Exam Questions 312-49v9

ECCouncil Computer Hacking Forensic Investigator (V9)

https://www.2passeasy.com/dumps/312-49v9/

NEW QUESTION 1
The Electronic Serial Number (ESN) is a unique _ recorded on a secure chip in a mobile phone by the manufacturer.

A. 16-bit identifier
B. 24-bit identifier
C. 32-bit identifier
D. 64-bit identifier

Answer: C

NEW QUESTION 2
Event correlation is a procedure that is assigned with a new meaning for a set of events that occur in a predefined interval of time.
Which type of correlation will you use if your organization wants to use different OS and network hardware platforms throughout the network?

A. Same-platform correlation
B. Cross-platform correlation
C. Multiple-platform correlation
D. Network-platform correlation

Answer: B

NEW QUESTION 3
The Recycle Bin is located on the Windows desktop. When you delete an item from the hard disk, Windows sends that deleted item to the Recycle Bin and the icon changes to full from empty, but items deleted from removable media, such as a floppy disk or network drive, are not stored in the Recycle Bin.
What is the size limit for Recycle Bin in Vista and later versions of the Windows?

A. No size limit
B. Maximum of 3.99 GB
C. Maximum of 4.99 GB
D. Maximum of 5.99 GB

Answer: A

NEW QUESTION 4
The need for computer forensics is highlighted by an exponential increase in the number of cybercrimes and litigations where large organizations were involved. Computer forensics plays an important role in tracking the cyber criminals. The main role of computer forensics is to:

A. Maximize the investigative potential by maximizing the costs
B. Harden organization perimeter security
C. Document monitoring processes of employees of the organization
D. Extract, process, and interpret the factual evidence so that it proves the attacker's actions in the court

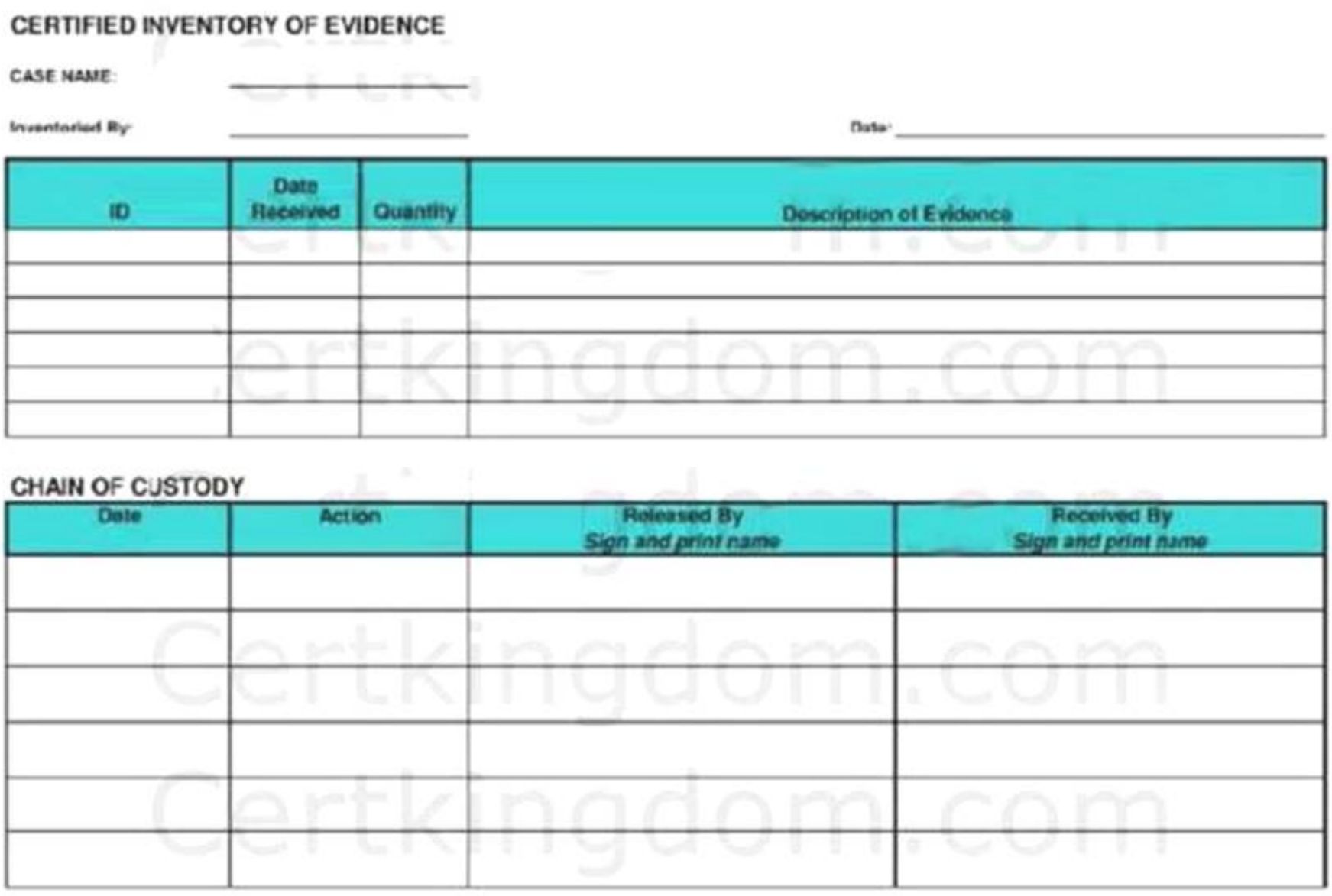
Answer: D

NEW QUESTION 5
Smith, an employee of a reputed forensic Investigation firm, has been hired by a private organization to investigate a laptop that is suspected to be involved in hacking of organization DC server. Smith wants to find all the values typed into the Run box in the Start menu. Which of the following registry key Smith will check to find the above information?

A. UserAssist Key
B. MountedDevices key
C. RunMRU key
D. TypedURLs key

Answer: C

NEW QUESTION 6
What document does the screenshot represent?



CERTIFIED INVENTORY OF EVIDENCE

CASE NAME: _____

Inventoried By: _____ Date: _____

ID	Date Received	Quantity	Description of Evidence

CHAIN OF CUSTODY

Date	Action	Released By *Sign and print name*	Received By *Sign and print name*

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

Answer: A

NEW QUESTION 7
Which of the following commands shows you all of the network services running on Windows-based servers?

A. Net start
B. Net use
C. Net Session
D. Net share

Answer: A

NEW QUESTION 8
Which of the following statements is incorrect related to acquiring electronic evidence at crime scene?

A. Sample banners are used to record the system activities when used by the unauthorized user
B. In warning banners, organizations give clear and unequivocal notice to intruders that by signing onto the system they are expressly consenting to such monitoring
C. The equipment is seized which is connected to the case, knowing the role of the computer which will indicate what should be taken
D. At the time of seizing process, you need to shut down the computer immediately

Answer: D

NEW QUESTION 9
Injection flaws are web application vulnerabilities that allow untrusted data to be Interpreted and executed as part of a command or query. Attackers exploit injection flaws by constructing malicious commands or queries that result in data loss or corruption, lack of accountability, or denial of access. Which of the following injection flaws involves the injection of malicious code through a web application?

A. SQL Injection
B. Password brute force
C. Nmap Scanning
D. Footprinting

Answer: A

NEW QUESTION 10
Which of the following commands shows you the NetBIOS name table each?

A. nbtstat -n
B. nbtstat -c
C. nbtstat -r
D. nbtstat -s

Answer: A

NEW QUESTION 10
What is a bit-stream copy?

A. Bit-Stream Copy is a bit-by-bit copy of the original storage medium and exact copy of the original disk
B. A bit-stream image is the file that contains the NTFS files and folders of all the data on a disk or partition
C. A bit-stream image is the file that contains the FAT32 files and folders of all the data on a disk or partition
D. Creating a bit-stream image transfers only non-deleted files from the original disk to the image disk

Answer: A

NEW QUESTION 12
Which of the following is not a part of disk imaging tool requirements?

A. The tool should not change the original content
B. The tool should log I/O errors in an accessible and readable form, including the type and location of the error
C. The tool must have the ability to be held up to scientific and peer review
D. The tool should not compute a hash value for the complete bit stream copy generated from an image file of the source

Answer: D

NEW QUESTION 13
Attackers can manipulate variables that reference files with "dot-dot-slash (./)" sequences and their variations such as
http://www.juggyDoy.corn/GET/process.php././././././././etc/passwd.
Identify the attack referred.

A. Directory traversal
B. SQL Injection
C. XSS attack
D. File injection

Answer: A

NEW QUESTION 15
What is a SCSI (Small Computer System Interface)?

A. A set of ANSI standard electronic interfaces that allow personal computers to communicate with peripheral hardware such as disk drives, tape drive
B. CD-ROM drives, printers, and scanners
C. A standard electronic interface used between a computer motherboard's data paths or bus and the computer's disk storage devices
D. A "plug-and-play" interface, which allows a device to be added without an adapter card and without rebooting the computer
E. A point-to-point serial bi-directional interface for transmitting data between computer devices at data rates of up to 4 Gbps

Answer: A

NEW QUESTION 19
Network forensics can be defined as the sniffing, recording, acquisition and analysis of the network traffic and event logs in order to investigate a network security incident.

A. True
B. False

Answer: A

NEW QUESTION 24
Digital evidence validation involves using a hashing algorithm utility to create a binary or hexadecimal number that represents the uniqueness of a data set, such as a disk drive or file.
Which of the following hash algorithms produces a message digest that is 128 bits long?

A. CRC-32
B. MD5
C. SHA-1
D. SHA-512

Answer: B

NEW QUESTION 25
LBA (Logical Block Address) addresses data by allotting a to each sector of the hard disk.

A. Sequential number

B. Index number
C. Operating system number
D. Sector number

Answer: A

NEW QUESTION 26
Which of the following attacks allows attacker to acquire access to the communication channels between the victim and server to extract the information?

A. Man-in-the-middle (MITM) attack
B. Replay attack
C. Rainbow attack
D. Distributed network attack

Answer: A

NEW QUESTION 30
What is the First Step required in preparing a computer for forensics investigation?

A. Do not turn the computer off or on, run any programs, or attempt to access data on a computer
B. Secure any relevant media
C. Suspend automated document destruction and recycling policies that may pertain to any relevant media or users at Issue
D. Identify the type of data you are seeking, the Information you are looking for, and the urgency level of the examination

Answer: A

NEW QUESTION 32
An Internet standard protocol (built on top of TCP/IP) that assures accurate synchronization to the millisecond of computer clock times in a network of computers. Which of the following statement is true for NTP Stratum Levels?

A. Stratum-0 servers are used on the network; they are not directly connected to computers which then operate as stratum-1 servers
B. Stratum-1 time server is linked over a network path to a reliable source of UTC time such as GPS, WWV, or CDMA transmissions
C. A stratum-2 server is directly linked (not over a network path) to a reliable source of UTC time such as GPS, WWV, or CDMA transmissions
D. A stratum-3 server gets its time over a network link, via NTP, from a stratum-2 server, and so on

Answer: D

NEW QUESTION 36
A forensic investigator is a person who handles the complete Investigation process, that is, the preservation, identification, extraction, and documentation of the evidence. The investigator has many roles and responsibilities relating to the cybercrime analysis. The role of the forensic investigator is to:

A. Take permission from all employees of the organization for investigation
B. Harden organization network security
C. Create an image backup of the original evidence without tampering with potential evidence
D. Keep the evidence a highly confidential and hide the evidence from law enforcement agencies

Answer: C

NEW QUESTION 37
Digital photography helps in correcting the perspective of the Image which Is used In taking the measurements of the evidence. Snapshots of the evidence and incident-prone areas need to be taken to help in the forensic process. Is digital photography accepted as evidence in the court of law?

A. Yes
B. No

Answer: A

NEW QUESTION 41
Which one of the following is not a consideration in a forensic readiness planning checklist?

A. Define the business states that need digital evidence
B. Identify the potential evidence available
C. Decide the procedure for securely collecting the evidence that meets the requirement fn a forensically sound manner
D. Take permission from all employees of the organization

Answer: D

NEW QUESTION 42
Shortcuts are the files with the extension .Ink that are created and are accessed by the users. These files provide you with information about:

A. Files or network shares
B. Running application
C. Application logs
D. System logs

Answer: A

NEW QUESTION 46
A computer forensic report is a report which provides detailed information on the complete forensics investigation process.

A. True
B. False

Answer: A

NEW QUESTION 48
Computer security logs contain information about the events occurring within an organization's systems and networks. Application and Web server log files are useful in detecting web attacks. The source, nature, and time of the attack can be determined by ____ of the compromised system.

A. Analyzing log files
B. Analyzing SAM file
C. Analyzing rainbow tables
D. Analyzing hard disk boot records

Answer: A

NEW QUESTION 52
What is a first sector ("sector zero") of a hard disk?

A. Master boot record
B. System boot record
C. Secondary boot record
D. Hard disk boot record

Answer: A

NEW QUESTION 53
Ever-changing advancement or mobile devices increases the complexity of mobile device examinations. Which or the following is an appropriate action for the mobile forensic investigation?

A. To avoid unwanted interaction with devices found on the scene, turn on any wireless interfaces such as Bluetooth and Wi-Fi radios
B. Do not wear gloves while handling cell phone evidence to maintain integrity of physical evidence
C. If the device's display is O
D. the screen's contents should be photographed and, if necessary, recorded manually, capturing the time, service status, battery level, and other displayed icons
E. If the phone is in a cradle or connected to a PC with a cable, then unplug the device from the computer

Answer: C

NEW QUESTION 57
When a system is compromised, attackers often try to disable auditing, in Windows 7; modifications to the audit policy are recorded as entries of Event ID_____ .

A. 4902
B. 3902
C. 4904
D. 3904

Answer: A

NEW QUESTION 60
Files stored in the Recycle Bin in its physical location are renamed as Dxy.ext, where, “X” represents the .

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

Answer: A

NEW QUESTION 62
Which of the following commands shows you the names of all open shared files on a server and number of file locks on each file?

A. Net sessions
B. Net file
C. Netconfig
D. Net share

Answer: B

NEW QUESTION 63

International Mobile Equipment Identifier (IMEI) is a 15-dlgit 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. Device Origin Code (DOC)
C. Manufacturer identification Code (MIC)
D. Integrated Circuit Code (ICC)

Answer: A

NEW QUESTION 68
Who is responsible for the following tasks?
? Secure the scene and ensure that it is maintained In a secure state until the Forensic Team advises
? Make notes about the scene that will eventually be handed over to the Forensic Team

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

Answer: A

NEW QUESTION 70
You should always work with original evidence

A. True
B. False

Answer: B

NEW QUESTION 72
During first responder procedure you should follow all laws while collecting the evidence, and contact a computer forensic examiner as soon as possible

A. True
B. False

Answer: A

NEW QUESTION 73
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, to cause a denial-of-service attack?

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

Answer: B

NEW QUESTION 74
Web applications provide an Interface between end users and web servers through a set of web pages that are generated at the server-end or contain script code to be executed dynamically within the client Web browser.

A. True
B. False

Answer: A

NEW QUESTION 76
Under no circumstances should anyone, with the exception of qualified computer forensics personnel, make any attempts to restore or recover information from a computer system or device that holds electronic information.

A. True
B. False

Answer: A

NEW QUESTION 77
In which step of the computer forensics investigation methodology would you run MD5 checksum on the evidence?

A. Obtain search warrant
B. Evaluate and secure the scene
C. Collect the evidence
D. Acquire the data

Answer: D

NEW QUESTION 81
When the operating system marks cluster as used, but does not allocate them to any file, such clusters are known as ____.

A. Lost clusters
B. Bad clusters
C. Empty clusters
D. Unused clusters

Answer: A

NEW QUESTION 83
Syslog is a client/server protocol standard for forwarding log messages across an IP network. Syslog uses ___ to transfer log messages in a clear text format.

A. TCP
B. FTP
C. SMTP
D. POP

Answer: A

NEW QUESTION 88
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 7029
B. 18 USC 7030
C. 18 USC 7361
D. 18 USC 7371

Answer: B

NEW QUESTION 90
If the partition size Is 4 GB, each cluster will be 32 K. Even If a file needs only 10 K, the entire 32 K will be allocated, resulting In 22 K of ____.

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

Answer: A

NEW QUESTION 94
Deposition enables opposing counsel to preview an expert witness's testimony at trial. Which of the following deposition is not a standard practice?

A. Both attorneys are present
B. Only one attorneys is present
C. No jury or judge
D. Opposing counsel asks questions

Answer: B

NEW QUESTION 98
Which of the following statements does not support the case assessment?

A. Review the case investigator's request for service
B. Identify the legal authority for the forensic examination request
C. Do not document the chain of custody
D. Discuss whether other forensic processes need to be performed on the evidence

Answer: C

NEW QUESTION 101
Task list command displays a list of applications and services with their Process ID (PID) for all tasks running on either a local or a remote computer.
Which of the following task list commands provides information about the listed processes, including the image name, PID, name, and number of the session for the process?

A. tasklist/s
B. tasklist/u
C. tasklist/p
D. tasklist/V

Answer: D

NEW QUESTION 102
A mobile operating system is the operating system that operates a mobile device like a mobile phone, smartphone, PDA, etc. It determines the functions and features available on mobile devices such as keyboards, applications, email, text messaging, etc. Which of the following mobile operating systems is free and open source?

A. Web OS
B. Android
C. Apple IOS
D. Symbian OS

Answer: B

NEW QUESTION 107
JPEG is a commonly used method of compressing photographic Images. It uses a compression algorithm to minimize the size of the natural image, without affecting the quality of the image. The JPEG lossy algorithm divides the image in separate blocks of ____.

A. 4x4 pixels
B. 8x8 pixels
C. 16x16 pixels
D. 32x32 pixels

Answer: B

NEW QUESTION 108
Jason, a renowned forensic investigator, is investigating a network attack that resulted in the compromise of several systems in a reputed multinational's network. He started Wireshark to capture the network traffic. Upon investigation, he found that the DNS packets travelling across the network belonged to a non-company configured IP. Which of the following attack Jason can infer from his findings?

A. DNS Poisoning
B. Cookie Poisoning Attack
C. DNS Redirection
D. Session poisoning

Answer: A

NEW QUESTION 109
First response to an incident may involve three different groups of people, and each will have differing skills and need to carry out differing tasks based on the incident. Who is responsible for collecting, preserving, and packaging electronic evidence?

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

Answer: C

NEW QUESTION 113
Quality of a raster Image is determined by the ____ and the amount of information in each pixel.

A. Total number of pixels
B. Image file format
C. Compression method
D. Image file size

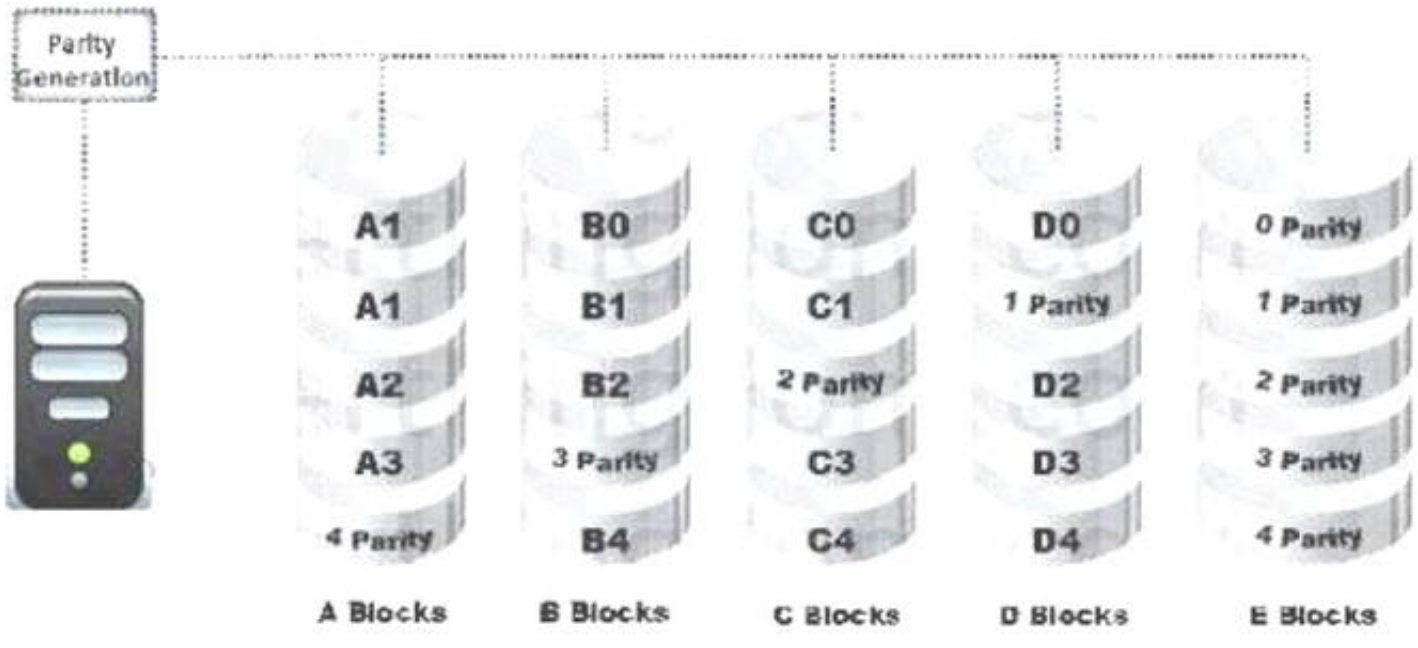
Answer: A

NEW QUESTION 115
What is a chain of custody?

A. A legal document that demonstrates the progression of evidence as it travels from the original evidence location to the forensic laboratory
B. It is a search warrant that is required for seizing evidence at a crime scene
C. It Is a document that lists chain of windows process events
D. Chain of custody refers to obtaining preemptive court order to restrict further damage of evidence in electronic seizures

Answer: A

NEW QUESTION 116
Data is striped at a byte level across multiple drives and parity information is distributed among all member drives.



What RAID level is represented here?

A. RAID Level0
B. RAID Level 1
C. RAID Level 3
D. RAID Level 5

Answer: D

NEW QUESTION 119
Wi-Fi Protected Access (WPA) is a data encryption method for WLANs based on 802.11 standards. Temporal Key Integrity Protocol (TKIP) enhances WEP by adding a rekeying mechanism to provide fresh encryption and integrity keys. Temporal keys are changed for every ____ .

A. 5,000 packets
B. 10.000 packets
C. 15,000 packets
D. 20.000 packets

Answer: B

NEW QUESTION 122
Email archiving is a systematic approach to save and protect the data contained in emails so that it can be accessed fast at a later date. There are two main archive types, namely Local Archive and Server Storage Archive. Which of the following statements is correct while dealing with local archives?

A. It is difficult to deal with the webmail as there is no offline archive in most case
B. So consult your counsel on the case as to the best way to approach and gain access to the required data on servers
C. Local archives do not have evidentiary value as the email client may alter the message data
D. Local archives should be stored together with the server storage archives in order to be admissible in a court of law
E. Server storage archives are the server information and settings stored on a local system whereas the local archives are the local email client information stored on the mail server

Answer: A

NEW QUESTION 126
A system with a simple logging mechanism has not been given much attention during development, this system is now being targeted by attackers, if the attacker wants to perform a new line injection attack, what will he/she inject into the log file?

A. Plaintext
B. Single pipe character
C. Multiple pipe characters
D. HTML tags

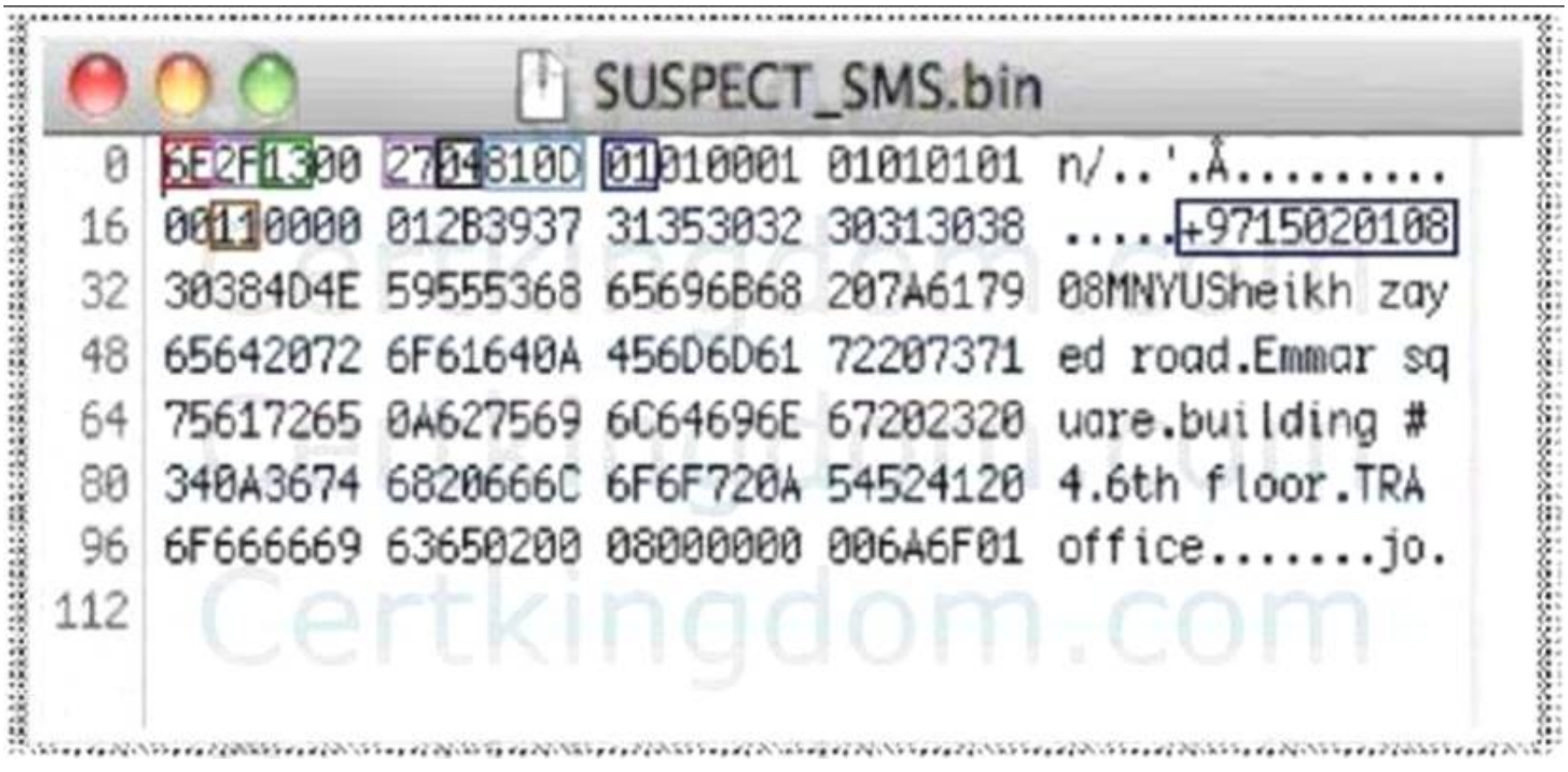
Answer: A

NEW QUESTION 130
Windows Security Accounts Manager (SAM) is a registry file which stores passwords in a hashed format. SAM file in Windows is located at:

A. C:\windows\system32\config\SAM
B. C:\windows\system32\con\SAM
C. C:\windows\system32\Boot\SAM
D. C:\windows\system32\drivers\SAM

Answer: A

NEW QUESTION 134
Determine the message length from following hex viewer record:



A. 6E2F
B. 13
C. 27
D. 810D

Answer: D

NEW QUESTION 136
What is the first step that needs to be carried out to investigate wireless attacks?

A. Obtain a search warrant
B. Identify wireless devices at crime scene
C. Document the scene and maintain a chain of custody
D. Detect the wireless connections

Answer: A

NEW QUESTION 139
You can interact with the Registry through intermediate programs. Graphical user interface (GUI) Registry editors such as Regedit.exe or Regedt32 exe are commonly used as intermediate programs in Windows 7. Which of the following is a root folder of the registry editor?

A. HKEY_USERS
B. HKEY_LOCAL_ADMIN
C. HKEY_CLASSES_ADMIN
D. HKEY_CLASSES_SYSTEM

Answer: A

NEW QUESTION 140
Which of the following is not an example of a cyber-crime?

A. Fraud achieved by the manipulation of the computer records
B. Firing an employee for misconduct
C. Deliberate circumvention of the computer security systems
D. Intellectual property theft, including software piracy

Answer: B

NEW QUESTION 144
Hard disk data addressing is a method of allotting addresses to each ___ of data on a hard disk

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

Answer: A

NEW QUESTION 147
Computer security logs contain information about the events occurring within an organization's systems and networks. Which of the following security logs contains Logs of network and host-based security software?

A. Operating System (OS) logs
B. Application logs
C. Security software logs
D. Audit logs

Answer: C

NEW QUESTION 150
Which of the following file in Novel GroupWise stores information about user accounts?

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

Answer: A

NEW QUESTION 151
Mobile phone forensics is the science of recovering digital evidence from a mobile phone under forensically sound conditions.

A. True
B. False

Answer: A

NEW QUESTION 155
File deletion is a way of removing a file from a computer's file system. What happens when a file is deleted in windows7?

A. The last letter of a file name is replaced by a hex byte code E5h
B. The operating system marks the file's name in the MFT with a special character that indicates that the file has been deleted
C. Corresponding clusters in FAT are marked as used
D. The computer looks at the clusters occupied by that file and does not avails space to store a new file

Answer: B

NEW QUESTION 157
Raw data acquisition format creates ____ of a data set or suspect drive.

A. Simple sequential flat files
B. Segmented files
C. Compressed image files
D. Segmented image files

Answer: A

NEW QUESTION 162
A rogue/unauthorized access point is one that Is not authorized for operation by a particular firm or network

A. True
B. False

Answer: A

NEW QUESTION 163
Which of the following passwords are sent over the wire (and wireless) network, or stored on some media as it is typed without any alteration?

A. Clear text passwords
B. Obfuscated passwords
C. Hashed passwords
D. Hex passwords

Answer: A

NEW QUESTION 167
Wireless network discovery tools use two different methodologies to detect, monitor and log a WLAN device (i.e. active scanning and passive scanning). Active scanning methodology involves ____ and waiting for responses from available wireless networks.

A. Broadcasting a probe request frame
B. Sniffing the packets from the airwave
C. Scanning the network
D. Inspecting WLAN and surrounding networks

Answer: A

NEW QUESTION 169
Graphics Interchange Format (GIF) is a ____ RGB bitmap Image format for Images with up to 256 distinct colors per frame.

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

Answer: A

NEW QUESTION 172
You have been given the task to investigate web attacks on a Windows-based server.
Which of the following commands will you use to look at which sessions the machine has opened with other systems?

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

Answer: B

NEW QUESTION 175
Netstat is a tool for collecting Information regarding network connections. It provides a simple view of TCP and UDP connections, and their state and network traffic statistics.
Which of the following commands shows you the TCP and UDP network connections, listening ports, and the identifiers?

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

Answer: A

NEW QUESTION 176
The evolution of web services and their increasing use in business offers new attack vectors in an application framework. Web services are based on XML protocols such as web Services Definition Language (WSDL) for describing the connection points, Universal Description, Discovery, and Integration (UDDI) for the description and discovery of Web services and Simple Object Access Protocol (SOAP) for communication between Web services that are vulnerable to various web application threats. Which of the following layer in web services stack is vulnerable to fault code leaks?

A. Presentation Layer
B. Security Layer
C. Discovery Layer
D. Access Layer

Answer: C

NEW QUESTION 179
Which root folder (hive) of registry editor contains a vast array of configuration information for the system, including hardware settings and software settings?

A. HKEY_USERS
B. HKEY_CURRENT_USER
C. HKEY_LOCAL_MACHINE
D. HKEY-CURRENT_CONFIG

Answer: C

NEW QUESTION 182
SIM is a removable component that contains essential information about the subscriber. It has both volatile and non- volatile memory. The file system of a SIM resides in ___ memory.

A. Volatile
B. Non-volatile

Answer: B

NEW QUESTION 187
Volatile information can be easily modified or lost when the system is shut down or rebooted. It helps to determine a logical timeline of the security incident and the users who would be responsible.

A. True
B. False

Answer: A

NEW QUESTION 188

Which table is used to convert huge word lists (i .e. dictionary files and brute-force lists) into password hashes?

A. Rainbow tables
B. Hash tables
C. Master file tables
D. Database tables

Answer: A

NEW QUESTION 189
A swap file is a space on a hard disk used as the virtual memory extension of a computer's RAM. Where is the hidden swap file in Windows located?

A. C:\pagefile.sys
B. C:\hiberfil.sys
C. C:\config.sys
D. C:\ALCSetup.log

Answer: A

NEW QUESTION 192
In an echo data hiding technique, the secret message is embedded into a ____ as an echo.

A. Cover audio signal
B. Phase spectrum of a digital signal
C. Pseudo-random signal
D. Pseudo- spectrum signal

Answer: A

NEW QUESTION 196
Log management includes all the processes and techniques used to collect, aggregate, and analyze computer-generated log messages. It consists of the hardware, software, network and media used to generate, transmit, store, analyze, and dispose of log data.

A. True
B. False

Answer: A

NEW QUESTION 198
Networks are vulnerable to an attack which occurs due to overextension of bandwidth, bottlenecks, network data interception, etc.
Which of the following network attacks refers to a process in which an attacker changes his or her IP address so that he or she appears to be someone else?

A. IP address spoofing
B. Man-in-the-middle attack
C. Denial of Service attack
D. Session sniffing

Answer: A

NEW QUESTION 200
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. Errors-To header
B. Content-Transfer-Encoding header
C. Mime-Version header
D. Content-Type header

Answer: A

NEW QUESTION 202
An image is an artifact that reproduces the likeness of some subject. These are produced by optical devices (i.e. cameras, mirrors, lenses, telescopes, and microscopes).
Which property of the image shows you the number of colors available for each pixel in an image?

A. Pixel
B. Bit Depth
C. File Formats
D. Image File Size

Answer: B

NEW QUESTION 206
The IIS log file format is a fixed (cannot be customized) ASCII text-based format. The IIS format includes basic items, such as client IP address, user name, date and time, service and instance, server name and IP address, request type, target of operation, etc. Identify the service status code from the following IIS log.

192.168.100.150, -, 03/6/11, 8:45:30, W3SVC2, SERVER, 172.15.10.30, 4210, 125, 3524, 100, 0, GET, /dollerlogo.gif,

A. W3SVC2
B. 4210
C. 3524
D. 100

Answer: D

NEW QUESTION 211
Which of the following Steganography techniques allows you to encode information that ensures creation of cover for secret communication?

A. Substitution techniques
B. Transform domain techniques
C. Cover generation techniques
D. Spread spectrum techniques

Answer: C

NEW QUESTION 215
Data files from original evidence should be used for forensics analysis

A. True
B. False

Answer: B

NEW QUESTION 220
Dumpster Diving refers to:

A. Searching for sensitive information in the user's trash bins and printer trash bins, and searching the user's desk for sticky notes
B. Looking at either the user's keyboard or screen while he/she is logging in
C. Convincing people to reveal the confidential information
D. Creating a set of dictionary words and names, and trying all the possible combinations to crack the password

Answer: A

NEW QUESTION 221
BMP (Bitmap) is a standard file format for computers running the Windows operating system. BMP images can range from black and white (1 bit per pixel) up to 24 bit color (16.7 million colors). Each bitmap file contains header, the RGBQUAD array, information header, and image data. Which of the following element specifies the dimensions, compression type, and color format for the bitmap?

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

Answer: B

NEW QUESTION 224
Which of the following statement is not correct when dealing with a powered-on computer at the crime scene?

A. If a computer is switched on and the screen is viewable, record the programs running on screen and photograph the screen
B. If a computer is on and the monitor shows some picture or screen saver, move the mouse slowly without depressing any mouse button and take a photograph of the screen and record the information displayed
C. If a monitor is powered on and the display is blank, move the mouse slowly without depressing any mouse button and take a photograph
D. If the computer is switched of
E. power on the computer to take screenshot of the desktop

Answer: D

NEW QUESTION 225
According to US federal rules, to present a testimony in a court of law, an expert witness needs to furnish certain information to prove his eligibility. Jason, a qualified computer forensic expert who has started practicing two years back, was denied an expert testimony in a computer crime case by the US Court of Appeals for the Fourth Circuit in Richmond, Virginia. Considering the US federal rules, what could be the most appropriate reason for the court to reject Jason's eligibility as an expert witness?

A. Jason was unable to furnish documents showing four years of previous experience in the field
B. Being a computer forensic expert, Jason is not eligible to present testimony in a computer crime case
C. Jason was unable to furnish documents to prove that he is a computer forensic expert
D. Jason was not aware of legal issues involved with computer crimes

Answer: A

NEW QUESTION 229

A mobile operating system manages communication between the mobile device and other compatible devices like computers, televisions, or printers.

Which mobile operating system architecture is represented here?

A. webOS System Architecture
B. Symbian OS Architecture
C. Android OS Architecture
D. Windows Phone 7 Architecture

Answer: C

NEW QUESTION 234
Preparing an image drive to copy files to is the first step in Linux forensics. For this purpose, what would the following command accomplish? dcfldd if=/dev/zero of=/dev/hda bs=4096 conv=noerror, sync

A. Fill the disk with zeros
B. Low-level format
C. Fill the disk with 4096 zeros
D. Copy files from the master disk to the slave disk on the secondary IDE controller

Answer: A

NEW QUESTION 237
Paraben Lockdown device uses which operating system to write hard drive data?Paraben? Lockdown device uses which operating system to write hard drive data?

A. Mac OS
B. Red Hat
C. Unix
D. Windows

Answer: D

NEW QUESTION 241
What type of file is represented by a colon (:) with a name following it in the Master File Table (MFT) of an NTFS disk?

A. Compressed file
B. Data stream file
C. Encrypted file
D. Reserved file

Answer: B

NEW QUESTION 244
What is one method of bypassing a system BIOS password?

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

Answer: B

NEW QUESTION 248
When investigating a network that uses DHCP to assign IP addresses, where would you look to determine which system (MAC address) had a specific IP address at a specific time?

A. On the individual computer ARP cacheOn the individual computer? ARP cache
B. In the Web Server log files
C. In the DHCP Server log files
D. There is no way to determine the specific IP address

Answer: C

NEW QUESTION 252
What hashing method is used to password protect Blackberry devices?

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

Answer: D

NEW QUESTION 253
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 258
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 the 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 cannot conduct any type of investigations on anyone and therefore cannot assist you
D. ISPs never maintain log files so they would be of no use to your investigation

Answer: B

NEW QUESTION 259
What does the acronym POST mean as it relates to a PC?

A. Power On Self Test
B. Pre Operational Situation Test
C. Primary Operating System Test
D. Primary Operations Short Test

Answer: A

NEW QUESTION 261
You are working in the Security Department of a 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 a 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?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 264
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 system configurationNever run a scan on your forensics workstation because it could change your system? 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 268
When performing a forensics analysis, what device is used to prevent the system from recording data on an evidence disk?

A. Write-blocker
B. Protocol analyzer
C. Firewall
D. Disk editor

Answer: A

NEW QUESTION 271
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 272
Where is the default location for Apache access logs on a Linux computer?

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

Answer: A

NEW QUESTION 277
How often must a company keep log files for them to be admissible in a court of law?

A. All log files are admissible in court no matter their frequency
B. Weekly
C. Monthly
D. Continuously

Answer: D

NEW QUESTION 280
When needing to search for a website that is no longer present on the Internet today but was online few years back, what site can be used to view the website collection of pages?view the website? collection of pages?

A. Proxify.net
B. Dnsstuff.com
C. Samspade.org
D. Archive.org

Answer: D

NEW QUESTION 285
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 289
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 293
What is the smallest physical storage unit on a hard drive?

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

Answer: C

NEW QUESTION 298
What technique used by Encase makes it virtually impossible to tamper with evidence once it has been acquired?

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

Answer: B

NEW QUESTION 301
You are called in to assist the police in an investigation involving a suspected drug dealer. The police searched the suspect house after aYou are called in to assist the police in an investigation involving a suspected drug dealer. The police searched the suspect? house after a warrant was obtained and they located a floppy disk in the suspect bedroom. The disk contains several files, but they appear to be passwordwarrant was obtained and they located a floppy disk in the suspect? bedroom. The disk contains several files, but they appear to be password protected. What are two common
methods used by password cracking software that you could use to obtain the password?

A. Limited force and library attack
B. Brute force and dictionary attack
C. Maximum force and thesaurus attack
D. Minimum force and appendix attack

Answer: B

NEW QUESTION 306
What happens when a file is deleted by a Microsoft operating system using the FAT file system?

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

Answer: D

NEW QUESTION 309
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 310
Davidson Trucking is a small transportation company that has three local offices in Detroit Michigan. Ten female employees that work for the company have gone to an attorney reporting that male employees repeatedly harassed them and that management did nothing to stop the problem. Davidson has employee policies that outline all company guidelines, including awareness on harassment and how it will not be tolerated. When the case is brought to court, whom should the prosecuting attorney call upon for not upholding company policy?

A. IT personnel
B. Employees themselves
C. Supervisors
D. Administrative assistant in charge of writing policies

Answer: C

NEW QUESTION 311
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?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 evidenceWhen 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 313
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 314
What must an investigator do before disconnecting an iPod from any type of computer?

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

Answer: A

NEW QUESTION 318
Which is a standard procedure to perform during all computer forensics investigations?

A. With the hard drive in the suspect PC, check the date and time in the system CMOSWith the hard drive in the suspect PC, check the date and time in the system? CMOS
B. With the hard drive removed from the suspect PC, check the date and time in the system CMOSWith the hard drive removed from the suspect PC, check the date and time in the system? CMOS
C. With the hard drive in the suspect PC, check the date and time in the File Allocation Table
D. With the hard drive removed from the suspect PC, check the date and time in the system RAMWith the hard drive removed from the suspect PC, check the date and time in the system? RAM

Answer: B

NEW QUESTION 320
The following is a log file screenshot from a default installation of IIS 6.0.

```
#Software: Microsoft Internet Information Services 6.0
#Version: 1.0
#Date: 2007-01-22 15:42:36
#Fields: date time s-sitename s-ip cs-method cs-uri-stem cs-uri-query s-port cs-user
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /index.html - 80 - 172.16.28.80
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /Development/index.asp - 80 - 172.16.28
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /Development/css/olcStyle.css - 80 - 17
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /favicon.ico - 80 - 172.16.28.80 Avant+
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /Development/css/dhtml_horiz.css - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /Development/images/index_01.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /Development/images/index_02.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /Development/images/index_03.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /Development/images/index_04.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /Development/images/index_06.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /Development/images/index_07.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /Development/images/index_08.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /Development/script/dhtml.js - 80 - 172
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /Development/images/greenArraw.jpg - 80
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /Development/images/board_01.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /Development/images/board_02.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
```

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

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

Answer: A

NEW QUESTION 323
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?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

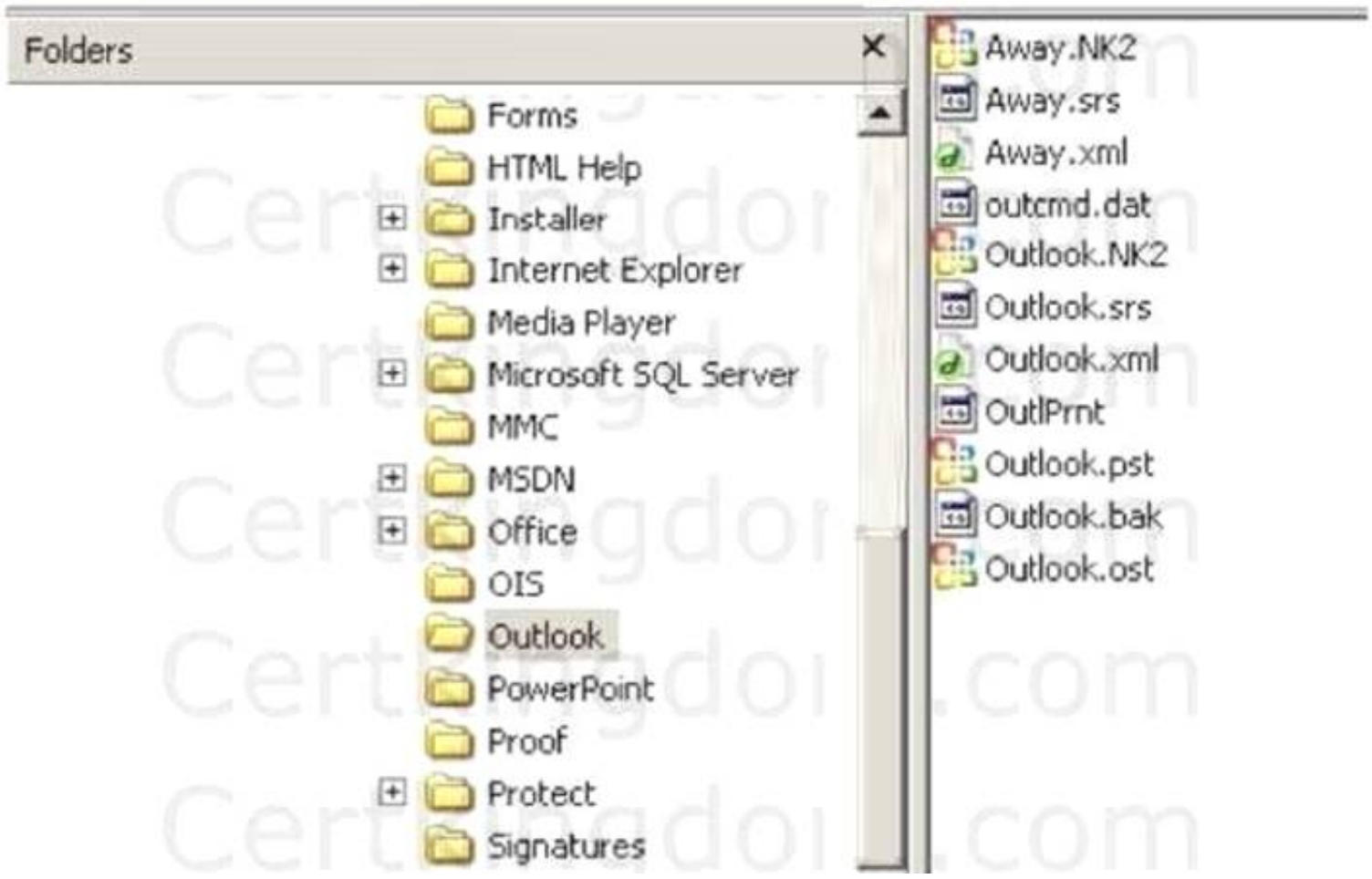
Answer: D

NEW QUESTION 328
Given the drive dimensions as follows and assuming a sector has 512 bytes, what is the capacity of the described hard drive?
22,164 cylinders/disk
80 heads/cylinder
63 sectors/track

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

Answer: A

NEW QUESTION 333
In the following directory listing,



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

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

Answer: D

NEW QUESTION 337
What feature of Decryption Collection allows an investigator to crack a password as quickly as possible?

A. Cracks every password in 10 minutes
B. Distribute processing over 16 or fewer computers
C. Support for Encrypted File System
D. Support for MD5 hash verification

Answer: B

NEW QUESTION 342
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 343
At what layer does a cross site scripting attack occur on?

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

Answer: B

NEW QUESTION 344
An investigator is searching through the firewall logs of a company and notices ICMP packets that are larger than 65,536 bytes. What type of activity is the investigator seeing?

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

Answer: B

NEW QUESTION 348
What advantage does the tool Evidor have over the built-in Windows search?

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

Answer: C

NEW QUESTION 350
George was recently fired from his job as an IT analyst at Pitts and Company in Dallas Texas. His main duties as an analyst were to support the company Active Directory structure and to create network polices. George now wants to break into the company network by cracking some ofcompany? Active Directory structure and to create network polices. George now wants to break into the company? network by cracking some of the service accounts he knows about. Which password cracking technique should George use in this situation?

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

Answer: C

NEW QUESTION 354
An employee is attempting to wipe out data stored on a couple of compact discs (CDs) and digital video discs (DVDs) by using a large magnet. You inform him that this method will not be effective in wiping out the data because CDs and DVDs are ____ media used to store large amounts of data and are not affected by the magnet.

A. Magnetic
B. Optical
C. Anti-Magnetic
D. Logical

Answer: B

NEW QUESTION 356
You are using DriveSpy, a forensic tool and want to copy 150 sectors where the starting sector is 1709 on the primary hard drive. Which of the following formats correctly specifies these sectors?

A. 0:1000, 150
B. 0:1709, 150
C. 1:1709, 150
D. 0:1709-1858

Answer: B

Explanation: DriveSpy can except two different formats: Drive #:Start Sector, # Sectors Drive#:Start Sector-Absolute End Sector. Drive # is zero based
Both Answer B and D would appear correct, and both formats are valid.

NEW QUESTION 358
Cylie is investigating a network breach at a state organization in Florida. She discovers that the intruders were able to gain access into the company firewalls by overloading them with IP packets. Cylie then discovers through her investigation that the intruders hacked into thecompany? firewalls by overloading them with IP packets. Cylie then discovers through her investigation that the intruders hacked into the company phone system and used the hard drives on their PBX system to store shared music files. What would this attack on the companycompany? phone system and used the hard drives on their PBX system to store shared music files. What would this attack on the company? PBX system be called?

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

Answer: A

NEW QUESTION 360
You are trying to locate Microsoft Outlook Web Access Default Portal using Google search on the Internet. What search string will you use to locate them?

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

Answer: A

NEW QUESTION 365
To make sure the evidence you recover and analyze with computer forensics software can be admitted in court, you must test and validate the software. What group is actively providing tools and creating procedures for testing and validating computer forensics software ?

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

Answer: C

NEW QUESTION 370
You are employed directly by an attorney to help investigate an alleged sexual harassment case at a large pharmaceutical manufacturer. While at the corporate office of the company, the CEO demands to know the status of the investigation. What prevents you from discussing the case with the CEO?

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

Answer: A

NEW QUESTION 373
As a CHFI professional, which of the following is the most important to your professional reputation?

Answer:

NEW QUESTION 376
Kyle is performing the final testing of an application he developed for the accounting department. His last round of testing is to ensure that the program is as secure as possible. Kyle runs the following command. What is he testing at this point?
#include #include int main(int argc, char *argv[]) { char buffer[10]; if (argc < 2) { fprintf (stderr, "USAGE: %sstring\n", argv[0]); return 1; } strcpy(buffer, argv[1]); return 0; }

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

Answer: C

NEW QUESTION 381
Where are files temporarily written in Unix when printing?

A. /usr/spool
B. /var/print
C. /spool
D. /var/spool

Answer: D

NEW QUESTION 386
Harold wants to set up a firewall on his network but is not sure which one would be the most appropriate. He knows he needs to allow FTP traffic to one of the servers on his network, but he wants to only allow FTP-PUT. Which firewall would be most appropriate for Harold? needs?

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

Answer: C

NEW QUESTION 391
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: AC

NEW QUESTION 393
A(n) ____ is one that's performed by a computer program rather than the attacker manually performing the steps in the attack sequence.

A. blackout attack
B. automated attack
C. distributed attack
D. central processing attack

Answer: B

NEW QUESTION 394
Steven has been given the task of designing a computer forensics lab for the company he works for. He has found documentation on all aspects of how to design a lab except the number of exits needed. How many exits should Steven include in his design for the computer forensics lab?

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

Answer: B

NEW QUESTION 398
What will the following URL produce in an unpatched IIS Web Server? http://www.thetargetsite.com/scripts/..%co%af../..%co%af../windows/system32/cmd.exe?/c+dir+c:\

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

Answer: A

NEW QUESTION 401
Why is it still possible to recover files that have been emptied from the Recycle Bin on a Windows computer?

A. The data is still present until the original location of the file is used
B. The data is moved to the Restore directory and is kept there indefinitely
C. The data will reside in the L2 cache on a Windows computer until it is manually deleted
D. It is not possible to recover data that has been emptied from the Recycle Bin

Answer: A

NEW QUESTION 403
Which of the following refers to the data that might still exist in a cluster even though the original file has been overwritten by another file?

A. Sector
B. Metadata
C. MFT
D. Slack Space

Answer: D

NEW QUESTION 407
What binary coding is used most often for e-mail purposes?

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

Answer: D

NEW QUESTION 408
While working for a prosecutor, What do you think you should do if the evidence you found appears to be exculpatory and is not being released to the defense ?

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

Answer: C

NEW QUESTION 410
When conducting computer forensic analysis, you must guard against
___ So that you remain focused on the primary job and insure that the level of work does not increase beyond what was originally expected.

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

Answer: B

NEW QUESTION 413
The newer Macintosh Operating System (MacOS X) is based on:

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

Answer: C

NEW QUESTION 415
A forensics investigator needs to copy data from a computer to some type of removable media so he can examine the information at another location. The problem is that the data is around 42GB in size. What type of removable media could the investigator use?

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

Answer: C

NEW QUESTION 420
In Linux, what is the smallest possible shellcode?

A. 8 bytes
B. 24 bytes
C. 800 bytes
D. 80 bytes

Answer: B

NEW QUESTION 422
On Linux/Unix based Web servers, what privilege should the daemon service be run under?

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

Answer: A

NEW QUESTION 426
When operating systems mark a cluster as used but not allocated, the cluster is considered as ____

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

Answer: C

NEW QUESTION 430
When examining a hard disk without a write-blocker, you should not start windows because Windows will write data to the:

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

Answer: A

NEW QUESTION 433
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. src port 22 and dst port 22
C. udp port 22 and host 172.16.28.1/24
D. net port 22

Answer: B

NEW QUESTION 438
You are assisting in the investigation of a possible Web Server hack. The company who called you stated that customers reported to them that whenever they entered the web address of the company in their browser, what they received was a pornographic web site. The company checked the web server and nothing appears wrong. When you type in the IP address of the web site in your browser everything appears normal. What is the name of the attack that affects the DNS cache of the name resolution servers, resulting in those servers directing users to the wrong web site?

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

Answer: B

NEW QUESTION 440
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. Snort
B. Airsnort
C. Ettercap
D. RaidSniff

Answer: C

NEW QUESTION 444
If an attacker's computer sends an IPID of 31400 to a zombie computer on an open port in IDLE scanning, what will be the response?

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

Answer: C

NEW QUESTION 449
Volatile Memory is one of the leading problems for forensics. Worms such as code Red are memory resident and do not 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: AC

NEW QUESTION 452
Which forensic investigating concept trails the whole incident from how the attack began to how the victim was affected?

A. Point-to-point
B. End-to-end
C. Thorough
D. Complete event analysis

Answer: B

NEW QUESTION 456
You are assigned to work in the computer forensics lab of a state police agency. While working on a high profile criminal case, you have followed every applicable procedure, however your boss is still concerned that the defense attorney might question whether evidence has been changed while at the lab. What can you do to prove that the evidence is the same as it was when it first entered the lab?

A. make an MD5 hash of the evidence and compare it with the original MD5 hash that was taken when the evidence first entered the lab
B. make an MD5 hash of the evidence and compare it to the standard database developed by NIST
C. there is no reason to worry about this possible claim because state labs are certified
D. sign a statement attesting that the evidence is the same as it was when it entered the lab

Answer: A

NEW QUESTION 461
You just passed your ECSA exam and are about to start your first consulting job running security audits for a financial institution in Los Angeles. The IT manager of the company you will be working for tries to see if you remember your ECSA class. He asks about the methodology you will be using to test the company's network. How would you answer?

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

Answer: D

NEW QUESTION 466
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 471
What method of computer forensics will allow you to trace all ever-established user accounts on a Windows 2000 server the course of its lifetime?

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

Answer: D

Explanation: Not MD5: MD5 checksums are used as integrity checks
User accounts are assigned a unique SID, and the SID are not reused.

NEW QUESTION 474
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 computerThe 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 475
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?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 479
When a file is deleted by Windows Explorer or through the MS-DOS delete command, the operating system inserts ____ in the first letter position of the filename in the FAT database.

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

Answer: D

Explanation: When a file is deleted, the first byte is replaced with 0xE5 to marked the file as deleted or erased, and is the same for FAT12/16/32. An 0xE5 translates also to a ASCII 229, a “O” with a tilde.
However, using the greek alphabet (see: http://www.ascii.ca/iso8859.7.htm) the ASCII code 229 is “the lowercase Greek Letter Epsilon, and Ascii code 243 is Lower case Greek Letter Sigma.
http://chexed.com/ComputerTips/asciicodes.php says that Ascii 229 is Lowercase Greek Letter Sigma
So, although D looks like the correct answer here, it may require more understanding of the underlying intent of the question.

NEW QUESTION 480
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: A

NEW QUESTION 482
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. Enumerate domain user accounts and built-in groups
B. Enumerate MX and A records from DNS
C. Establish a remote connection to the Domain Controller
D. Poison the DNS records with false records

Answer: A

NEW QUESTION 486
What will the following Linux command accomplish? dd if=/dev/mem of=/home/sam/mem.bin bs=1024

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

Answer: C

NEW QUESTION 488
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 SQL injection
B. Your website is vulnerable to CSS
C. Your website is vulnerable to web bugs
D. Your website is not vulnerable

Answer: B

NEW QUESTION 492
In the following email header, where did the email first originate from?

```
Microsoft Mail Internet Headers Version 2.0
Received: from smtp1.somedomain.com ([199.190.129.133]) by somedomain.com
with Microsoft SMTPSVC(6.0.3790.1830);
         Fri, 1 Jun 2007 09:43:08 -0500
Received: from david1.state.us.gov.us (david1.state.ok.gov [172.16.28.115])
        by smtp1.somedomain.com (8.13.1/8.12.11) with ESMTP id l51EfCEh032241
        for <someone@somedomain.com>; Fri, 1 Jun 2007 09:41:13 -0500
Received: from simon1.state.ok.gov.us ([172.18.0.199]) by
david1.state.ok.gov.us with Microsoft SMTPSVC(6.0.3790.1830);
         Fri, 1 Jun 2007 09:41:13 -0500
X-Ninja-PIM: Scanned by Ninja
X-Ninja-AttachmentFiltering: (no action)
X-MimeOLE: Produced By Microsoft Exchange V6.5.7235.2
Content-class: urn:content-classes:message
Return-Receipt-To: "Johnson, Jimmy" <jimmy@somewherelese.com>
MIME-Version: 1.0
```

A. Somedomain.com
B. Smtp1.somedomain.com
C. Simon1.state.ok.gov.us
D. David1.state.ok.gov.us

Answer: C

NEW QUESTION 495
What type of attack occurs when an attacker can force a router to stop forwarding packets by flooding the router with many open connections simultaneously so that all the hosts behind the router are effectively disabled?

A. ARP redirect
B. Physical attack
C. Digital attack
D. Denial of service

Answer: D

NEW QUESTION 497
The following excerpt is taken from a honeypot log. The log captures activities across three days. There are several intrusion attempts; however, a few are successful.
(Note: The objective of this question is to test whether the student can read basic information from log entries and interpret the nature of attack.)
Apr 24 14:46:46 [4663]: spp_portscan: portscan detected from 194.222.156.169
Apr 24 14:46:46 [4663]: IDS27/FIN Scan: 194.222.156.169:56693 -> 172.16.1.107:482 Apr 24 18:01:05 [4663]:
IDS/DNS-version-query: 212.244.97.121:3485 -> 172.16.1.107:53
Apr 24 19:04:01 [4663]: IDS213/ftp-passwd-retrieval: 194.222.156.169:1425 -> 172.16.1.107:21
Apr 25 08:02:41 [5875]: spp_portscan: PORTSCAN DETECTED from 24.9.255.53
Apr 25 02:08:07 [5875]: IDS277/DNS-version-query: 63.226.81.13:4499 -> 172.16.1.107:53
Apr 25 02:08:07 [5875]: IDS277/DNS-version-query: 63.226.81.13:4630 -> 172.16.1.101:53
Apr 25 02:38:17 [5875]: IDS/RPC-rpcinfo-query: 212.251.1.94:642 -> 172.16.1.107:111
Apr 25 19:37:32 [5875]: IDS230/web-cgi-space-wildcard: 198.173.35.164:4221 -> 172.16.1.107:80
Apr 26 05:45:12 [6283]: IDS212/dns-zone-transfer: 38.31.107.87:2291 -> 172.16.1.101:53 Apr 26 06:43:05 [6283]:
IDS181/nops-x86: 63.226.81.13:1351 -> 172.16.1.107:53
Apr 26 06:44:25 victim7 PAM_pwdb[12509]: (login) session opened for user simple by (uid=0)
Apr 26 06:44:36 victim7 PAM_pwdb[12521]: (su) session opened for user simon by simple(uid=506) Apr 26 06:45:34 [6283]: IDS175/socks-probe:
24.112.167.35:20 -> 172.16.1.107:1080
Apr 26 06:52:10 [6283]: IDS127/telnet-login-incorrect: 172.16.1.107:23 -> 213.28.22.189:4558
From the options given below choose the one which best interprets the following entry: Apr 26 06:43:05 [6283]: IDS181/nops-x86: 63.226.81.13:1351 -> 172.16.1.107:53

A. An IDS evasion technique
B. A buffer overflow attempt
C. A DNS zone transfer
D. Data being retrieved from 63.226.81.13

Answer: A

NEW QUESTION 500
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 503
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. Make a bit-stream disk-to-disk file
B. Make a bit-stream disk-to-image file
C. Create a sparse data copy of a folder or file
D. Create a compressed copy of the file with DoubleSpace

Answer: C

NEW QUESTION 508
What type of analysis helps to identify the time and sequence of events in an investigation?

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

Answer: D

NEW QUESTION 511
What operating system would respond to the following command? C:\> nmap -sW 10.10.145.65

A. Windows XP
B. Mac OS X
C. FreeBSD
D. Windows 95

Answer: C

NEW QUESTION 514
One way to identify the presence of hidden partitions on a suspect hard drive is to:One way to identify the presence of hidden partitions on a suspect? hard drive is to:

A. Add up the total size of all known partitions and compare it to the total size of the hard drive
B. Examine the FAT and identify hidden partitions by noting an ?in the artition Type?fieldExamine the FAT and identify hidden partitions by noting an ??in the ?artition Type?field
C. Examine the LILO and note an ?in the artition Type?fieldExamine the LILO and note an ??in the ?artition Type?field It is not possible to have hidden partitions on a hard drive

Answer: A

NEW QUESTION 519
Harold is a security analyst who has just run the rdisk /s command to grab the backup SAM file on a computer. Where should Harold navigate on the computer to find the file?

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

Answer: C

NEW QUESTION 520
In General, ____ Involves the investigation of data that can be retrieved from the hard disk or other disks of a computer by applying scientific methods to retrieve the data.

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

Answer: D

NEW QUESTION 522
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 527
Sectors in hard disks typically contain how many bytes?

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

Answer: B

NEW QUESTION 531
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 533
The use of warning banners helps a company avoid litigation by overcoming an employees assumed when connecting to the company intranet, network, or virtual private network (VPN) and will allow the company investigators to monitor, search, and retrievecompany? intranet, network, or virtual private network (VPN) and will allow the company? 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 538
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

Explanation: Answer “Silver-Platter Doctrine” is probably the most correct. However, the Silver-Platter Doctrine allowed the Federal court to introduce illegally or improperly “State” seized evidence as long as Federal officers had no role in obtaining it. Also wanted to note that this Doctrine was declared unconstitional in 1960, Elkins vs United States

NEW QUESTION 541
How many possible sequence number combinations are there in TCP/IP protocol?

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

Answer: C

NEW QUESTION 542
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 546
When investigating a computer forensics case where Microsoft Exchange and Blackberry Enterprise server are used, where would investigator need to search to find email sent from a Blackberry device?

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

Answer: C

NEW QUESTION 550
After undergoing an external IT audit, George realizes his network is vulnerable to DDoS attacks. What countermeasures could he take to prevent DDoS attacks?

A. Enable BGP
B. Enable direct broadcasts

C. Disable BGP
D. Disable direct broadcasts

Answer: D

NEW QUESTION 552
After attending a CEH security seminar, you make a list of changes you would like to perform on your network to increase its security. One of the first things you change is to switch the RestrictAnonymous setting from 0 to 1 on your servers. This, as you were told, would prevent anonymous users from establishing a null session on the server. Using Userinfo tool mentioned at the seminar, you succeed in establishing a null session with one of the servers. Why is that?

A. RestrictAnonymous must be set to "2" for complete security
B. There is no way to always prevent an anonymous null session from establishing
C. RestrictAnonymous must be set to "10" for complete security
D. RestrictAnonymous must be set to "3" for complete security

Answer: A

NEW QUESTION 553
Software firewalls work at which layer of the OSI model?

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

Answer: C

NEW QUESTION 554
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 search engines that link to .net domains
B. All sites that link to ghttech.net
C. Sites that contain the code: link:www.ghttech.net
D. All sites that ghttech.net links to

Answer: B

NEW QUESTION 557
What information do you need to recover when searching a victim computer for a crime committed with specific e-mail message?What information do you need to recover when searching a victim? computer for a crime committed with specific e-mail message?

A. Internet service provider information
B. E-mail header
C. Username and password
D. Firewall log

Answer: B

NEW QUESTION 558
Click on the Exhibit Button Paulette works for an IT security consulting company that is currently performing an audit for the firm ACE Unlimited. Paulette's duties include logging on to all the company's network equipment to ensure IOS versions are up-to-date and all the other security settings are as stringent as possible. Paulette presents the following screenshot to her boss so he can inform the client about necessary changes need to be made. From the screenshot, what changes should the client company make?

A. The banner should include the Cisco tech support contact information as well
B. The banner should have more detail on the version numbers for the networkeQuipment
C. The banner should not state "only authorized IT personnel may proceed"
D. Remove any identifying numbers, names, or version information

Answer: D

NEW QUESTION 561
In a FAT32 system, a 123 KB file will use how many sectors?

A. 34
B. 25
C. 11
D. 56
E. 246

Answer: E

Explanation: If you assume that we are using 512 bytes sectors, then 123x1024/512 = 246 sectors would be needed.

NEW QUESTION 562
What does the superblock in Linux define?

A. file synames
B. disk geometr
C. location of the first inode
D. available space

Answer: C

NEW QUESTION 565
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. BPG
B. ATM
C. OSPF
D. UDP

Answer: C

NEW QUESTION 570
An "idle" system is also referred to as what?

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

Answer: C

NEW QUESTION 571
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 has been compromised using a t0rnrootkit
B. The system administrator has created an incremental backup
C. The system files have been copied by a remote attacker
D. Nothing in particular as these can be operational files

Answer: D

NEW QUESTION 572
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 577
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 581
What does ICMP Type 3/Code 13 mean?

A. Administratively Blocked
B. Host Unreachable

C. Protocol Unreachable
D. Port Unreachable

Answer: A

NEW QUESTION 586
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 587
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. Fuzzing
B. Tailgating
C. Backtrapping
D. Man trap attack

Answer: C

NEW QUESTION 588
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. Simple Network Management Protocol
B. Cisco Discovery Protocol
C. Border Gateway Protocol
D. Broadcast System Protocol

Answer: B

NEW QUESTION 591
What file structure database would you expect to find on floppy disks?

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

Answer: D

Explanation: NTFS is not designed for removable media, although used on some removable media that is very large, never for floppy disks.
FAT32 has a minimum space requirement which is larger than floppy disks FAT16 would seem like a logical choice, but is not usually used on floppies FAT12 would be on floppy disks, and probably not seen on anything else. Since floppy disk media is small in size (less than 2 MB), a FAT12 file system has lower overhead and is more efficient.

NEW QUESTION 595
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: AC

Explanation: To be effective with throwing the hard drive into the fire, the fire would have to be hot enough to melt the platters into molten metal, which requires an industrial furnance. This requires special facilities.
Running powerful magnets over the disk, such as degaussing the disk, may destroy the data, but may also be ineffective. In some cases, the degaussing process for tape and disk may render the disk unusable for use again. (of course throwing the drives into a furnance also guarantee that as well).
Formatting the disk multiple times with a low level disk utility is the best way to go, and still beable to re-use the disk for later projects. The keys are “multiple” and “low level”. A low level format is typicall a slow, thorough, format that is a wipe. Multiple – as opposed to once – is recommended. There is a theory on “how many times”, some schools say at least three times. The problem with this answer is that with newer drives, such as ATA and SCSI, low level formats can destroy the volumes as well, and some BIOS may actually ignore the LLF directives.
Overwritting the disk with junk data would perform some form of wipe because the old data is wiped out, but still may be recoverd.
Note:
According to some websites:
Physical Methods that will not work to destroy data on a hard drive include:Throwing it in the water (this does not do much)Setting it on fire (the temperature is not going to be high enough at home)Throwing it out of the window. Hard drives can take quite a bit of G force. They are not heavy so the impact of the hard drive on the ground is not likely to destroy the platters.Drive over the hard drive. A car, or even a tank, driving over a hard drive will do nothing, any more than they would driving over a book. Unless the drive is actually flattened, the platters are not going to be destroyed

NEW QUESTION 598
Before performing a logical or physical search of a drive in Encase, what must be added to the program?

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

Answer: B

NEW QUESTION 603
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 employees’ 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 606
While looking through the IIS log file of a web server, you find the following entries:

```
2007-01-23 14:18:39 W3SVC1 172.16.28.102 GET /Development/index.asp
2007-01-23 14:18:39 W3SVC1 172.16.28.102 GET /login.asp?username=if ((select user)='sa' OR (select user)='dbo')
select 1 else select 1/0
2007-01-23 14:18:39 W3SVC1 172.16.28.102 GET /Developments/index_02.jpg
2007-01-23 14:18:39 W3SVC1 172.16.28.102 GET /Development/index 04.jpg
```

What is evident from this log file?

A. Web bugs
B. Cross site scripting
C. Hidden fields
D. SQL injection is possible

Answer: D

NEW QUESTION 610
When investigating a Windows System, it is important to view the contents of the page or swap file because:

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

Answer: C

NEW QUESTION 612
What are the security risks of running a "repair" installation for Windows XP?

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

Answer: D

NEW QUESTION 616
You are running through a series of tests on your network to check for any security vulnerabilities. After normal working hours, you initiate a DoS attack against

your external firewall. The firewall Quickly freezes up and becomes unusable. You then initiate an FTP connection from an external IP into your internal network. The connection is successful even though you have FTP blocked at the external firewall. What has happened?

A. The firewall failed-open
B. The firewall failed-closed
C. The firewall ACL has been purged
D. The firewall failed-bypass

Answer: A

NEW QUESTION 618
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 621
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 626
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. ICMP ping sweep
B. Ping trace
C. Tracert
D. Smurf scan

Answer: A

NEW QUESTION 628
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 632
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 637
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 640
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 employee computer that was protected with the NTFS Encrypted File System (EFS) and you had observed him copy the files to astored on the employee? 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 disk and secure his computer. Will you be able to break the encryption so that you can verify that the employee was in possession of the proprietary information?

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

Answer: C

NEW QUESTION 643
Jones had been trying to penetrate a remote production system for the past two weeks. This time however, he is able to get into the system. He was able to use the system for a period of three weeks. However law enforcement agencies were recording his every activity and this was later presented as evidence. The organization had used a virtual environment to trap Jones. What is a virtual environment?

A. A system using Trojaned commands
B. A honeypot that traps hackers
C. An environment set up after the user logs in
D. An environment set up before an user logs in

Answer: B

NEW QUESTION 644
What TCP/UDP port does the toolkit program netstat use?

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

Answer: B

NEW QUESTION 646
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 sets all packets with a TTL of one
B. Firewalk sets all packets with a TTL of zero
C. Firewalk cannot pass through Cisco firewalls
D. Firewalk cannot be detected by network sniffers

Answer: A

NEW QUESTION 650
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 651
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, o comment?Say, ?o comment
C. Answer all the reporter questions as completely as possibleAnswer all the reporter? questions as completely as possible
D. Answer only the questions that help your case

Answer: B

NEW QUESTION 652
What is the name of the standard Linux command that can be used to create bit-stream images?

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

Answer: D

NEW QUESTION 656
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. True negatives
C. True positives
D. False positives

Answer: A

NEW QUESTION 661
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: A

Explanation: The Ping of Death occurs when the ICMP Header field contains a packet size lager than 65507 bytes.

NEW QUESTION 665
If a suspect computer is located in an area that may have toxic chemicals, you must:

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

Answer: A

NEW QUESTION 668
Jason is the security administrator of ACMA metal Corporation. One day he notices the company's Oracle database server has been compromised and the customer information along with financial data has been stolen. The financial loss will be in millions of dollars if the database gets into the hands of the competitors. Jason wants to report this crime to the law enforcement agencies immediately. Which organization coordinates computer crimes investigations throughout the United States?

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

Answer: B

NEW QUESTION 669
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
E. boot.ini

Answer: E

Explanation: The OS isn’t specified, but if this was a Windows OS, then this would be boot.ini
The answer is CMOS. The startup of a computer is the boot sequence, and the boot sequence is defined in the CMOS. The common occurrence is to boot off a floppy, and you need to see that the floppy (usually the A drive) is first in the sequence. If you don’t, and the hard drive is first, then booting the system wil boot the hard drive and alter the evidence.

NEW QUESTION 670
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 673
A honey pot deployed with the IP 172.16.1.108 was compromised by an attacker . Given below is an excerpt from a Snort binary capture of the attack. Decipher the activity carried out by the attacker by studying the log. Please note that you are required to infer only what is explicit in the excerpt.
(Note: The student is being tested on concepts learnt during passive OS fingerprinting, basic TCP/IP connection concepts and the ability to read packet signatures from a sniff dump.)
03/15-20:21:24.107053 211.185.125.124:3500 -> 172.16.1.108:111 TCP TTL:43 TOS:0x0 ID:29726 IpLen:20
DgmLen:52 DF
A* Seq: 0x9B6338C5 Ack: 0x5820ADD0 Win: 0x7D78 TcpLen: 32 TCP Options (3) => NOP NOP TS: 23678634 2878772
=+
+=
03/15-20:21:24.452051 211.185.125.124:789 -> 172.16.1.103:111 UDP TTL:43 TOS:0x0 ID:29733 IpLen:20
DgmLen:84 Len: 64
01 0A 8A 0A 00 00 00 00 00 00 00 02 00 01 86 A0 ....
00 00 00 02 00 00 00 03 00 00 00 00 00 00 00 00 ....
00 00 00 00 00 00 00 00 00 01 86 B8 00 00 00 01 ....
00 00 00 11 00 00 00 00 ....
=+
+= 03/15-20:21:24.730436 211.185.125.124:790 -> 172.16.1.103:32773
UDP TTL:43 TOS:0x0 ID:29781 IpLen:20 DgmLen:1104 Len: 1084
47 F7 9F 63 00 00 00 00 00 00 00 02 00 01 86 B8 G..c...........
00 00 00 01 00 00 00 01 00 00 00 01 00 00 00 20 ....
3A B1 5E E5 00 00 00 09 6C 6F 63 61 6C 68 6F 73 :.^.....localhost
=+
+=+=+ 03/15-20:21:36.539731 211.185.125.124:4450 -> 172.16.1.108:39168
TCP TTL:43 TOS:0x0 ID:31660 IpLen:20 DgmLen:71 DF
AP Seq: 0x9C6D2BFF Ack: 0x59606333 Win: 0x7D78 TcpLen: 32 TCP Options (3) => NOP NOP TS: 23679878 2880015
63 64 20 2F 3B 20 75 6E 61 6D 65 20 2D 61 3B 20 cd /; uname -a; 69 64 3B id;

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

Answer: A

NEW QUESTION 674
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 676
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 680
Lance wants to place a honeypot on his network. Which of the following would be your recommendations?

A. Use a system that has a dynamic addressing on the network
B. Use a system that is not directly interacing with the router
C. Use it on a system in an external DMZ in front of the firewall
D. It doesn't matter as all replies are faked

Answer: D

NEW QUESTION 684
What is the following command trying to accomplish? C:\> nmap -sU -p445 192.168.0.0/24

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

Answer: B

NEW QUESTION 689
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. CB radio
B. 2.4Ghz Cordless phones
C. Satellite television
D. Computers on his wired network

Answer: B

NEW QUESTION 691
In a virtual test environment, Michael is testing the strength and security of BGP using multiple routers to mimic the backbone of the Internet. This project will help him write his doctoral thesis on "bringing down the Internet". Without sniffing the traffic between the routers, Michael sends millions of RESET packets to the routers in an attempt to shut one or all of them down. After a few hours, one of the routers finally shuts itself down. What will the other routers communicate between themselves?

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

Answer: A

NEW QUESTION 692
One technique for hiding information is to change the file extension from the correct one to one that might not be noticed by an investigator. For example, changing a
.jpg extension to a .doc extension so that a picture file appears to be a document. What can an investigator examine to verify that a file has the correct extension?

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

Answer: B

NEW QUESTION 695
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. Internal Penetration Testing
D. Firewall Penetration Testing

Answer: B

NEW QUESTION 699
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 312-49v9 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 312-49v9 Product From:

https://www.2passeasy.com/dumps/312-49v9/

Money Back Guarantee

312-49v9 Practice Exam Features:

* 312-49v9 Questions and Answers Updated Frequently

* 312-49v9 Practice Questions Verified by Expert Senior Certified Staff

* 312-49v9 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* 312-49v9 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year