EC-Council

Exam Questions 312-49v10

Computer Hacking Forensic Investigator (CHFI-v10)

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

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

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

Answer: C

NEW QUESTION 2
- (Exam Topic 1)
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 3
- (Exam Topic 1)
A suspect is accused of violating the acceptable use of computing resources, as he has visited adult websites and downloaded images. The investigator wants to demonstrate that the suspect did indeed visit these sites. However, the suspect has cleared the search history and emptied the cookie cache. Moreover, he has removed any images he might have downloaded. What can the investigator do to prove the violation?

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

Answer: A

NEW QUESTION 4
- (Exam Topic 1)
Chris has been called upon to investigate a hacking incident reported by one of his clients. The company suspects the involvement of an insider accomplice in the attack. Upon reaching the incident scene, Chris secures the physical area, records the scene using visual media. He shuts the system down by pulling the power plug so that he does not disturb the system in any way. He labels all cables and connectors prior to disconnecting any. What do you think would be the next sequence of events?

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

Answer: B

NEW QUESTION 5
- (Exam Topic 1)
What type of attack occurs when an attacker can force a router to stop forwarding packets by flooding the router with many open connections simultaneously so that all the hosts behind the router are effectively disabled?

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

Answer: B

NEW QUESTION 6
- (Exam Topic 1)
Jason is the security administrator of ACMA metal Corporation. One day he notices the company's Oracle database server has been compromised and the customer information along with financial data has been stolen. The financial loss will be in millions of dollars if the database gets into the hands of the competitors. Jason wants to report this crime to the law enforcement agencies immediately.
Which organization coordinates computer crimes investigations throughout the United States?

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

Answer: B

NEW QUESTION 7
- (Exam Topic 1)
Area density refers to:

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

Answer: A

NEW QUESTION 8
- (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 9
- (Exam Topic 1)
A state department site was recently attacked and all the servers had their disks erased. The incident response team sealed the area and commenced investigation. During evidence collection they came across a zip disks that did not have the standard labeling on it. The incident team ran the disk on an isolated system and found that the system disk was accidentally erased. They decided to call in the FBI for further investigation. Meanwhile, they short listed possible suspects including three summer interns. Where did the incident team go wrong?

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

Answer: C

NEW QUESTION 10
- (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 10
- (Exam Topic 2)
Steven has been given the task of designing a computer forensics lab for the company he works for. He has found documentation on all aspects of how to design a lab except the number of exits needed. How many exits should Steven include in his design for the computer forensics lab?

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

Answer: B

NEW QUESTION 11
- (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 12
- (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 15
- (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 17
- (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 19
- (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 22
- (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 23
- (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 26
- (Exam Topic 1)
If you plan to startup a suspect's computer, you must modify the to ensure that you do not contaminate or alter data on the suspect's hard drive by booting to the hard drive.

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

Answer: C

NEW QUESTION 30
- (Exam Topic 1)
When investigating a Windows System, it is important to view the contents of the page or swap file because:

A. Windows stores all of the systems configuration information in this file
B. This is file that windows use to communicate directly with Registry
C. A Large volume of data can exist within the swap file of which the computer user has no knowledge
D. This is the file that windows use to store the history of the last 100 commands that were run from the command line

Answer: C

NEW QUESTION 32
- (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 34
- (Exam Topic 1)
Melanie was newly assigned to an investigation and asked to make a copy of all the evidence from the compromised system. Melanie did a DOS copy of all the files on the system. What would be the primary reason for you to recommend a disk imaging tool?

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

Answer: C

NEW QUESTION 38
- (Exam Topic 1)
In a computer forensics investigation, what describes the route that evidence takes from the time you find it until the case is closed or goes to court?

A. rules of evidence
B. law of probability
C. chain of custody
D. policy of separation

Answer: C

NEW QUESTION 40
- (Exam Topic 1)
What method of computer forensics will allow you to trace all ever-established user accounts on a Windows 2000 sever the course of its lifetime?

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

Answer: C

NEW QUESTION 45
- (Exam Topic 1)
You should make at least how many bit-stream copies of a suspect drive?

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

Answer: B

NEW QUESTION 49
- (Exam Topic 1)
George is the network administrator of a large Internet company on the west coast. Per corporate policy, none of the employees in the company are allowed to use

FTP or SFTP programs without obtaining approval from the IT department. Few managers are using SFTP program on their computers. Before talking to his boss, George wants to have some proof of their activity. George wants to use Ethereal to monitor network traffic, but only SFTP traffic to and from his network. What filter should George use in Ethereal?

A. src port 23 and dst port 23
B. udp port 22 and host 172.16.28.1/24
C. net port 22
D. src port 22 and dst port 22

Answer: D

NEW QUESTION 50
- (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 52
- (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 56
- (Exam Topic 1)
Which Intrusion Detection System (IDS) usually produces the most false alarms due to the unpredictable behaviors of users and networks?

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

Answer: B

NEW QUESTION 61
- (Exam Topic 1)
Julia is a senior security analyst for Berber Consulting group. She is currently working on a contract for a small accounting firm in Florid a. They have given her permission to perform social engineering attacks on the company to see if their in-house training did any good. Julia calls the main number for the accounting firm and talks to the receptionist. Julia says that she is an IT technician from the company's main office in Iowa. She states that she needs the receptionist's network username and password to troubleshoot a problem they are having. Julia says that Bill Hammond, the CEO of the company, requested this information. After hearing the name of the CEO, the receptionist gave Julia all the information she asked for. What principal of social engineering did Julia use?

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

Answer: D

NEW QUESTION 63
- (Exam Topic 1)
You have compromised a lower-level administrator account on an Active Directory network of a small company in Dallas, Texas. You discover Domain Controllers through enumeration. You connect to one of the Domain Controllers on port 389 using ldp.exe. What are you trying to accomplish here?

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

Answer: D

NEW QUESTION 66
- (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 69
- (Exam Topic 1)
Volatile Memory is one of the leading problems for forensics. Worms such as code Red are memory resident and do write themselves to the hard drive, if you turn the system off they disappear. In a lab environment, which of the following options would you suggest as the most appropriate to overcome the problem of capturing volatile memory?

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

Answer: C

NEW QUESTION 72
- (Exam Topic 1)
You are the network administrator for a small bank in Dallas, Texas. To ensure network security, you enact a security policy that requires all users to have 14 character passwords. After giving your users 2 weeks notice, you change the Group Policy to force 14 character passwords. A week later you dump the SAM database from the standalone server and run a password-cracking tool against it. Over 99% of the passwords are broken within an hour. Why were these passwords cracked so Quickly?

A. Passwords of 14 characters or less are broken up into two 7-character hashes
B. A password Group Policy change takes at least 3 weeks to completely replicate throughout a network
C. Networks using Active Directory never use SAM databases so the SAM database pulled was empty
D. The passwords that were cracked are local accounts on the Domain Controller

Answer: A

NEW QUESTION 76
- (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 77
- (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 80
- (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 83
- (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 85
- (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 87
- (Exam Topic 1)
Why should you note all cable connections for a computer you want to seize as evidence?

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

Answer: A

NEW QUESTION 89
- (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 94
- (Exam Topic 1)
Which of the following should a computer forensics lab used for investigations have?

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

Answer: B

NEW QUESTION 98
- (Exam Topic 1)
Harold is a web designer who has completed a website for ghttech.net. As part of the maintenance agreement he signed with the client, Harold is performing research online and seeing how much exposure the site has received so far. Harold navigates to google.com and types in the following search.
link:www.ghttech.net What will this search produce?

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

Answer: B

NEW QUESTION 100
- (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 101
- (Exam Topic 1)
During the course of a corporate investigation, you find that an Employee is committing a crime. Can the Employer file a criminal complaint with Police?

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

Answer: A

NEW QUESTION 102
- (Exam Topic 1)
In General, Involves the investigation of data that can be retrieved from the hard disk or other disks of a computer by applying scientific methods to retrieve the data.

A. Network Forensics
B. Data Recovery
C. Disaster Recovery
D. Computer Forensics

Answer: D

NEW QUESTION 107
- (Exam Topic 1)
What is the name of the Standard Linux Command that is also available as windows application that can be used to create bit-stream images?

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

Answer: D

NEW QUESTION 110
- (Exam Topic 1)
Bill is the accounting manager for Grummon and Sons LLC in Chicago. On a regular basis, he needs to send PDF documents containing sensitive information through E-mail to his customers.
Bill protects the PDF documents with a password and sends them to their intended recipients. Why PDF passwords do not offer maximum protection?

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

Answer: A

NEW QUESTION 111
- (Exam Topic 1)
Bob has been trying to penetrate a remote production system for the past two weeks. This time however, he is able to get into the system. He was able to use the System for a period of three weeks. However, law enforcement agencies were recoding his every activity and this was later presented as evidence.
The organization had used a Virtual Environment to trap Bob. What is a Virtual Environment?

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

Answer: A

NEW QUESTION 115
- (Exam Topic 1)
You work as a penetration tester for Hammond Security Consultants. You are currently working on a contract for the state government of California. Your next step is to initiate a DoS attack on their network. Why would you want to initiate a DoS attack on a system you are testing?

A. Show outdated equipment so it can be replaced
B. List weak points on their network
C. Use attack as a launching point to penetrate deeper into the network
D. Demonstrate that no system can be protected against DoS attacks

Answer: B

NEW QUESTION 118
- (Exam Topic 1)
When obtaining a warrant, it is important to:

A. particularlydescribe the place to be searched and particularly describe the items to be seized

B. generallydescribe the place to be searched and particularly describe the items to be seized
C. generallydescribe the place to be searched and generally describe the items to be seized
D. particularlydescribe the place to be searched and generally describe the items to be seized

Answer: A

NEW QUESTION 119
- (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 123
- (Exam Topic 1)
With the standard Linux second extended file system (Ext2fs), a file is deleted when the inode internal link count reaches .

A. 10
B. 100
C. 1

Answer: A

NEW QUESTION 128
- (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 129
- (Exam Topic 1)
Kyle is performing the final testing of an application he developed for the accounting department. His last round of testing is to ensure that the program is as secure as possible. Kyle runs the following
command. What is he testing at this point?
#include #include int main(int argc, char
*argv[]) { char buffer[10]; if (argc < 2) { fprintf (stderr, "USAGE: %s string\n", argv[0]); return 1; } strcpy(buffer, argv[1]); return 0; }

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

Answer: A

NEW QUESTION 130
- (Exam Topic 1)
An Expert witness give an opinion if:

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

Answer: A

NEW QUESTION 131
- (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 135
- (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 140
- (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 143
- (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 145
- (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 150
- (Exam Topic 4)
An investigator seized a notebook device installed with a Microsoft Windows OS. Which type of files would support an investigation of the data size and structure in the device?

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

Answer: D

NEW QUESTION 154
- (Exam Topic 4)
In a Fllesystem 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 155
- (Exam Topic 4)
Which of the following statements pertaining to First Response is true?

A. First Response is a part of the investigation phase

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

Answer: A

NEW QUESTION 159
- (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 162
- (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 167
- (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 168
- (Exam Topic 4)
Fill In the missing Master Boot Record component.
* 1. Master boot code
* 2. Partition table
* 3. _____

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

Answer: A

NEW QUESTION 170
- (Exam Topic 4)
Assume there Is a file named myflle.txt In C: drive that contains hidden data streams. Which of the following commands would you Issue to display the contents of a data stream?

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

Answer: A

NEW QUESTION 173
- (Exam Topic 4)
An investigator wants to extract passwords from SAM and System Files. Which tool can the Investigator use to obtain a list of users, passwords, and their hashes In this case?

A. PWdump7
B. HashKey

C. Nuix
D. FileMerlin

Answer: A

NEW QUESTION 175
- (Exam Topic 4)
Which layer in the IoT architecture is comprised of hardware parts such as sensors, RFID tags, and devices that play an important role in data collection?

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

Answer: B

NEW QUESTION 180
- (Exam Topic 4)
Donald made an OS disk snapshot of a compromised Azure VM under a resource group being used by the affected company as a part of forensic analysis process. He then created a vhd file out of the snapshot and stored it in a file share and as a page blob as backup in a storage account under different region. What Is the next thing he should do as a security measure?

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

Answer: C

NEW QUESTION 184
- (Exam Topic 4)
For the purpose of preserving the evidentiary chain of custody, which of the following labels is not appropriate?

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

Answer: D

NEW QUESTION 188
- (Exam Topic 4)
SO/IEC 17025 is an accreditation for which of the following:

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

Answer: C

NEW QUESTION 189
- (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 190
- (Exam Topic 4)
Robert needs to copy an OS disk snapshot of a compromised VM to a storage account in different region for further investigation. Which of the following should he use in this scenario?

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

Answer: D

NEW QUESTION 194

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

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

Answer: B

NEW QUESTION 197
- (Exam Topic 4)
Place the following In order of volatility from most volatile to the least volatile.

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

Answer: B

NEW QUESTION 200
- (Exam Topic 3)
Which of the following Perl scripts will help an investigator to access the executable image of a process?

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

Answer: D

NEW QUESTION 205
- (Exam Topic 3)
Which list contains the most recent actions performed by a Windows User?

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

Answer: A

NEW QUESTION 209
- (Exam Topic 3)
Which of the following file system uses Master File Table (MFT) database to store information about every file and directory on a volume?

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

Answer: D

NEW QUESTION 214
- (Exam Topic 3)
What technique is used by JPEGs for compression?

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

Answer: C

NEW QUESTION 219
- (Exam Topic 3)
Buffer overflow vulnerability of a web application occurs when it fails to guard its buffer properly and allows writing beyond its maximum size. Thus, it overwrites the
. There are multiple forms of buffer overflow, including a Heap Buffer Overflow and a Format String Attack.

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

Answer: A

NEW QUESTION 220
- (Exam Topic 3)
What system details can an investigator obtain from the NetBIOS name table cache?

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

Answer: C

NEW QUESTION 221
- (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 225
- (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 229
- (Exam Topic 3)
What does the bytes 0x0B-0x53 represent in the boot sector of NTFS volume on Windows 2000?

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

Answer: C

NEW QUESTION 234
- (Exam Topic 3)
A company's policy requires employees to perform file transfers using protocols which encrypt traffic. You suspect some employees are still performing file transfers using unencrypted protocols because the employees don't like changes. You have positioned a network sniffer to capture traffic from the laptops used by employees in the data ingest department. Using Wireshark to examine the captured traffic, which command can be used as a display filter to find unencrypted file transfers?

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

Answer: B

NEW QUESTION 236
- (Exam Topic 3)
Amber, a black hat hacker, has embedded malware into a small enticing advertisement and posted it on a popular ad-network that displays across various websites. What is she doing?

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

Answer: A

NEW QUESTION 237
- (Exam Topic 3)

In which cloud crime do attackers try to compromise the security of the cloud environment in order to steal data or inject a malware?

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

Answer: D

NEW QUESTION 240
- (Exam Topic 3)
During forensics investigations, investigators tend to collect the system time at first and compare it with UTC. What does the abbreviation UTC stand for?

A. Coordinated Universal Time
B. Universal Computer Time
C. Universal Time for Computers
D. Correlated Universal Time

Answer: A

NEW QUESTION 242
- (Exam Topic 3)
What malware analysis operation can the investigator perform using the jv16 tool?

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

Answer: D

NEW QUESTION 246
- (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 251
- (Exam Topic 3)
A forensic examiner is examining a Windows system seized from a crime scene. During the examination of a suspect file, he discovered that the file is password protected. He tried guessing the password using the suspect's available information but without any success. Which of the following tool can help the investigator to solve this issue?

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

Answer: A

NEW QUESTION 254
- (Exam Topic 3)
Andie, a network administrator, suspects unusual network services running on a windows system. Which of the following commands should he use to verify unusual network services started on a Windows system?

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

Answer: D

NEW QUESTION 256
- (Exam Topic 3)
Which of the following network attacks refers to sending huge volumes of email to an address in an attempt to overflow the mailbox or overwhelm the server where the email address is hosted so as to cause a
denial-of-service attack?

A. Email spamming
B. Phishing
C. Email spoofing

D. Mail bombing

Answer: D

NEW QUESTION 259
- (Exam Topic 3)
Which among the following laws emphasizes the need for each Federal agency to develop, document, and implement an organization-wide program to provide information security for the information systems that support its operations and assets?
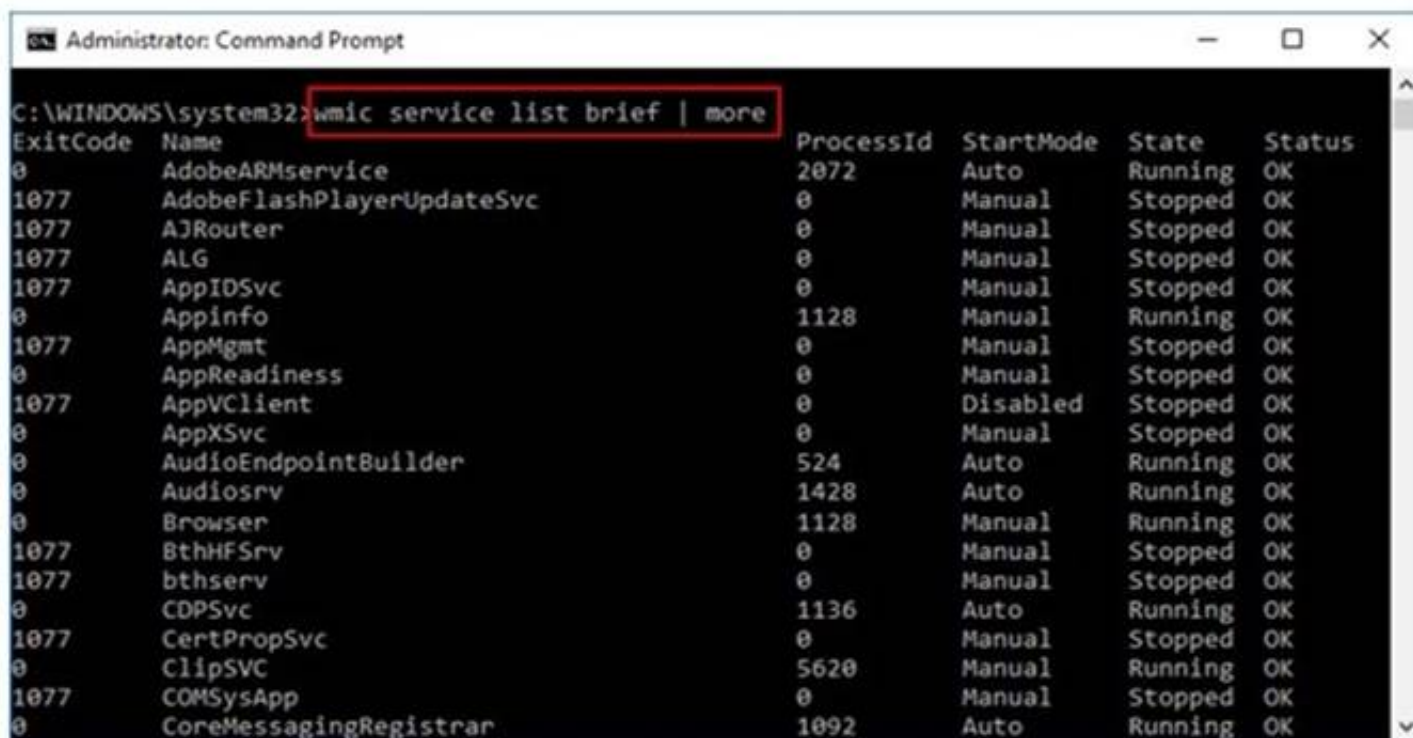
A. FISMA
B. HIPAA
C. GLBA
D. SOX

Answer: A

NEW QUESTION 264
- (Exam Topic 3)
What is the investigator trying to view by issuing the command displayed in the following screenshot?

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

Answer: D

NEW QUESTION 266
- (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 269
- (Exam Topic 3)
An investigator enters the command sqlcmd -S WIN-CQQMK62867E -e -s"," -E as part of collecting the primary data file and logs from a database. What does the "WIN-CQQMK62867E" represent?

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

Answer: B

NEW QUESTION 271
- (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 275
- (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 277
- (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 282
- (Exam Topic 3)
Select the tool appropriate for examining the dynamically linked libraries of an application or malware.

A. DependencyWalker
B. SysAnalyzer
C. PEiD
D. ResourcesExtract

Answer: A

NEW QUESTION 284
- (Exam Topic 3)
POP3 is an Internet protocol, which is used to retrieve emails from a mail server. Through which port does an email client connect with a POP3 server?

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

Answer: A

NEW QUESTION 289
- (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 291
- (Exam Topic 3)
Which of the following registry hive gives the configuration information about which application was used to open various files on the system?

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

Answer: A

NEW QUESTION 294

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

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

Answer: D

NEW QUESTION 298
- (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 303
- (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 307
- (Exam Topic 3)
As part of extracting the system data, Jenifer has used the netstat command. What does this tool reveal?

A. Status of users connected to the internet
B. Net status of computer usage
C. Information about network connections
D. Status of network hardware

Answer: C

NEW QUESTION 310
- (Exam Topic 3)
What is the role of Alloc.c in Apache core?

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

Answer: A

NEW QUESTION 311
- (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 316
- (Exam Topic 3)
Which of the following standard represents a legal precedent set in 1993 by the Supreme Court of the United States regarding the admissibility of expert witnesses' testimony during federal legal proceedings?

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

Answer: D

NEW QUESTION 319
- (Exam Topic 3)
Which among the following web application threats is resulted when developers expose various internal implementation objects, such as files, directories, database records, or key-through references?

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

Answer: C

NEW QUESTION 321
- (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 324
- (Exam Topic 3)
Report writing is a crucial stage in the outcome of an investigation. Which information should not be included in the report section?

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

Answer: A

NEW QUESTION 329
- (Exam Topic 3)
Which of the following is a MAC-based File Recovery Tool?

A. VirtualLab
B. GetDataBack
C. Cisdem DataRecovery 3
D. Smart Undeleter

Answer: C

NEW QUESTION 332
- (Exam Topic 3)
Which of the following information is displayed when Netstat is used with -ano switch?

A. Ethernet statistics
B. Contents of IP routing table
C. Details of routing table
D. Details of TCP and UDP connections

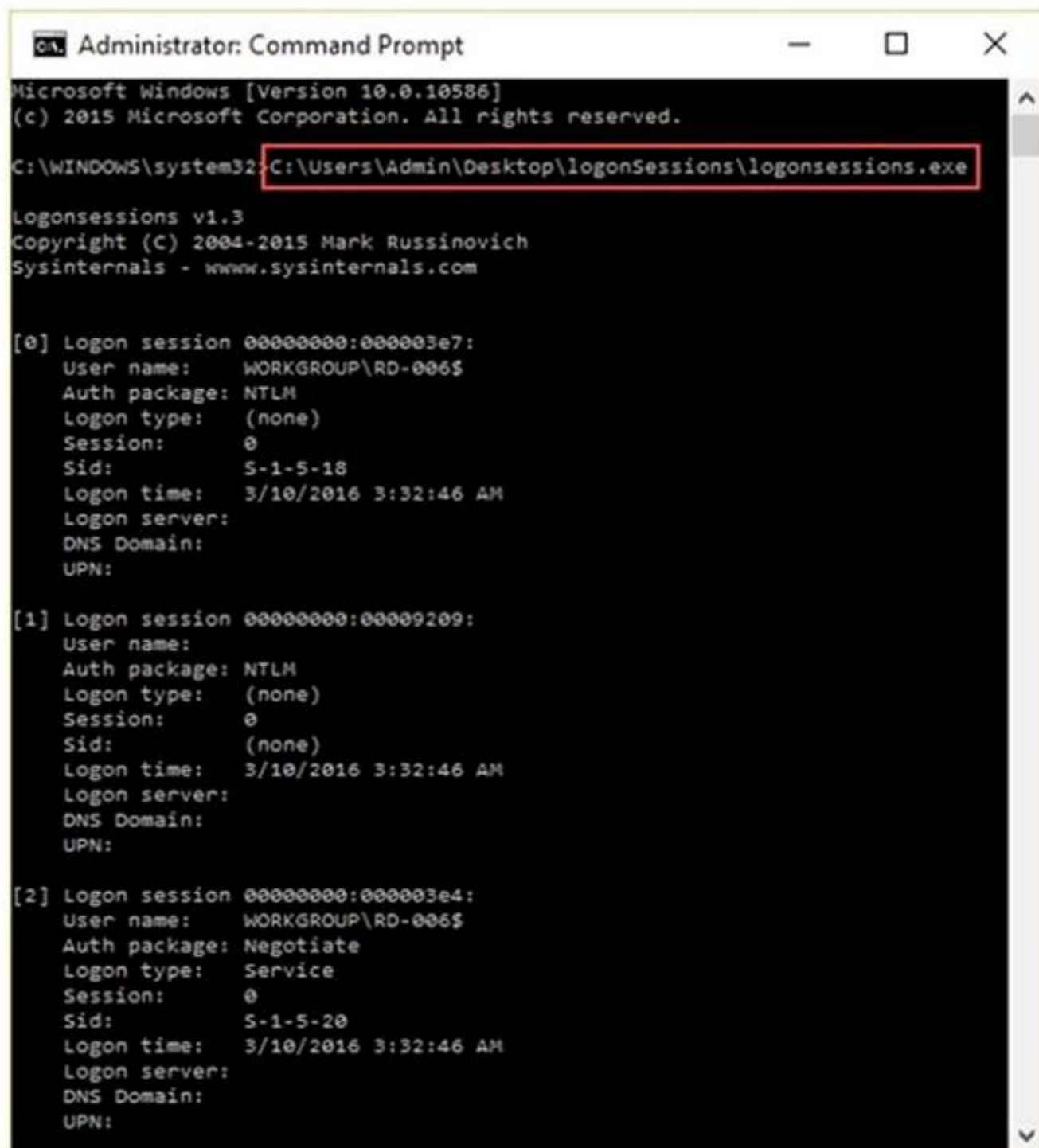**Answer:** D

NEW QUESTION 337
- (Exam Topic 3)
What is the investigator trying to analyze if the system gives the following image as output?

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

Answer: B

NEW QUESTION 340
- (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 344
- (Exam Topic 3)
Data Files contain Multiple Data Pages, which are further divided into Page Header, Data Rows, and Offset Table. Which of the following is true for Data Rows?

A. Data Rows store the actual data
B. Data Rows present Page typ
C. Page ID, and so on
D. Data Rows point to the location of actual data
E. Data Rows spreads data across multiple databases

Answer: B

NEW QUESTION 349
- (Exam Topic 3)
Jacob is a computer forensics investigator with over 10 years of 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's testimony in this case?

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

Answer: D

NEW QUESTION 351
- (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 353
- (Exam Topic 3)
Identify the file system that uses $BitMap file to keep track of all used and unused clusters on a volume.

A. NTFS
B. FAT
C. EXT
D. FAT32

Answer: A

NEW QUESTION 358
- (Exam Topic 3)
Which of the following is found within the unique instance ID key and helps investigators to map the entry from USBSTOR key to the MountedDevices key?

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

Answer: A

NEW QUESTION 362
- (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 363
- (Exam Topic 3)
UEFI is a specification that defines a software interface between an OS and platform firmware. Where does this interface store information about files present on a disk?

A. BIOS-MBR
B. GUID Partition Table (GPT)
C. Master Boot Record (MBR)
D. BIOS Parameter Block

Answer: B

NEW QUESTION 365
- (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 366
- (Exam Topic 3)
NTFS sets a flag for the file once you encrypt it and creates an EFS attribute where it stores Data Decryption Field (DDF) and Data Recovery Field (DDR). Which of the following is not a part of DDF?

A. Encrypted FEK
B. Checksum
C. EFS Certificate Hash
D. Container Name

Answer: B

NEW QUESTION 369
- (Exam Topic 2)
What is one method of bypassing a system BIOS password?

A. Removing the processor
B. Removing the CMOS battery
C. Remove all the system memory
D. Login to Windows and disable the BIOS password

Answer: B

NEW QUESTION 370
- (Exam Topic 2)
Smith, a forensic examiner, was analyzing a hard disk image to find and acquire deleted sensitive files. He stumbled upon a $Recycle.Bin folder in the root directory of the disk. Identify the operating system in use.

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

Answer: D

NEW QUESTION 372
- (Exam Topic 2)
Annie is searching for certain deleted files on a system running Windows XP OS. Where will she find the files if they were not completely deleted from the system?

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

Answer: B

NEW QUESTION 376
- (Exam Topic 2)
What must an investigator do before disconnecting an iPod from any type of computer?

A. Unmount the iPod
B. Mount the iPod
C. Disjoin the iPod
D. Join the iPod

Answer: A

NEW QUESTION 379
- (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 381
- (Exam Topic 2)
Harold is a computer forensics investigator working for a consulting firm out of Atlanta Georgia. Harold is called upon to help with a corporate espionage case in Miami Florida. Harold assists in the investigation by
pulling all the data from the computers allegedly used in the illegal activities. He finds that two suspects in the company where stealing sensitive corporate information and selling it to competing companies. From the email and instant messenger logs recovered, Harold has discovered that the two employees notified the buyers by writing symbols on the back of specific stop signs. This way, the buyers knew when and where to meet with the alleged suspects to buy the stolen

material. What type of steganography did these two suspects use?

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

Answer: B

NEW QUESTION 385
- (Exam Topic 2)
Which of the following files stores information about a local Google Drive installation such as User email ID, Local Sync Root Path, and Client version installed?

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

Answer: D

NEW QUESTION 389
- (Exam Topic 2)
Charles has accidentally deleted an important file while working on his Mac computer. He wants to recover the deleted file as it contains some of his crucial business secrets. Which of the following tool will help Charles?

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

Answer: C

NEW QUESTION 393
- (Exam Topic 2)
How will you categorize a cybercrime that took place within a CSP's cloud environment?

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

Answer: D

NEW QUESTION 397
- (Exam Topic 2)
Under confession, an accused criminal admitted to encrypting child pornography pictures and then hiding them within other pictures. What technique did the accused criminal employ?

A. Typography
B. Steganalysis
C. Picture encoding
D. Steganography

Answer: D

NEW QUESTION 402
- (Exam Topic 2)
What will the following Linux command accomplish? dd if=/dev/mem of=/home/sam/mem.bin bs=1024

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

Answer: C

NEW QUESTION 407
- (Exam Topic 2)

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

Answer: B

NEW QUESTION 408
- (Exam Topic 2)
On an Active Directory network using NTLM authentication, where on the domain controllers are the passwords stored?

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

Answer: A

NEW QUESTION 412
- (Exam Topic 2)
NTFS has reduced slack space than FAT, thus having lesser potential to hide data in the slack space. This is because:

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

Answer: C

NEW QUESTION 416
- (Exam Topic 2)
Which of the following techniques can be used to beat steganography?

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

Answer: B

NEW QUESTION 418
- (Exam Topic 2)
Sniffers that place NICs in promiscuous mode work at what layer of the OSI model?

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

Answer: C

NEW QUESTION 422
- (Exam Topic 2)
All Blackberry email is eventually sent and received through what proprietary RIM-operated mechanism?

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

Answer: A

NEW QUESTION 423
- (Exam Topic 2)
Which of the following files gives information about the client sync sessions in Google Drive on Windows?

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

Answer: B

NEW QUESTION 428
- (Exam Topic 2)
Which among the following is an act passed by the U.S. Congress in 2002 to protect investors from the possibility of fraudulent accounting activities by corporations?

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

Answer:

C

NEW QUESTION 430
- (Exam Topic 2)
Which file is a sequence of bytes organized into blocks understandable by the system's linker?

A. executable file
B. source file
C. Object file
D. None of these

Answer: C

NEW QUESTION 435
- (Exam Topic 2)
Why would you need to find out the gateway of a device when investigating a wireless attack?

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

Answer: D

NEW QUESTION 439
- (Exam Topic 2)
The surface of a hard disk consists of several concentric rings known as tracks; each of these tracks has smaller partitions called disk blocks. What is the size of each block?

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

Answer: B

NEW QUESTION 443
- (Exam Topic 2)
Your company's network just finished going through a SAS 70 audit. This audit reported that overall, your network is secure, but there are some areas that needs improvement. The major area was SNMP security. The audit company recommended turning off SNMP, but that is not an option since you have so many remote nodes to keep track of. What step could you take to help secure SNMP on your network?

A. Block all internal MAC address from using SNMP
B. Block access to UDP port 171
C. Block access to TCP port 171
D. Change the default community string names

Answer: D

NEW QUESTION 447
- (Exam Topic 2)
Ivanovich, a forensics investigator, is trying to extract complete information about running processes from a system. Where should he look apart from the RAM and virtual memory?

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

Answer: A

NEW QUESTION 452
- (Exam Topic 2)
What hashing method is used to password protect Blackberry devices?

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

Answer: D

NEW QUESTION 456
- (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 460
- (Exam Topic 2)
When carrying out a forensics investigation, why should you never delete a partition on a dynamic disk?

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

Answer: C

NEW QUESTION 465
- (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 467
- (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 472
- (Exam Topic 2)
Which of the following technique creates a replica of an evidence media?

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

Answer: C

NEW QUESTION 474
- (Exam Topic 2)
When should an MD5 hash check be performed when processing evidence?

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

Answer: C

NEW QUESTION 479
- (Exam Topic 2)
When is it appropriate to use computer forensics?

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

Answer: A

NEW QUESTION 480
- (Exam Topic 2)

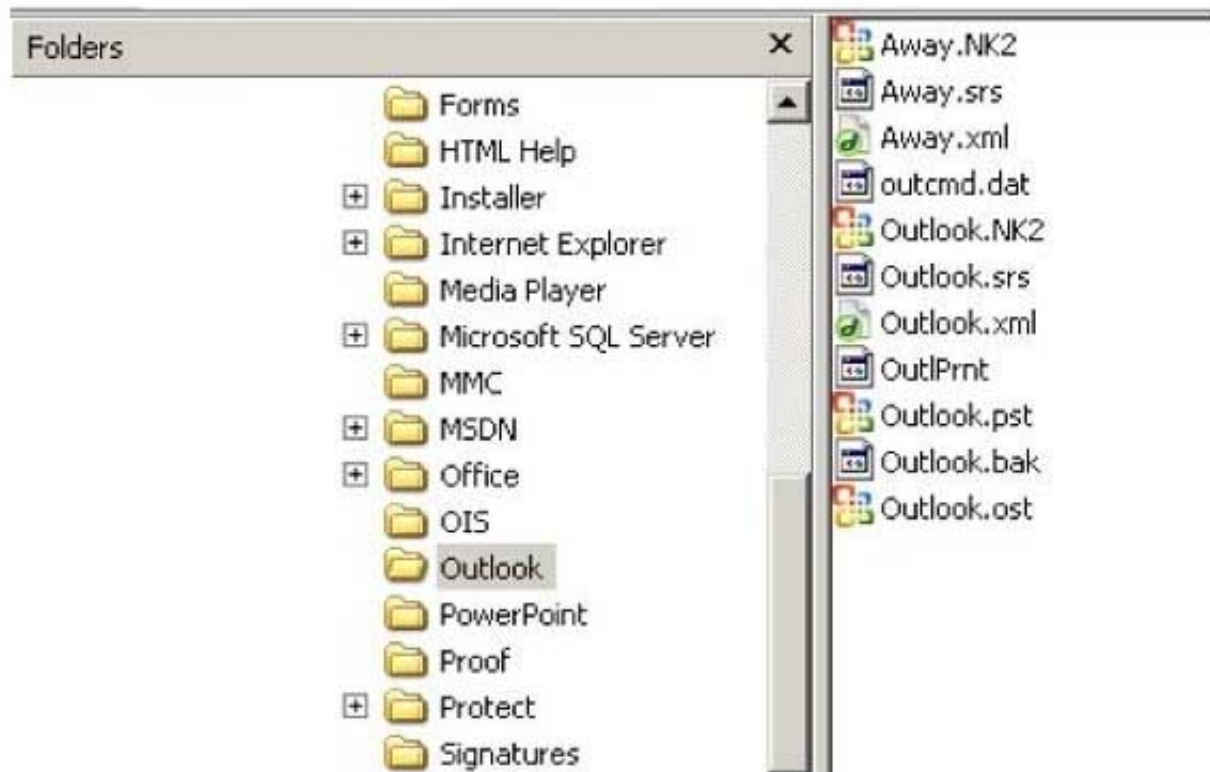Which among the following files provides email header information in the Microsoft Exchange server?

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

Answer: B

NEW QUESTION 481
- (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 483
- (Exam Topic 2)
Jason discovered a file named $RIYG6VR.doc in the C:\$Recycle.Bin\<USER SID>\ while analyzing a hard disk image for the deleted data. What inferences can he make from the file name?

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

Answer: D

NEW QUESTION 485
- (Exam Topic 2)
When operating systems mark a cluster as used but not allocated, the cluster is considered as

A. Corrupt
B. Bad
C. Lost
D. Unallocated

Answer: C

NEW QUESTION 486
- (Exam Topic 2)
What is the default IIS log location?

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

Answer: B

NEW QUESTION 491
- (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 492
- (Exam Topic 2)
What file is processed at the end of a Windows XP boot to initialize the logon dialog box?

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

Answer: A

NEW QUESTION 496
- (Exam Topic 2)
Paul is a computer forensics investigator working for Tyler & Company Consultants. Paul has been called upon to help investigate a computer hacking ring broken up by the local police. Paul begins to inventory the
PCs found in the hackers hideout. Paul then comes across a PDA left by them that is attached to a number of different peripheral devices. What is the first step that Paul must take with the PDA to ensure the integrity of the investigation?

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

Answer: D

NEW QUESTION 501
- (Exam Topic 2)
Smith, as a part his forensic investigation assignment, seized a mobile device. He was asked to recover the Subscriber Identity Module (SIM card) data in the mobile device. Smith found that the SIM was protected by a Personal Identification Number (PIN) code, but he was also aware that people generally leave the PIN numbers to the defaults or use easily guessable numbers such as 1234. He made three unsuccessful attempts, which blocked the SIM card. What can Jason do in this scenario to reset the PIN and access SIM data?

A. He should contact the network operator for a Temporary Unlock Code (TUK)
B. Use system and hardware tools to gain access
C. He can attempt PIN guesses after 24 hours
D. He should contact the network operator for Personal Unlock Number (PUK)

Answer: D

NEW QUESTION 504
- (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 509
- (Exam Topic 2)
Which of the following attacks allows an attacker to access restricted directories, including application source code, configuration and critical system files, and to execute commands outside of the web server's root directory?

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

Answer: C

NEW QUESTION 511
- (Exam Topic 2)
An on-site incident response team is called to investigate an alleged case of computer tampering within their company. Before proceeding with the investigation, the CEO informs them that the incident will be classified as low level. How long will the team have to respond to the incident?

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

Answer: A

NEW QUESTION 516
- (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 518
- (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 522
- (Exam Topic 2)
Which of the following is a list of recently used programs or opened files?

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

Answer: A

NEW QUESTION 526
- (Exam Topic 2)
In handling computer-related incidents, which IT role should be responsible for recovery, containment, and prevention to constituents?

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

Answer: B

NEW QUESTION 530
- (Exam Topic 2)
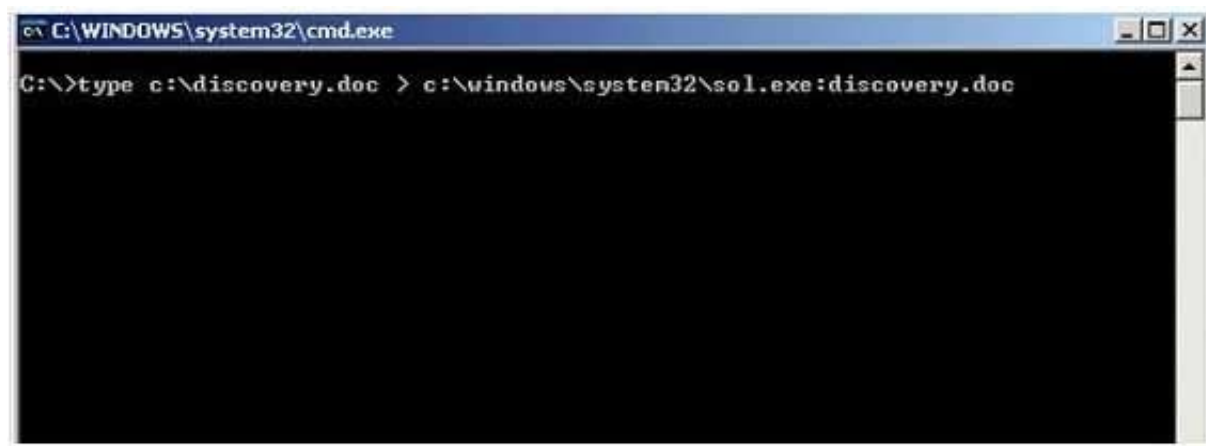At what layer does a cross site scripting attack occur on?

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

Answer: B

NEW QUESTION 531
- (Exam Topic 2)
What feature of Windows is the following command trying to utilize?

```
C:\WINDOWS\system32\cmd.exe                                    _ □ X

C:\>type c:\discovery.doc > c:\windows\system32\sol.exe:discovery.doc
```

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

Answer: C

NEW QUESTION 534
- (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 538
- (Exam Topic 2)
Which of the following is an iOS Jailbreaking tool?

A. Kingo Android ROOT
B. Towelroot
C. One Click Root
D. Redsn0w

Answer: D

NEW QUESTION 541
......

Relate Links

100% Pass Your 312-49v10 Exam with Exambible Prep Materials

https://www.exambible.com/312-49v10-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/