



EC-Council

Exam Questions 312-49v10

Computer Hacking Forensic Investigator (CHFI-v10)

About ExamBible

[Your Partner of IT Exam](#)

Found in 1998

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

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

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

NEW QUESTION 1

- (Exam Topic 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)

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

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

Answer: A

NEW QUESTION 4

- (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 5

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 6

- (Exam Topic 3)

What technique is used by JPEGs for compression?

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

Answer: C

NEW QUESTION 7

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 8

- (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 9

- (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 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 10

- (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 13

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 17

- (Exam Topic 3)

While collecting Active Transaction Logs using SQL Server Management Studio, the query `Select * from ::fn_dblog(NULL, NULL)` displays the active portion of the transaction log file. Here, assigning NULL values implies?

- A. Start and end points for log sequence numbers are specified
- B. Start and end points for log files are not specified
- C. Start and end points for log files are specified
- D. Start and end points for log sequence numbers are not specified

Answer: B

NEW QUESTION 22

- (Exam Topic 3)

Which U.S. law sets the rules for sending emails for commercial purposes, establishes the minimum requirements for commercial messaging, gives the recipients of emails the right to ask the senders to stop emailing them, and spells out the penalties in case the above said rules are violated?

- A. NO-SPAM Act
- B. American: NAVSO P-5239-26 (RLL)
- C. CAN-SPAM Act
- D. American: DoD 5220.22-M

Answer: C

NEW QUESTION 26

- (Exam Topic 3)

What do you call the process in which an attacker uses magnetic field over the digital media device to delete any previously stored data?

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

Answer: C

NEW QUESTION 30

- (Exam Topic 3)

Which component in the hard disk moves over the platter to read and write information?

- A. Actuator
- B. Spindle
- C. Actuator Axis
- D. Head

Answer: D

NEW QUESTION 31

- (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 36

- (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 38

- (Exam Topic 3)

Which of the following tools is not a data acquisition hardware tool?

- A. UltraKit
- B. Atola Insight Forensic
- C. F-Response Imager
- D. Triage-Responder

Answer: C

NEW QUESTION 39

- (Exam Topic 3)

UEFI is a specification that defines a software interface between an OS and platform firmware. Where does this interface store information about files present on a disk?

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

Answer: B

NEW QUESTION 40

- (Exam Topic 3)

Which of the following components within the android architecture stack take care of displaying windows owned by different applications?

- A. Media Framework
- B. Surface Manager
- C. Resource Manager
- D. Application Framework

Answer: D

NEW QUESTION 45

- (Exam Topic 3)

> NMAP -sn 192.168.11.200-215 The NMAP command above performs which of the following?

- A. A trace sweep
- B. A port scan
- C. A ping scan
- D. An operating system detect

Answer: C

NEW QUESTION 47

- (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 51

- (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 52

- (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 53

- (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 55

- (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 57

- (Exam Topic 3)

Which of the following Linux command searches through the current processes and lists the process IDs those match the selection criteria to stdout?

- A. pstree
- B. pgrep
- C. ps
- D. grep

Answer: B

NEW QUESTION 59

- (Exam Topic 3)

An investigator has found certain details after analysis of a mobile device. What can reveal the manufacturer information?

- A. Equipment Identity Register (EIR)
- B. Electronic Serial Number (ESN)
- C. International mobile subscriber identity (IMSI)
- D. Integrated circuit card identifier (ICCID)

Answer: B

NEW QUESTION 62

- (Exam Topic 3)

During an investigation, Noel found the following SIM card from the suspect's mobile. What does the code 89 44 represent?

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

Answer: B

NEW QUESTION 65

- (Exam Topic 3)

Which ISO Standard enables laboratories to demonstrate that they comply with quality assurance and provide valid results?

- A. ISO/IEC 16025
- B. ISO/IEC 18025
- C. ISO/IEC 19025
- D. ISO/IEC 17025

Answer: D

NEW QUESTION 69

- (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 71

- (Exam Topic 3)

Which one of the following is not a first response procedure?

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

Answer: C

NEW QUESTION 73

- (Exam Topic 3)

Which of the following files store the MySQL database data permanently, including the data that had been deleted, helping the forensic investigator in examining the case and finding the culprit?

- A. mysql-bin
- B. mysql-log
- C. iblog
- D. ibdata1

Answer: D

NEW QUESTION 76

- (Exam Topic 3)

What is the framework used for application development for iOS-based mobile devices?

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

Answer: A

NEW QUESTION 81

- (Exam Topic 3)

What is the name of the first reserved sector in File allocation table?

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

Answer: C

NEW QUESTION 85

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 89

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 93

- (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 96

- (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 100

- (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 104

- (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 106

- (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 109

- (Exam Topic 3)

Which list contains the most recent actions performed by a Windows User?

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

Answer: A

NEW QUESTION 111

- (Exam Topic 3)

During forensics investigations, investigators tend to collect the system time at first and compare it with UTC. What does the abbreviation UTC stand for?

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

Answer: A

NEW QUESTION 116

- (Exam Topic 3)

What is the location of a Protective MBR in a GPT disk layout?

- A. Logical Block Address (LBA) 2
- B. Logical Block Address (LBA) 0
- C. Logical Block Address (LBA) 1
- D. Logical Block Address (LBA) 3

Answer: C

NEW QUESTION 121

- (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 122

- (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 124

- (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 127

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 130

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 133

- (Exam Topic 3)

Examination of a computer by a technically unauthorized person will almost always result in:

- A. Rendering any evidence found inadmissible in a court of law
- B. Completely accurate results of the examination
- C. The chain of custody being fully maintained
- D. Rendering any evidence found admissible in a court of law

Answer: A

NEW QUESTION 138

- (Exam Topic 3)

In both pharming and phishing attacks an attacker can create websites that look similar to legitimate sites with the intent of collecting personal identifiable information from its victims. What is the difference between pharming and phishing attacks?

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

Answer: B

NEW QUESTION 141

- (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 144

- (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 146

- (Exam Topic 3)

Which among the following U.S. laws requires financial institutions—companies that offer consumers financial products or services such as loans, financial or

investment advice, or insurance—to protect their customers' information against security threats?

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

Answer: C

NEW QUESTION 151

- (Exam Topic 3)

In which registry does the system store the Microsoft security IDs?

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

Answer: D

NEW QUESTION 154

- (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 157

- (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 158

- (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 161

- (Exam Topic 3)

Which of the following email headers specifies an address for mailer-generated errors, like "no such user" bounce messages, to go to (instead of the sender's address)?

- A. Mime-Version header
- B. Content-Type header
- C. Content-Transfer-Encoding header
- D. Errors-To header

Answer: D

NEW QUESTION 162

- (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 165

- (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 169

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 172

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 175

- (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 180

- (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 183

- (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 187

- (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 188

- (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 190

- (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 193

- (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 195

- (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 197

- (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 198

- (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 203

- (Exam Topic 3)

As part of extracting the system data, Jenifer has used the netstat command. What does this tool reveal?

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

Answer: C

NEW QUESTION 205

- (Exam Topic 3)

Which among the following search warrants allows the first responder to search and seize the victim's computer components such as hardware, software, storage devices, and documentation?

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

Answer: C

NEW QUESTION 209

- (Exam Topic 3)

While analyzing a hard disk, the investigator finds that the file system does not use UEFI-based interface. Which of the following operating systems is present on the hard disk?

- A. Windows 10
- B. Windows 8
- C. Windows 7
- D. Windows 8.1

Answer: C

NEW QUESTION 213

- (Exam Topic 3)

Which cloud model allows an investigator to acquire the instance of a virtual machine and initiate the forensics examination process?

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

Answer: B

NEW QUESTION 217

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 222

- (Exam Topic 3)

Which program uses different techniques to conceal a malware's code, thereby making it difficult for security mechanisms to detect or remove it?

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

Answer: D

NEW QUESTION 227

- (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 229

- (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 232

- (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 233

- (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 237

- (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 241

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 243

- (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 244

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 249

- (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 252

- (Exam Topic 3)

Which of the following standard represents a legal precedent regarding the admissibility of scientific examinations or experiments in legal cases?

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

Answer: C

NEW QUESTION 253

- (Exam Topic 3)

What does the Rule 101 of Federal Rules of Evidence states?

- A. Scope of the Rules, where they can be applied
- B. Purpose of the Rules
- C. Limited Admissibility of the Evidence
- D. Rulings on Evidence

Answer: A

NEW QUESTION 257

- (Exam Topic 3)

Which of the following information is displayed when Netstat is used with -ano switch?

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

Answer: D

NEW QUESTION 261

- (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 262

- (Exam Topic 2)

Which of the following attacks allows an attacker to access restricted directories, including application source code, configuration and critical system files, and to execute commands outside of the web server's root directory?

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

Answer: C

NEW QUESTION 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.

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 269

- (Exam Topic 2)

Which of the following tool creates a bit-by-bit image of an evidence media?

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

Answer: C

NEW QUESTION 274

- (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 278

- (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 280

- (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 282

- (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 287

- (Exam Topic 2)

Tyler is setting up a wireless network for his business that he runs out of his home. He has followed all the directions from the ISP as well as the wireless router manual. He does not have any encryption set and the SSID is being broadcast. On his laptop, he can pick up the wireless signal for short periods of time, but then the connection drops and the signal goes away. Eventually the wireless signal shows back up, but drops intermittently. What could be Tyler issue with his home wireless network?

- A. Computers on his wired network
- B. Satellite television
- C. 2.4Ghz Cordless phones
- D. CB radio

Answer: C

NEW QUESTION 288

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 289

- (Exam Topic 2)

What is the CIDR from the following screenshot?

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

Answer: D

NEW QUESTION 294

- (Exam Topic 2)

What will the following command accomplish in Linux?
fdisk /dev/hda

- A. Partition the hard drive
- B. Format the hard drive
- C. Delete all files under the /dev/hda folder
- D. Fill the disk with zeros

Answer: A

NEW QUESTION 296

- (Exam Topic 2)

What file is processed at the end of a Windows XP boot to initialize the logon dialog box?

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

Answer: A

NEW QUESTION 300

- (Exam Topic 2)

What encryption technology is used on Blackberry devices Password Keeper?

- A. 3DES
- B. AES
- C. Blowfish
- D. RC5

Answer: B

NEW QUESTION 304

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 306

- (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 307

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 309

- (Exam Topic 2)

Wireless access control attacks aim to penetrate a network by evading WLAN access control measures such as AP MAC filters and Wi-Fi port access controls. Which of the following wireless access control attacks allow the attacker to set up a rogue access point outside the corporate perimeter and then lure the employees of the organization to connect to it?

- A. Ad hoc associations
- B. Client mis-association
- C. MAC spoofing
- D. Rogue access points

Answer: B

NEW QUESTION 312

- (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 317

- (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 321

- (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 324

- (Exam Topic 2)

Company ABC has employed a firewall, IDS, Antivirus, Domain Controller, and SIEM. The company's domain controller goes down. From which system would you begin your investigation?

- A. Domain Controller
- B. Firewall
- C. SIEM
- D. IDS

Answer: C

NEW QUESTION 327

- (Exam Topic 2)

While searching through a computer under investigation, you discover numerous files that appear to have had the first letter of the file name replaced by the hex code byte 5h. What does this indicate on the computer?

- A. The files have been marked as hidden
- B. The files have been marked for deletion
- C. The files are corrupt and cannot be recovered
- D. The files have been marked as read-only

Answer: B

NEW QUESTION 328

- (Exam Topic 2)

What must be obtained before an investigation is carried out at a location?

- A. Search warrant
- B. Subpoena
- C. Habeas corpus
- D. Modus operandi

Answer: A

NEW QUESTION 333

- (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 336

- (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 341

- (Exam Topic 2)

What type of attack sends SYN requests to a target system with spoofed IP addresses?

- A. SYN flood
- B. Ping of death
- C. Cross site scripting
- D. Land

Answer: A

NEW QUESTION 344

- (Exam Topic 2)

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

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

Answer: A

NEW QUESTION 347

- (Exam Topic 2)

While presenting his case to the court, Simon calls many witnesses to the stand to testify. Simon decides to call Hillary Taft, a lay witness, to the stand. Since Hillary is a lay witness, what field would she be considered an expert in?

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

Answer: B

NEW QUESTION 349

- (Exam Topic 2)

An expert witness is a _____ who is normally appointed by a party to assist the formulation and preparation of a party's claim or defense.

- A. Expert in criminal investigation
- B. Subject matter specialist
- C. Witness present at the crime scene
- D. Expert law graduate appointed by attorney

Answer: B

NEW QUESTION 351

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 354

- (Exam Topic 2)

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

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

Answer: A

NEW QUESTION 357

- (Exam Topic 2)

What is the slave device connected to the secondary IDE controller on a Linux OS referred to?

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

Answer: B

NEW QUESTION 358

- (Exam Topic 2)

Smith, a forensic examiner, was analyzing a hard disk image to find and acquire deleted sensitive files. He stumbled upon a \$Recycle.Bin folder in the root directory of the disk. Identify the operating system in use.

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

Answer: D

NEW QUESTION 359

- (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 360

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 362

- (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 365

- (Exam Topic 2)

Where is the startup configuration located on a router?

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

Answer: C

NEW QUESTION 367

- (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 368

- (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 371

- (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 376

- (Exam Topic 2)

To check for POP3 traffic using Ethereal, what port should an investigator search by?

- A. 143
- B. 25
- C. 110
- D. 125

Answer: C

NEW QUESTION 379

- (Exam Topic 2)

Which among the following is an act passed by the U.S. Congress in 2002 to protect investors from the possibility of fraudulent accounting activities by corporations?

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

Answer: C

NEW QUESTION 382

- (Exam Topic 2)

What is the primary function of the tool CHKDSK in Windows that authenticates the file system reliability of a volume?

- A. Repairs logical file system errors
- B. Check the disk for hardware errors
- C. Check the disk for connectivity errors
- D. Check the disk for Slack Space

Answer: A

NEW QUESTION 384

- (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 385

- (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 389

- (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 390

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 392

- (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 393

- (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)

Charles has accidentally deleted an important file while working on his Mac computer. He wants to recover the deleted file as it contains some of his crucial business secrets. Which of the following tool will help Charles?

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

Answer: C

NEW QUESTION 402

- (Exam Topic 2)

What is the smallest physical storage unit on a hard drive?

- A. Track
- B. Cluster
- C. Sector
- D. Platter

Answer: C

NEW QUESTION 405

- (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 408

- (Exam Topic 2)

Travis, a computer forensics investigator, is finishing up a case he has been working on for over a month involving copyright infringement and embezzlement. His last task is to prepare an investigative report for the president of the company he has been working for. Travis must submit a hard copy and an electronic copy to this president. In what electronic format should Travis send this report?

- A. TIFF-8
- B. DOC
- C. WPD
- D. PDF

Answer: D

NEW QUESTION 411

- (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 412

- (Exam Topic 2)

Why would a company issue a dongle with the software they sell?

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

Answer: C

NEW QUESTION 414

- (Exam Topic 2)

When marking evidence that has been collected with the “aaa/ddmmyy/nnnn/zz” format, what does the “nnnn” denote?

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

Answer: D

NEW QUESTION 415

- (Exam Topic 2)

All Blackberry email is eventually sent and received through what proprietary RIM-operated mechanism?

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

Answer: A

NEW QUESTION 418

- (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 421

- (Exam Topic 2)

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

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

Answer: A

NEW QUESTION 425

- (Exam Topic 2)

Which of the following is a record of the characteristics of a file system, including its size, the block size, the empty and the filled blocks and their respective counts, the size and location of the inode tables, the disk block map and usage information, and the size of the block groups?

- A. Inode bitmap block
- B. Superblock
- C. Block bitmap block
- D. Data block

Answer: B

NEW QUESTION 426

- (Exam Topic 2)

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

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

Answer: A

NEW QUESTION 427

- (Exam Topic 2)

What technique is used by JPEGs for compression?

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

Answer: C

NEW QUESTION 429

- (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 430

- (Exam Topic 2)

This type of testimony is presented by someone who does the actual fieldwork and does not offer a view in court.

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

Answer: D

NEW QUESTION 433

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 434

- (Exam Topic 2)

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

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

Answer: A

NEW QUESTION 435

- (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 439

- (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 440

- (Exam Topic 2)

In handling computer-related incidents, which IT role should be responsible for recovery, containment, and prevention to constituents?

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

Answer: B

NEW QUESTION 441

- (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 442

- (Exam Topic 2)

Which of the following Registry components include offsets to other cells as well as the LastWrite time for the key?

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

Answer: C

NEW QUESTION 446

- (Exam Topic 2)

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

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

Answer: A

NEW QUESTION 451

- (Exam Topic 2)

Which of the following techniques can be used to beat steganography?

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

Answer: B

NEW QUESTION 455

- (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.

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 459

- (Exam Topic 2)

Files stored in the Recycle Bin in its physical location are renamed as Dxy.ext, where “x” represents the _____.

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

Answer: A

NEW QUESTION 461

- (Exam Topic 2)

Which of the following is NOT a part of pre-investigation phase?

- A. Building forensics workstation
- B. Gathering information about the incident
- C. Gathering evidence data
- D. Creating an investigation team

Answer: C

NEW QUESTION 464

- (Exam Topic 2)

When a router receives an update for its routing table, what is the metric value change to that path?

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

Answer: C

NEW QUESTION 465

- (Exam Topic 2)

Why should you never power on a computer that you need to acquire digital evidence from?

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

Answer: A

NEW QUESTION 467

- (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 469

- (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 470

- (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 473

- (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 475

- (Exam Topic 2)

Why would you need to find out the gateway of a device when investigating a wireless attack?

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

Answer: D

NEW QUESTION 480

- (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 481

- (Exam Topic 2)

What hashing method is used to password protect Blackberry devices?

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

Answer: D

NEW QUESTION 485

- (Exam Topic 2)

Which password cracking technique uses details such as length of password, character sets used to construct the password, etc.?

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

Answer: A

NEW QUESTION 489

- (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 492

- (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 497

- (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 499

- (Exam Topic 1)

Why should you note all cable connections for a computer you want to seize as evidence?

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

D. to know what hardware existed

Answer: A

NEW QUESTION 503

- (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 506

- (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 509

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 514

- (Exam Topic 1)

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

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

Answer: A

NEW QUESTION 518

- (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 521

- (Exam Topic 1)

Jessica works as systems administrator for a large electronics firm. She wants to scan her network quickly to detect live hosts by using ICMP ECHO Requests. What type of scan is Jessica going to perform?

- A. Tracert
- B. Smurf scan
- C. Ping trace
- D. ICMP ping sweep

Answer: D

NEW QUESTION 522

- (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 527

- (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 530

- (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 535

- (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 540

- (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 544

- (Exam Topic 1)

The objective of this act was to protect consumers' personal financial information held by financial institutions and their service providers.

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

Answer: A

NEW QUESTION 547

- (Exam Topic 1)

Michael works for Kimball Construction Company as senior security analyst. As part of yearly security audit, Michael scans his network for vulnerabilities. Using Nmap, Michael conducts XMAS scan and most of the ports scanned do not give a response. In what state are these ports?

- A. Closed
- B. Open
- C. Stealth
- D. Filtered

Answer: B

NEW QUESTION 552

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 555

- (Exam Topic 1)

Area density refers to:

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

Answer: A

NEW QUESTION 556

- (Exam Topic 1)

Printing under a Windows Computer normally requires which one of the following files types to be created?

- A. EME
- B. MEM
- C. EMF
- D. CME

Answer: C

NEW QUESTION 558

- (Exam Topic 1)

What is kept in the following directory? HKLM\SECURITY\Policy\Secrets

- A. Cached password hashes for the past 20 users
- B. Service account passwords in plain text
- C. IAS account names and passwords
- D. Local store PKI Kerberos certificates

Answer: B

NEW QUESTION 559

- (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 561

- (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 564

- (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 565

- (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 568

- (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 573

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 577

- (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 582

- (Exam Topic 1)

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

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

Answer: D

NEW QUESTION 583

- (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 587

- (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 592

- (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 594

- (Exam Topic 1)

Office Documents (Word, Excel and PowerPoint) contain a code that allows tracking the MAC or unique identifier of the machine that created the document. What is that code called?

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

Answer: A

NEW QUESTION 599

- (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 601

- (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 605

- (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 609

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 611

- (Exam Topic 1)

What is the name of the Standard Linux Command that is also available as windows application that can be used to create bit-stream images?

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

Answer: D

NEW QUESTION 612

- (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 616

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 620

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 625

- (Exam Topic 1)

During the course of a corporate investigation, you find that an Employee is committing a crime. Can the Employer file a criminal complaint with Police?

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

Answer: A

NEW QUESTION 628

- (Exam Topic 1)

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

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

Answer: A

NEW QUESTION 629

- (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 630

- (Exam Topic 1)

In the context of file deletion process, which of the following statement holds true?

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

Answer: C

NEW QUESTION 634

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 639

- (Exam Topic 1)

Microsoft Outlook maintains email messages in a proprietary format in what type of file?

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

Answer: C

NEW QUESTION 641

- (Exam Topic 1)

You are working as a Computer forensics investigator for a corporation on a computer abuse case. You discover evidence that shows the subject of your

investigation is also embezzling money from the company. The company CEO and the corporate legal counsel advise you to contact law enforcement and provide them with the evidence that you have found. The law enforcement officer that responds requests that you put a network sniffer on your network and monitor all traffic to the subject's computer. You inform the officer that you will not be able to comply with that request because doing so would:

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

Answer: C

NEW QUESTION 642

- (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 643

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 646

- (Exam Topic 1)

What is the following command trying to accomplish?

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

Answer: A

NEW QUESTION 649

- (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 650

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 655

- (Exam Topic 1)

What should you do when approached by a reporter about a case that you are working on or have worked on?

- A. Refer the reporter to the attorney that retained you
- B. Say, "no comment"

- C. Answer all the reporter's questions as completely as possible
- D. Answer only the questions that help your case

Answer: A

NEW QUESTION 660

- (Exam Topic 1)

What file structure database would you expect to find on floppy disks?

- A. NTFS
- B. FAT32
- C. FAT16
- D. FAT12

Answer: D

NEW QUESTION 663

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 668

- (Exam Topic 1)

You have been asked to investigate after a user has reported a threatening e-mail they have received from an external source. Which of the following are you most interested in when trying to trace the source of the message?

- A. The X509 Address
- B. The SMTP reply Address
- C. The E-mail Header
- D. The Host Domain Name

Answer: C

NEW QUESTION 672

- (Exam Topic 1)

How many characters long is the fixed-length MD5 algorithm checksum of a critical system file?

- A. 128
- B. 64
- C. 32
- D. 16

Answer: C

NEW QUESTION 673

- (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 677

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 682

- (Exam Topic 1)

If you plan to startup a suspect's computer, you must modify the _____ to ensure that you do not contaminate or alter data on the suspect's hard drive by booting to the hard drive.

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

Answer: C

NEW QUESTION 684

- (Exam Topic 1)

Frank is working on a vulnerability assessment for a company on the West coast. The company hired Frank to assess its network security through scanning, pen tests, and vulnerability assessments. After discovering numerous known vulnerabilities detected by a temporary IDS he set up, he notices a number of items that show up as unknown but Questionable in the logs. He looks up the behavior on the Internet, but cannot find anything related. What organization should Frank submit the log to find out if it is a new vulnerability or not?

- A. APIPA
- B. IANA
- C. CVE
- D. RIPE

Answer: C

NEW QUESTION 687

- (Exam Topic 1)

Kimberly is studying to be an IT security analyst at a vocational school in her town. The school offers many different programming as well as networking languages. What networking protocol language should she learn that routers utilize?

- A. ATM
- B. UDP
- C. BPG
- D. OSPF

Answer: D

NEW QUESTION 689

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 690

- (Exam Topic 1)

Which is a standard procedure to perform during all computer forensics investigations?

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

Answer: A

NEW QUESTION 691

- (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 692

- (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 694

- (Exam Topic 1)

When you carve an image, recovering the image depends on which of the following skills?

- A. Recognizing the pattern of the header content
- B. Recovering the image from a tape backup
- C. Recognizing the pattern of a corrupt file
- D. Recovering the image from the tape backup

Answer: A

NEW QUESTION 695

- (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 700

- (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 705

- (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 707

- (Exam Topic 1)

You are contracted to work as a computer forensics investigator for a regional bank that has four 30 TB storage area networks that store customer data.

What method would be most efficient for you to acquire digital evidence from this network?

- A. create a compressed copy of the file with DoubleSpace
- B. create a sparse data copy of a folder or file
- C. make a bit-stream disk-to-image file
- D. make a bit-stream disk-to-disk file

Answer: C

NEW QUESTION 708

- (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 713

- (Exam Topic 1)

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

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

Answer: A

NEW QUESTION 714

- (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 719

- (Exam Topic 1)

You are carrying out the last round of testing for your new website before it goes live. The website has many dynamic pages and connects to a SQL backend that accesses your product inventory in a database. You come across a web security site that recommends inputting the following code into a search field on web pages to check for vulnerabilities: When you type this and click on search, you receive a pop-up window that says: "This is a test." What is the result of this test?

- A. Your website is vulnerable to CSS
- B. Your website is not vulnerable
- C. Your website is vulnerable to SQL injection
- D. Your website is vulnerable to web bugs

Answer: A

NEW QUESTION 721

- (Exam Topic 1)

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

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

Answer: D

NEW QUESTION 725

- (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 730

- (Exam Topic 1)

What is a good security method to prevent unauthorized users from "tailgating"?

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

Answer: A

NEW QUESTION 735

- (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 736

- (Exam Topic 1)

Melanie was newly assigned to an investigation and asked to make a copy of all the evidence from the compromised system. Melanie did a DOS copy of all the files on the system. What would be the primary reason for you to recommend a disk imaging tool?

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

Answer: C

NEW QUESTION 738

- (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 739

- (Exam Topic 1)

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

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

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

Answer: A

NEW QUESTION 744

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 746

- (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 748

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 750

- (Exam Topic 1)

It takes _____ mismanaged case/s to ruin your professional reputation as a computer forensics examiner?

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

Answer: C

NEW QUESTION 755

- (Exam Topic 1)

_____ is simply the application of Computer Investigation and analysis techniques in the interests of determining potential legal evidence.

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

Answer: B

NEW QUESTION 759

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 764

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 769

- (Exam Topic 1)

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

```
#include <stdio.h>
#include <string.h>
int main(int argc, char *argv[]) {
    char buffer[10];
    if (argc < 2) {
        fprintf(stderr, "USAGE: %s string\n", argv[0]);
        return 1;
    }
    strcpy(buffer, argv[1]);
    return 0;
}
```

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

Answer: A

NEW QUESTION 770

- (Exam Topic 1)

What is the target host IP in the following command?

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

Answer: A

NEW QUESTION 771

- (Exam Topic 1)

Simon is a former employee of Trinitron XML Inc. He feels he was wrongly terminated and wants to hack into his former company's network. Since Simon remembers some of the server names, he attempts to run the axfr and ixfr commands using DIG. What is Simon trying to accomplish here?

- A. Send DOS commands to crash the DNS servers
- B. Perform DNS poisoning
- C. Perform a zone transfer
- D. Enumerate all the users in the domain

Answer: C

NEW QUESTION 776

- (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 780

- (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 783

- (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 784

- (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 785

- (Exam Topic 1)

Diskcopy is:

- A. a utility by AccessData
- B. a standard MS-DOS command
- C. Digital Intelligence utility
- D. dd copying tool

Answer: B

Explanation:

diskcopy is a STANDARD DOS utility. C:\WINDOWS>diskcopy /? Copies the contents of one floppy disk to another.

NEW QUESTION 789

- (Exam Topic 1)

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

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

Answer: A

NEW QUESTION 792

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 795

- (Exam Topic 1)

Law enforcement officers are conducting a legal search for which a valid warrant was obtained.

While conducting the search, officers observe an item of evidence for an unrelated crime that was not included in the warrant. The item was clearly visible to the officers and immediately identified as evidence. What is the term used to describe how this evidence is admissible?

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

Answer: A

NEW QUESTION 800

- (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 805

.....

Relate Links

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

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

Contact us

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

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