B

NEW QUESTION 25
- (Exam Topic 1)
Software firewalls work at which layer of the OSI model?

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

Answer: D

NEW QUESTION 30
- (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 31
- (Exam Topic 1)
What will the following command accomplish?

A. Test ability of a router to handle over-sized packets
B. Test the ability of a router to handle under-sized packets
C. Test the ability of a WLAN to handle fragmented packets
D. Test the ability of a router to handle fragmented packets

Answer: A

NEW QUESTION 32
- (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 34
- (Exam Topic 1)
If an attacker's computer sends an IPID of 31400 to a zombie computer on an open port in IDLE scanning, what will be the response?

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

Answer: D

NEW QUESTION 36
- (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 41
- (Exam Topic 1)
You are assisting a Department of Defense contract company to become compliant with the stringent security policies set by the DoD. One such strict rule is that firewalls must only allow incoming connections that were first initiated by internal computers. What type of firewall must you implement to abide by this policy?

A. Packet filtering firewall
B. Circuit-level proxy firewall
C. Application-level proxy firewall
D. Stateful firewall

Answer: D

NEW QUESTION 45
- (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 49
- (Exam Topic 1)
When examining a hard disk without a write-blocker, you should not start windows because Windows will write data to the:

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

Answer: A

NEW QUESTION 51
- (Exam Topic 1)
What method of computer forensics will allow you to trace all ever-established user accounts on a Windows 2000 sever the course of its lifetime?

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

Answer: C

NEW QUESTION 55
- (Exam Topic 1)
In the context of file deletion process, which of the following statement holds true?

A. When files are deleted, the data is overwritten and the cluster marked as available
B. The longer a disk is in use, the less likely it is that deleted files will be overwritten
C. While booting, the machine may create temporary files that can delete evidence
D. Secure delete programs work by completely overwriting the file in one go

Answer: C

NEW QUESTION 57
- (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 58
- (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 63
- (Exam Topic 1)
_____ is simply the application of Computer Investigation and analysis techniques in the interests of determining potential legal evidence.

A. Network Forensics
B. Computer Forensics
C. Incident Response
D. Event Reaction

Answer: B

NEW QUESTION 68
- (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 73
- (Exam Topic 1)
You are conducting an investigation of fraudulent claims in an insurance company that involves complex text searches through large numbers of documents.
Which of the following tools would allow you to quickly and efficiently search for a string within a file on the bitmap image of the target computer?

A. Stringsearch
B. grep
C. dir
D. vim

Answer: B

NEW QUESTION 76
- (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 80
- (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 81
- (Exam Topic 1)
Office Documents (Word, Excel and PowerPoint) contain a code that allows tracking the MAC or unique identifier of the machine that created the document. What is that code called?

A. Globally unique ID
B. Microsoft Virtual Machine Identifier
C. Personal Application Protocol
D. Individual ASCII string

Answer: A

NEW QUESTION 83
- (Exam Topic 1)
A honey pot deployed with the IP 172.16.1.108 was compromised by an attacker. Given below is an excerpt from a Snort binary capture of the attack. Decipher the activity carried out by the attacker by studying the log. Please note that you are required to infer only what is explicit in the excerpt.
(Note: The student is being tested on concepts learnt during passive OS fingerprinting, basic TCP/IP connection concepts and the ability to read packet signatures from a sniff dump.)
03/15-20:21:24.107053 211.185.125.124:3500 -> 172.16.1.108:111
TCP TTL:43 TOS:0x0 ID:29726 IpLen:20 DgmLen:52 DF
A* Seq: 0x9B6338C5 Ack: 0x5820ADD0 Win: 0x7D78 TcpLen: 32 TCP Options (3) => NOP NOP TS: 23678634 2878772
=+= 03/15-20:21:24.452051 211.185.125.124:789 -> 172.16.1.103:111
UDP TTL:43 TOS:0x0 ID:29733 IpLen:20 DgmLen:84
Len: 64
01 0A 8A 0A 00 00 00 00 00 00 00 02 00 01 86 A0 ....
00 00 00 02 00 00 00 03 00 00 00 00 00 00 00 00 ....
00 00 00 00 00 00 00 00 00 01 86 B8 00 00 00 01 ....
00 00 00 11 00 00 00 00 ....
=+= 03/15-20:21:24.730436 211.185.125.124:790 ->
172.16.1.103:32773
UDP TTL:43 TOS:0x0 ID:29781 IpLen:20 DgmLen:1104 Len: 1084
47 F7 9F 63 00 00 00 00 00 00 00 02 00 01 86 B8

A. The attacker has conducted a network sweep on port 111
B. The attacker has scanned and exploited the system using Buffer Overflow
C. The attacker has used a Trojan on port 32773
D. The attacker has installed a backdoor

Answer: A

NEW QUESTION 87
- (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 91
- (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 96
- (Exam Topic 1)
Volatile Memory is one of the leading problems for forensics. Worms such as code Red are memory resident and do write themselves to the hard drive, if you turn the system off they disappear. In a lab environment, which of the following options would you suggest as the most appropriate to overcome the problem of capturing volatile memory?

A. Use VMware to be able to capture the data in memory and examine it
B. Give the Operating System a minimal amount of memory, forcing it to use a swap file
C. Create a Separate partition of several hundred megabytes and place the swap file there
D. Use intrusion forensic techniques to study memory resident infections

Answer: C

NEW QUESTION 97
- (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 99
- (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 104
- (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 109
- (Exam Topic 1)
In what way do the procedures for dealing with evidence in a criminal case differ from the procedures for dealing with evidence in a civil case?

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

Answer: C

NEW QUESTION 112
- (Exam Topic 1)
When examining a file with a Hex Editor, what space does the file header occupy?

A. the last several bytes of the file
B. the first several bytes of the file

C. none, file headers are contained in the FAT
D. one byte at the beginning of the file

Answer: D

NEW QUESTION 117

- (Exam Topic 1)
When examining the log files from a Windows IIS Web Server, how often is a new log file created?

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

Answer: A

NEW QUESTION 119

- (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 123

- (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 125

- (Exam Topic 1)
What is a good security method to prevent unauthorized users from "tailgating"?

A. Man trap
B. Electronic combination locks
C. Pick-resistant locks
D. Electronic key systems

Answer: A

NEW QUESTION 128

- (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 129

- (Exam Topic 1)
You are running known exploits against your network to test for possible vulnerabilities. To test the strength of your virus software, you load a test network to mimic your production network. Your software successfully blocks some simple macro and encrypted viruses. You decide to really test the software by using virus code where the code rewrites itself entirely and the signatures change from child to child, but the functionality stays the same. What type of virus is this that you are testing?

A. Polymorphic
B. Metamorphic
C. Oligomorhic
D. Transmorphic

Answer: B

NEW QUESTION 132
- (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 134
- (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 135
- (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 140
- (Exam Topic 1)
Which response organization tracks hoaxes as well as viruses?

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

Answer: D

NEW QUESTION 144
- (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 146
- (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 148
- (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 152
- (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 157
- (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 158
- (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 161
- (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 165
- (Exam Topic 1)
With the standard Linux second extended file system (Ext2fs), a file is deleted when the inode internal link count reaches .

A. 10
B. 100
C. 1

Answer: A

NEW QUESTION 168
- (Exam Topic 1)
Kyle is performing the final testing of an application he developed for the accounting department. His last round of testing is to ensure that the program is as secure as possible. Kyle runs the following
command. What is he testing at this point?
#include #include int main(int argc, char
*argv[]) { char buffer[10]; if (argc < 2) { fprintf (stderr, "USAGE: %s string\n", argv[0]); return 1; } strcpy(buffer, argv[1]); return 0; }

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

Answer: A

NEW QUESTION 173
- (Exam Topic 1)
You just passed your ECSA exam and are about to start your first consulting job running security audits for a financial institution in Los Angeles. The IT manager of the company you will be working for tries to see if you remember your ECSA class. He asks about the methodology you will be using to test the company's network. How would you answer?

A. Microsoft Methodology
B. Google Methodology
C. IBM Methodology
D. LPT Methodology

Answer: D

NEW QUESTION 176
- (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 181
- (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 184
- (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 188
- (Exam Topic 4)
An investigator seized a notebook device installed with a Microsoft Windows OS. Which type of files would support an investigation of the data size and structure in the device?

A. Ext2 and Ext4
B. APFSandHFS
C. HFS and GNUC
D. NTFSandFAT

Answer: D

NEW QUESTION 191
- (Exam Topic 4)
Which of the following Ii considered as the starting point of a database and stores user data and database objects in an MS SQL server?

A. Ibdata1
B. Application data files (ADF)
C. Transaction log data files (LDF)
D. Primary data files (MDF)

Answer: C

NEW QUESTION 192
- (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 196
- (Exam Topic 4)
A forensic examiner encounters a computer with a failed OS installation and the master boot record (MBR) or partition sector damaged. Which of the following tools can find and restore files and Information In the disk?

A. Helix
B. R-Studio
C. NetCat
D. Wireshark

Answer: B

NEW QUESTION 198
- (Exam Topic 4)
Ronald, a forensic investigator, has been hired by a financial services organization to Investigate an attack on their MySQL database server, which Is hosted on a Windows machine named WIN-DTRAI83202X. Ronald wants to retrieve information on the changes that have been made to the database. Which of the following files should Ronald examine for this task?

A. relay-log.info
B. WIN-DTRAI83202Xrelay-bin.index
C. WIN-DTRAI83202Xslow.log
D. WIN-DTRAI83202X-bin.nnnnnn

Answer: C

NEW QUESTION 203
- (Exam Topic 4)
A call detail record (CDR) provides metadata about calls made over a phone service. From the following data fields, which one Is not contained in a CDR.

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

Answer: C

NEW QUESTION 205
- (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 206
- (Exam Topic 4)
Which of the following applications will allow a forensic investigator to track the user login sessions and user transactions that have occurred on an MS SQL Server?

A. ApexSQL Audit
B. netcat
C. Notepad++
D. Event Log Explorer

Answer: A

NEW QUESTION 207
- (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 210
- (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 211
- (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 215
- (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 216
- (Exam Topic 4)
Fred, a cybercrime Investigator for the FBI, finished storing a solid-state drive In a static resistant bag and filled out the chain of custody form. Two days later. John grabbed the solid-state drive and created a clone of It (with write blockers enabled) In order to Investigate the drive. He did not document the chain of custody though. When John was finished, he put the solid-state drive back in the static resistant and placed it back in the evidence locker. A day later, the court trial began and upon presenting the evidence and the supporting documents, the chief Justice outright rejected them. Which of the following statements strongly support the reason for rejecting the evidence?

A. Block clones cannot be created with solid-state drives
B. Write blockers were used while cloning the evidence
C. John did not document the chain of custody
D. John investigated the clone instead of the original evidence itself

Answer: C

NEW QUESTION 221
- (Exam Topic 4)
A cybercriminal is attempting to remove evidence from a Windows computer. He deletes the file evIdence1.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 226
- (Exam Topic 4)
Jack is reviewing file headers to verify the file format and hopefully find more Information of the file. After a careful review of the data chunks through a hex editor; Jack finds the binary value Oxffd8ff. Based on the above Information, what type of format is the file/image saved as?

A. BMP

B. GIF
C. ASCII
D. JPEG

Answer: D

NEW QUESTION 231
- (Exam Topic 4)
During an Investigation, the first responders stored mobile devices In specific containers to provide network Isolation. All the following are examples of such pieces of equipment, except for:

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

Answer: D

NEW QUESTION 232
- (Exam Topic 4)
Which layer in the IoT architecture is comprised of hardware parts such as sensors, RFID tags, and devices that play an important role in data collection?

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

Answer: B

NEW QUESTION 237
- (Exam Topic 4)
Which of the following Windows event logs record events related to device drives and hardware changes?

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

Answer: B

NEW QUESTION 240
- (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 244
- (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 246
- (Exam Topic 4)
Which of the following tools is used to dump the memory of a running process, either immediately or when an error condition occurs?

A. FATKit
B. Coreography
C. Belkasoft Live RAM Capturer
D. CacheInf

Answer: C

NEW QUESTION 251
- (Exam Topic 4)
A computer forensics Investigator or forensic analyst Is a specially trained professional who works with law enforcement as well as private businesses to retrieve Information from computers and other types of data storage devices. For this, the analyst should have an excellent working knowledge of all aspects of the computer. Which of the following is not a duty of the analyst during a criminal investigation?

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

Answer: D

NEW QUESTION 253
- (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 257
- (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 258
- (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 263
- (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 268
- (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 271
- (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 274
- (Exam Topic 3)
Which of the following Perl scripts will help an investigator to access the executable image of a process?

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

Answer: D

NEW QUESTION 276
- (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 281
- (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 283
- (Exam Topic 3)
Which cloud model allows an investigator to acquire the instance of a virtual machine and initiate the forensics examination process?

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

Answer: B

NEW QUESTION 284
- (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 289
- (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 292
- (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 295
- (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 298
- (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 300
- (Exam Topic 3)
What does the bytes 0x0B-0x53 represent in the boot sector of NTFS volume on Windows 2000?

A. Jump instruction and the OEM ID
B. BIOS Parameter Block (BPB) and the OEM ID
C. BIOS Parameter Block (BPB) and the extended BPB
D. Bootstrap code and the end of the sector marker

Answer: C

NEW QUESTION 303
- (Exam Topic 3)
A company's policy requires employees to perform file transfers using protocols which encrypt traffic. You suspect some employees are still performing file transfers using unencrypted protocols because the employees don't like changes. You have positioned a network sniffer to capture traffic from the laptops used by employees in the data ingest department. Using Wireshark to examine the captured traffic, which command can be used as a display filter to find unencrypted file transfers?

A. tcp.port = 23
B. tcp.port == 21
C. tcp.port == 21 || tcp.port == 22
D. tcp.port != 21

Answer: B

NEW QUESTION 308
- (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 310
- (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 314
- (Exam Topic 3)
Which of the following commands shows you the username and IP address used to access the system via a remote login session and the type of client from which they are accessing the system?

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

Answer: B

NEW QUESTION 315
- (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 320
- (Exam Topic 3)
Which of the following web browser uses the Extensible Storage Engine (ESE) database format to store browsing records, including history, cache, and cookies?

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

Answer: C

NEW QUESTION 323
- (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 328
- (Exam Topic 3)
Which one of the following is not a first response procedure?

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

Answer: C

NEW QUESTION 333
- (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 336
- (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 340
- (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 345
- (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 350
- (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 355
- (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 357
- (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 358

- (Exam Topic 3)
What is the investigator trying to view by issuing the command displayed in the following screenshot?
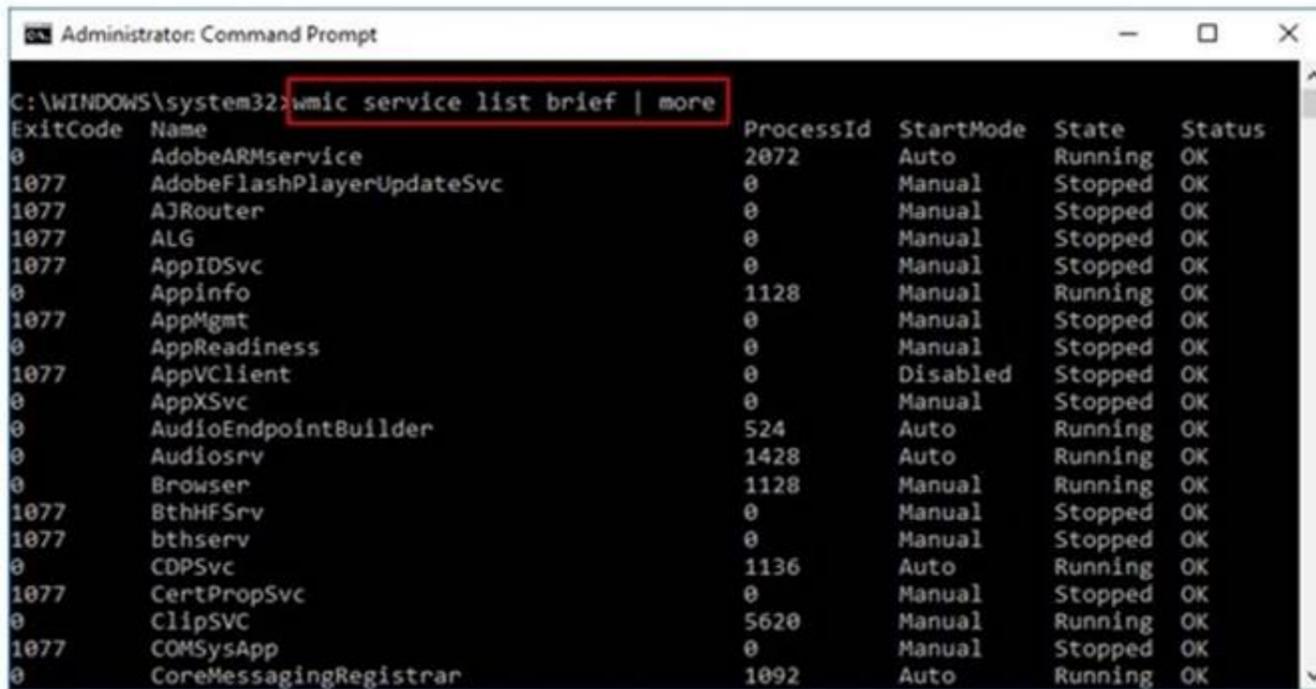
A. List of services stopped
B. List of services closed recently
C. List of services recently started
D. List of services installed

Answer: D

NEW QUESTION 360
- (Exam Topic 3)
In which registry does the system store the Microsoft security IDs?

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

Answer: D

NEW QUESTION 364
- (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 367
- (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 368
- (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 373
- (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 376
- (Exam Topic 3)
Which of the following registry hive gives the configuration information about which application was used to open various files on the system?

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

Answer: A

NEW QUESTION 381
- (Exam Topic 3)
When a user deletes a file, the system creates a $I file to store its details. What detail does the $I file not contain?

A. File Size
B. File origin and modification
C. Time and date of deletion
D. File Name

Answer: B

NEW QUESTION 385
- (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 388
- (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 389
- (Exam Topic 3)
Which of the following is a precomputed table containing word lists like dictionary files and brute force lists and their hash values?

A. Directory Table
B. Rainbow Table
C. Master file Table (MFT)
D. Partition Table

Answer: B

NEW QUESTION 391
- (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 395
- (Exam Topic 3)
What is the framework used for application development for iOS-based mobile devices?

A. Cocoa Touch
B. Dalvik
C. Zygote
D. AirPlay

Answer: A

NEW QUESTION 400
- (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 403
- (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 404
- (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 408
- (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 412
- (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 415
- (Exam Topic 3)
Pick the statement which does not belong to the Rule 804. Hearsay Exceptions; Declarant Unavailable.

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

Answer: D

NEW QUESTION 416
- (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 418
- (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 423
- (Exam Topic 3)
Which of the following is a federal law enacted in the US to control the ways that financial institutions deal with the private information of individuals?

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

Answer: C

NEW QUESTION 428
- (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 432
- (Exam Topic 3)
Which of the following is NOT an anti-forensics technique?

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

Answer: A

NEW QUESTION 437
- (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 441

- (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 444
- (Exam Topic 3)

Which of the following is found within the unique instance ID key and helps investigators to map the entry from USBSTOR key to the MountedDevices key?

A. ParentIDPrefix
B. LastWrite
C. UserAssist key
D. MRUListEx key

Answer: A

NEW QUESTION 447
- (Exam Topic 3)

The Apache server saves diagnostic information and error messages that it encounters while processing requests. The default path of this file is usr/local/apache/logs/error.log in Linux. Identify the Apache error log from the following logs.

A. http://victim.com/scripts/..%c0%af../..%c0%af../..%c0%af../..%c0%af../..%c0%af../..%c0%af../..%c0%af../winnt/system32/cmd.exe?/c+dir+C:\Winnt\system32\Logfiles\W3SVC1
B. [Wed Oct 11 14:32:52 2000] [error] [client 127.0.0.1] client denied by server configuration:/export/home/live/ap/htdocs/test
C. 127.0.0.1 - frank [10/Oct/2000:13:55:36 -0700]"GET /apache_pb.gif HTTP/1.0" 200 2326
D. 127.0.0.1 - - [10/Apr/2007:10:39:11 +0300]] [error] "GET /apache_pb.gif HTTP/1.0" 200 2326

Answer: B

NEW QUESTION 451
- (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 454
- (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 459
- (Exam Topic 3)

Randy has extracted data from an old version of a Windows-based system and discovered info file Dc5.txt in the system recycle bin. What does the file name denote?

A. A text file deleted from C drive in sixth sequential order
B. A text file deleted from C drive in fifth sequential order
C. A text file copied from D drive to C drive in fifth sequential order
D. A text file copied from C drive to D drive in fifth sequential order

Answer: B

NEW QUESTION 460
- (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 465
- (Exam Topic 2)
Jacob is a computer forensics investigator with over 10 years experience in investigations and has written over 50 articles on computer forensics. He has been called upon as a qualified witness to testify the accuracy and integrity of the technical log files gathered in an investigation into computer fraud. What is the term used for Jacob testimony in this case?

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

Answer: B

NEW QUESTION 469
- (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 470
- (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 471
- (Exam Topic 2)
Adam, a forensic investigator, is investigating an attack on Microsoft Exchange Server of a large organization. As the first step of the investigation, he examined the PRIV.EDB file and found the source from where the mail originated and the name of the file that disappeared upon execution. Now, he wants to examine the MIME stream content. Which of the following files is he going to examine?

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

Answer: A

NEW QUESTION 473
- (Exam Topic 2)
Cylie is investigating a network breach at a state organization in Florida. She discovers that the intruders were able to gain access into the company firewalls by overloading them with IP packets. Cylie then discovers through her investigation that the intruders hacked into the company phone system and used the hard drives on their PBX system to store shared music files. What would this attack on the company PBX system be called?

A. Phreaking
B. Squatting
C. Crunching
D. Pretexting

Answer: A

NEW QUESTION 477
- (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 478
- (Exam Topic 2)
Where is the default location for Apache access logs on a Linux computer?

A. usr/local/apache/logs/access_log
B. bin/local/home/apache/logs/access_log
C. usr/logs/access_log
D. logs/usr/apache/access_log

Answer: A

NEW QUESTION 483
- (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 487
- (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 490
- (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 493
- (Exam Topic 2)
What type of equipment would a forensics investigator store in a StrongHold bag?

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

Answer: D

NEW QUESTION 497
- (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 499

- (Exam Topic 2)
Jacky encrypts her documents using a password. It is known that she uses her daughter's year of birth as part of the password. Which password cracking technique would be optimal to crack her password?

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

Answer: A

NEW QUESTION 500
- (Exam Topic 2)
Sniffers that place NICs in promiscuous mode work at what layer of the OSI model?

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

Answer: C

NEW QUESTION 504
- (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 505
- (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 509
- (Exam Topic 2)
Which of the following files gives information about the client sync sessions in Google Drive on Windows?

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

Answer: B

NEW QUESTION 511
- (Exam Topic 2)
Which among the following is an act passed by the U.S. Congress in 2002 to protect investors from the possibility of fraudulent accounting activities by corporations?

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

Answer: C

NEW QUESTION 514
- (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 518
- (Exam Topic 2)
What does 254 represent in ICCID 89254021520014515744?

A. Industry Identifier Prefix
B. Country Code
C. Individual Account Identification Number
D. Issuer Identifier Number

Answer: B

NEW QUESTION 520
- (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 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 528
- (Exam Topic 2)
Data is striped at a byte level across multiple drives, and parity information is distributed among all member drives.
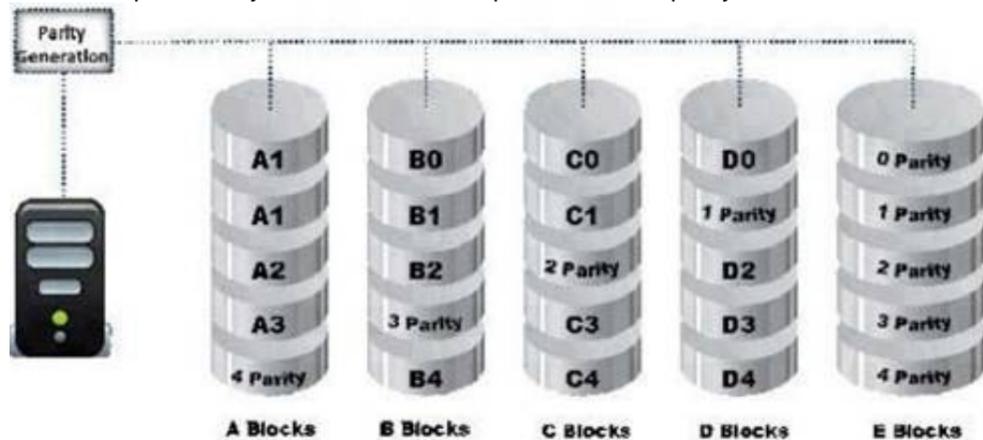
What RAID level is represented here?

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

Answer: B

NEW QUESTION 532
- (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 536
- (Exam Topic 2)
Which of the following are small pieces of data sent from a website and stored on the user's computer by the user's web browser to track, validate, and maintain

specific user information?

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

Answer: C

NEW QUESTION 538
- (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 542
- (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 544
- (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 548
- (Exam Topic 2)
When is it appropriate to use computer forensics?

A. If copyright and intellectual property theft/misuse has occurred
B. If employees do not care for their boss management techniques
C. If sales drop off for no apparent reason for an extended period of time
D. If a financial institution is burglarized by robbers

Answer: A

NEW QUESTION 551
- (Exam Topic 2)
Which of the following data structures stores attributes of a process, as well as pointers to other attributes and data structures?

A. Lsproc
B. DumpChk
C. RegEdit
D. EProcess

Answer: D

NEW QUESTION 552
- (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 553
- (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 555
- (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 557
- (Exam Topic 2)
This type of testimony is presented by someone who does the actual fieldwork and does not offer a view in
court.

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

Answer: D

NEW QUESTION 558
- (Exam Topic 2)
Which of the following files DOES NOT use Object Linking and Embedding (OLE) technology to embed and link to other objects?

A. Portable Document Format
B. MS-office Word Document
C. MS-office Word OneNote
D. MS-office Word PowerPoint

Answer: A

NEW QUESTION 560
- (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 565
- (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 570
- (Exam Topic 2)
What type of attack sends spoofed UDP packets (instead of ping packets) with a fake source address to the IP broadcast address of a large network?

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

Answer: A

NEW QUESTION 573
- (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 575
- (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 577
- (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 581
- (Exam Topic 2)
Daryl, a computer forensics investigator, has just arrived at the house of an alleged computer hacker. Daryl takes pictures and tags all computer and peripheral equipment found in the house. Daryl packs all the items found in his van and takes them back to his lab for further examination. At his lab, Michael his assistant helps him with the investigation. Since Michael is still in training, Daryl supervises all of his work very carefully. Michael is not quite sure about the procedures to copy all the data off the computer and peripheral devices. How many data acquisition tools should Michael use when creating copies of the evidence for the investigation?

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

Answer: A

NEW QUESTION 586
- (Exam Topic 2)
Which of the following Event Correlation Approach checks and compares all the fields systematically and
intentionally for positive and negative correlation with each other to determine the correlation across one or multiple fields?

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

Answer: B

NEW QUESTION 589
- (Exam Topic 2)
Which of the following attacks allows an attacker to access restricted directories, including application source code, configuration and critical system files, and to execute commands outside of the web server's root directory?

A. Parameter/form tampering
B. Unvalidated input
C. Directory traversal
D. Security misconfiguration

Answer: C

NEW QUESTION 594
- (Exam Topic 2)
Which MySQL log file contains information on server start and stop?

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

Answer: D

NEW QUESTION 598
- (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 599
- (Exam Topic 2)
While presenting his case to the court, Simon calls many witnesses to the stand to testify. Simon decides to call Hillary Taft, a lay witness, to the stand. Since Hillary is a lay witness, what field would she be considered an expert in?

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

Answer: B

NEW QUESTION 602
- (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 607
- (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 609
- (Exam Topic 2)
Richard is extracting volatile data from a system and uses the command doskey/history. What is he trying to extract?

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

Answer: B

NEW QUESTION 613
- (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 618
- (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 623
- (Exam Topic 2)
Which of the following acts as a network intrusion detection system as well as network intrusion prevention system?

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

Answer: C

NEW QUESTION 624
- (Exam Topic 2)
Which password cracking technique uses details such as length of password, character sets used to construct the password, etc.?

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

Answer: A

NEW QUESTION 629
- (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 631
- (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 635
- (Exam Topic 2)
At what layer does a cross site scripting attack occur on?

A. Presentation
B. Application
C. Session
D. Data Link

Answer: B

NEW QUESTION 636
- (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 640
- (Exam Topic 2)
Pagefile.sys is a virtual memory file used to expand the physical memory of a computer. Select the registry path for the page file:

A. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management
B. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\System Management
C. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Device Management
D. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\PrefetchParameters

Answer: A

NEW QUESTION 645

- (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 646
- (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 650
- (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 653
- (Exam Topic 2)
Linux operating system has two types of typical bootloaders namely LILO (Linux Loader) and GRUB (Grand Unified Bootloader). In which stage of the booting process do the bootloaders become active?

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

Answer: A

NEW QUESTION 658
......

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

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

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

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

Money Back Guarantee

312-49v10 Practice Exam Features:

* 312-49v10 Questions and Answers Updated Frequently

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

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

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