

# EC-Council

## Exam Questions 312-49v10

Computer Hacking Forensic Investigator (CHFI-v10)



#### 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)

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

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

**Answer: B**

#### NEW QUESTION 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)

In Linux OS, different log files hold different information, which help the investigators to analyze various issues during a security incident. What information can the investigators obtain from the log file `var/log/dmesg`?

- A. Kernel ring buffer information
- B. All mail server message logs
- C. Global system messages
- D. Debugging log messages

**Answer: A**

#### NEW QUESTION 5

- (Exam Topic 3)

Chong-lee, a forensics executive, suspects that a malware is continuously making copies of files and folders on a victim system to consume the available disk space. What type of test would confirm his claim?

- A. File fingerprinting
- B. Identifying file obfuscation
- C. Static analysis
- D. Dynamic analysis

**Answer: A**

#### NEW QUESTION 6

- (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 7

- (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 8**

- (Exam Topic 3)

Where should the investigator look for the Edge browser's browsing records, including history, cache, and cookies?

- A. ESE Database
- B. Virtual Memory
- C. Sparse files
- D. Slack Space

**Answer: A**

**NEW QUESTION 9**

- (Exam Topic 3)

Brian needs to acquire data from RAID storage. Which of the following acquisition methods is recommended to retrieve only the data relevant to the investigation?

- A. Static Acquisition
- B. Sparse or Logical Acquisition
- C. Bit-stream disk-to-disk Acquisition
- D. Bit-by-bit Acquisition

**Answer: B**

**NEW QUESTION 10**

- (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 10**

- (Exam Topic 3)

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

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

**Answer: C**

**NEW QUESTION 13**

- (Exam Topic 3)

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

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

**Answer: D**

**NEW QUESTION 17**

- (Exam Topic 3)

Which of the following examinations refers to the process of providing the opposing side in a trial the opportunity to question a witness?

- A. Cross Examination
- B. Direct Examination
- C. Indirect Examination
- D. Witness Examination

**Answer: A**

**NEW QUESTION 18**

- (Exam Topic 3)

Gary, a computer technician, is facing allegations of abusing children online by befriending them and sending them illicit adult images from his office computer. What type of investigation does this case require?

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

**Answer: B**

#### **NEW QUESTION 20**

- (Exam Topic 3)

What do you call the process of studying the changes that have taken place across a system or a machine after a series of actions or incidents?

- A. Windows Services Monitoring
- B. System Baselineing
- C. Start-up Programs Monitoring
- D. Host integrity Monitoring

**Answer: D**

#### **NEW QUESTION 21**

- (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 22**

- (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 type
- 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 24**

- (Exam Topic 3)

Which among the following laws emphasizes the need for each Federal agency to develop, document, and implement an organization-wide program to provide information security for the information systems that support its operations and assets?

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

**Answer: A**

#### **NEW QUESTION 28**

- (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 33**

- (Exam Topic 3)

Which of these rootkit detection techniques function by comparing a snapshot of the file system, boot records, or memory with a known and trusted baseline?

- A. Signature-Based Detection
- B. Integrity-Based Detection
- C. Cross View-Based Detection
- D. Heuristic/Behavior-Based Detection

**Answer: B**

**NEW QUESTION 38**

- (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 43**

- (Exam Topic 3)

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

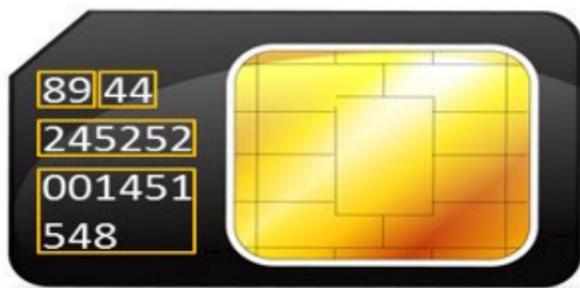
- A. tcp.port = 23
- B. tcp.port == 21
- C. tcp.port == 21 || tcp.port == 22
- D. tcp.port != 21

**Answer: B**

**NEW QUESTION 45**

- (Exam Topic 3)

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



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

**Answer: B**

**NEW QUESTION 49**

- (Exam Topic 3)

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

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

**Answer: B**

**NEW QUESTION 51**

- (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 54**

- (Exam Topic 3)

Which of the following does Microsoft Exchange E-mail Server use for collaboration of various e-mail applications?

- A. Simple Mail Transfer Protocol (SMTP)
- B. Messaging Application Programming Interface (MAPI)
- C. Internet Message Access Protocol (IMAP)
- D. Post Office Protocol version 3 (POP3)

**Answer: B**

#### NEW QUESTION 59

- (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 63

- (Exam Topic 3)

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

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

**Answer: B**

#### NEW QUESTION 67

- (Exam Topic 3)

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

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

**Answer: B**

#### NEW QUESTION 70

- (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 74

- (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 79

- (Exam Topic 3)

Select the tool appropriate for finding the dynamically linked lists of an application or malware.

- A. SysAnalyzer
- B. ResourcesExtract
- C. PEiD
- D. Dependency Walker

**Answer: D**

**NEW QUESTION 82**

- (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 86**

- (Exam Topic 3)

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

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

**Answer: B**

**NEW QUESTION 89**

- (Exam Topic 3)

As a Certified Ethical Hacker, you were contracted by a private firm to conduct an external security assessment through penetration testing . What document describes the specifics of the testing, the associated violations, and essentially protects both the organization's interest and your liabilities as a tester?

- A. Project Scope
- B. Rules of Engagement
- C. Non-Disclosure Agreement
- D. Service Level Agreement

**Answer: B**

**NEW QUESTION 90**

- (Exam Topic 3)

Which among the following U.S. laws requires financial institutions—companies that offer consumers financial products or services such as loans, financial or investment advice, or insurance—to protect their customers' information against security threats?

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

**Answer: C**

**NEW QUESTION 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 95**

- (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 100**

- (Exam Topic 3)

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

- A. TestDisk for Windows

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

**Answer:** D

**NEW QUESTION 104**

- (Exam Topic 3)

Which part of Metasploit framework helps users to hide the data related to a previously deleted file or currently unused by the allocated file.

- A. Waffin FS
- B. RuneFS
- C. FragFS
- D. Slacker

**Answer:** D

**NEW QUESTION 107**

- (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 112**

- (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 115**

- (Exam Topic 3)

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

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

**Answer:** D

**NEW QUESTION 118**

- (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 122**

- (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 125**

- (Exam Topic 3)

Which among the following tools can help a forensic investigator to access the registry files during postmortem analysis?

- A. RegistryChangesView
- B. RegDIIView
- C. RegRipper
- D. ProDiscover

**Answer: C**

#### NEW QUESTION 130

- (Exam Topic 3)

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

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

**Answer: B**

#### NEW QUESTION 133

- (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 134

- (Exam Topic 3)

During an investigation of an XSS attack, the investigator comes across the term "[a-zA-Z0-9\%]+" in analyzed evidence details. What is the expression used for?

- A. Checks for upper and lower-case alphanumeric string inside the tag, or its hex representation
- B. Checks for forward slash used in HTML closing tags, its hex or double-encoded hex equivalent
- C. Checks for opening angle bracket, its hex or double-encoded hex equivalent
- D. Checks for closing angle bracket, hex or double-encoded hex equivalent

**Answer: B**

#### NEW QUESTION 138

- (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 142

- (Exam Topic 3)

Which of the following registry hive gives the configuration information about which application was used to open various files on the system?

- A. HKEY\_CLASSES\_ROOT
- B. HKEY\_CURRENT\_CONFIG
- C. HKEY\_LOCAL\_MACHINE
- D. HKEY\_USERS

**Answer: A**

#### NEW QUESTION 147

- (Exam Topic 3)

Which of the following is NOT an anti-forensics technique?

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

**Answer: A**

#### NEW QUESTION 152

- (Exam Topic 3)

Which of the following statements is true regarding SMTP Server?

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

**Answer: C**

#### NEW QUESTION 153

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

**Answer: D**

#### NEW QUESTION 156

- (Exam Topic 3)

Report writing is a crucial stage in the outcome of an investigation. Which information should not be included in the report section?

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

**Answer: A**

#### NEW QUESTION 160

- (Exam Topic 3)

Which of the following is NOT a physical evidence?

- A. Removable media
- B. Cables
- C. Image file on a hard disk
- D. Publications

**Answer: C**

#### NEW QUESTION 161

- (Exam Topic 3)

To reach a bank web site, the traffic from workstations must pass through a firewall. You have been asked to review the firewall configuration to ensure that workstations in network 10.10.10.0/24 can only reach the bank web site 10.20.20.1 using https. Which of the following firewall rules meets this requirement?

- A. if (source matches 10.10.10.0/24 and destination matches 10.20.20.1 and port matches 443) then permit
- B. if (source matches 10.10.10.0/24 and destination matches 10.20.20.1 and port matches 80 or 443) then permit
- C. if (source matches 10.10.10.0 and destination matches 10.20.20.1 and port matches 443) then permit

**Answer: A**

#### NEW QUESTION 165

- (Exam Topic 3)

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

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

**Answer: C**

#### NEW QUESTION 169

- (Exam Topic 3)

Which of the following is a tool to reset Windows admin password?

- A. R-Studio

- B. Windows Password Recovery Bootdisk
- C. Windows Data Recovery Software
- D. TestDisk for Windows

**Answer: B**

**NEW QUESTION 173**

- (Exam Topic 3)

Sheila is a forensics trainee and is searching for hidden image files on a hard disk. She used a forensic investigation tool to view the media in hexadecimal code for simplifying the search process. Which of the following hex codes should she look for to identify image files?

- A. ff d8 ff
- B. 25 50 44 46
- C. d0 0f 11 e0
- D. 50 41 03 04

**Answer: A**

**NEW QUESTION 176**

- (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 180**

- (Exam Topic 3)

Which of the following is a part of a Solid-State Drive (SSD)?

- A. Head
- B. Cylinder
- C. NAND-based flash memory
- D. Spindle

**Answer: C**

**NEW QUESTION 185**

- (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 188**

- (Exam Topic 3)

Which of the following is a MAC-based File Recovery Tool?

- A. VirtualLab
- B. GetDataBack
- C. Cisdem DataRecovery 3
- D. Smart Undelete

**Answer: C**

**NEW QUESTION 190**

- (Exam Topic 3)

Which of the following Perl scripts will help an investigator to access the executable image of a process?

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

**Answer: D**

**NEW QUESTION 191**

- (Exam Topic 3)

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

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

**Answer: A**

**NEW QUESTION 193**

- (Exam Topic 3)

What system details can an investigator obtain from the NetBIOS name table cache?

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

**Answer: C**

**NEW QUESTION 194**

- (Exam Topic 3)

Which of the following techniques delete the files permanently?

- A. Steganography
- B. Artifact Wiping
- C. Data Hiding
- D. Trail obfuscation

**Answer: B**

**NEW QUESTION 196**

- (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 197**

- (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 202**

- (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 206**

- (Exam Topic 3)

What must an attorney do first before you are called to testify as an expert?

- A. Qualify you as an expert witness
- B. Read your curriculum vitae to the jury
- C. Engage in damage control
- D. Prove that the tools you used to conduct your examination are perfect

Answer: A

**NEW QUESTION 211**

- (Exam Topic 3)

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

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

Answer: C

**NEW QUESTION 216**

- (Exam Topic 3)

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

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

Answer: A

**NEW QUESTION 220**

- (Exam Topic 3)

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

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

Answer: A

**NEW QUESTION 224**

- (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 228**

- (Exam Topic 3)

An investigator is analyzing a checkpoint firewall log and comes across symbols. What type of log is he looking at?



- A. Security event was monitored but not stopped
- B. Malicious URL detected
- C. An email marked as potential spam
- D. Connection rejected

Answer: C

**NEW QUESTION 232**

- (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 234**

- (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 236**

- (Exam Topic 2)

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

```

2007-06-14 23:59:05 192.168.254.1 action=Permit sent=16169 rcvd=180962 src=24.119.229.125 dst=10.120.10.122 src_port=38
2007-06-14 23:59:06 192.168.254.1 action=Deny sent=0 rcvd=12288 src=10.130.9.2 dst=224.0.0.2 src_port=49415 dst_port=49
2007-06-14 23:59:07 192.168.254.1 action=Permit sent=844 rcvd=486 src=24.119.229.125 dst=10.120.10.122 src_port=38660 d
2007-06-14 23:59:07 192.168.254.1 action=Permit sent=549 rcvd=404 src=192.168.254.80 dst=208.188.166.68 src_port=13113
2007-06-14 23:59:07 192.168.254.1 action=Permit sent=549 rcvd=404 src=192.168.254.80 dst=208.188.166.68 src_port=14857
2007-06-14 23:59:07 192.168.254.1 action=Deny sent=0 rcvd=12288 src=10.130.9.3 dst=224.0.0.2 src_port=49415 dst_port=49
2007-06-14 23:59:09 192.168.254.1 action=Permit sent=13795 rcvd=149962 src=70.185.206.122 dst=10.120.10.122 src_port=61
2007-06-14 23:59:09 192.168.254.1 action=Permit sent=690 rcvd=415 src=70.185.198.247 dst=10.120.10.122 src_port=48392 d
2007-06-14 23:59:09 192.168.254.1 action=Permit sent=12219 rcvd=140495 src=70.185.206.122 dst=10.120.10.122 src_port=61
2007-06-14 23:59:09 192.168.254.1 action=Deny sent=0 rcvd=12288 src=10.130.9.2 dst=224.0.0.2 src_port=49415 dst_port=49
2007-06-14 23:59:10 192.168.254.1 action=Deny sent=0 rcvd=12288 src=10.130.9.3 dst=224.0.0.2 src_port=49415 dst_port=49
2007-06-14 18:34:04 192.168.254.1 action=Permit sent=3018 rcvd=34134 src=70.185.198.247 dst=10.120.10.122 src_port=4480
2007-06-14 18:34:05 192.168.254.1 action=Permit sent=799 rcvd=6686 src=70.185.198.247 dst=10.120.10.122 src_port=46344
2007-06-14 18:34:07 192.168.254.1 action=Permit sent=2780 rcvd=18874 src=70.185.198.247 dst=10.120.10.122 src_port=4532
2007-06-14 18:34:07 192.168.254.1 action=Permit sent=2737 rcvd=8922 src=24.119.169.162 dst=10.120.10.122 src_port=2689
2007-06-14 18:34:09 192.168.254.1 action=Permit sent=2094 rcvd=23180 src=70.185.198.247 dst=10.120.10.122 src_port=4685
2007-06-14 18:34:11 192.168.254.1 action=Permit sent=2612 rcvd=68608 src=70.185.198.247 dst=10.120.10.122 src_port=4711
2007-06-14 18:34:12 192.168.254.1 action=Permit sent=4131 rcvd=71135 src=24.119.169.162 dst=10.120.10.122 src_port=1665
2007-06-14 18:34:13 192.168.254.1 action=Permit sent=646 rcvd=1803 src=70.185.198.247 dst=10.120.10.122 src_port=47368
2007-06-14 21:47:29 192.168.254.1 action=Permit sent=729 rcvd=1115 src=70.185.198.247 dst=10.120.10.122 src_port=48136
2007-06-14 21:47:30 192.168.254.1 action=Permit sent=766 rcvd=415 src=70.185.206.122 dst=10.120.10.122 src_port=62212 d
2007-06-14 21:47:35 192.168.254.1 action=Permit sent=5054 rcvd=81725 src=24.119.169.162 dst=10.120.10.122 src_port=7809
2007-06-14 21:47:37 192.168.254.1 action=Permit sent=26196 rcvd=233409 src=24.119.229.125 dst=10.120.10.122 src_port=38
2007-06-14 21:47:40 192.168.254.1 action=Deny sent=0 rcvd=12288 src=10.130.9.2 dst=224.0.0.2 src_port=49415 dst_port=49
2007-06-14 21:47:41 192.168.254.1 action=Permit sent=18121 rcvd=210841 src=216.97.160.253 dst=10.120.10.122 src_port=94
2007-06-14 21:47:42 192.168.254.1 action=Permit sent=5741 rcvd=102596 src=24.119.169.162 dst=10.120.10.122 src_port=579
2007-06-14 21:47:42 192.168.254.1 action=Permit sent=2982 rcvd=24075 src=24.119.169.162 dst=10.120.10.122 src_port=641
2007-06-14 21:47:43 192.168.254.1 action=Permit sent=2597 rcvd=28655 src=24.119.169.162 dst=10.120.10.122 src_port=1600
2007-06-14 21:47:46 192.168.254.1 action=Permit sent=840 rcvd=491 src=24.119.169.162 dst=10.120.10.122 src_port=13185 d
2007-06-14 21:47:49 192.168.254.1 action=Permit sent=3348 rcvd=18192 src=24.119.169.162 dst=10.120.10.122 src_port=4737
2007-06-14 21:47:55 192.168.254.1 action=Permit sent=3780 rcvd=34120 src=24.119.169.162 dst=10.120.10.122 src_port=3713
2007-06-14 21:47:57 192.168.254.1 action=Permit sent=3604 rcvd=30265 src=24.119.169.162 dst=10.120.10.122 src_port=6785
2007-06-14 21:47:58 192.168.254.1 action=Permit sent=3406 rcvd=39223 src=24.119.169.162 dst=10.120.10.122 src_port=5761
2007-06-14 21:47:59 192.168.254.1 action=Deny sent=0 rcvd=12288 src=10.130.9.3 dst=224.0.0.2 src_port=49415 dst_port=49
2007-06-14 21:48:04 192.168.254.1 action=Permit sent=549 rcvd=404 src=192.168.254.42 dst=208.188.166.68 src_port=7696 d
2007-06-14 21:48:05 192.168.254.1 action=Deny sent=0 rcvd=12288 src=10.130.9.2 dst=224.0.0.2 src_port=49415 dst_port=49
2007-06-14 21:48:09 192.168.254.1 action=Deny sent=0 rcvd=12288 src=10.130.9.3 dst=224.0.0.2 src_port=49415 dst_port=49
2007-06-14 21:48:09 192.168.254.1 action=Deny sent=0 rcvd=12288 src=10.130.9.2 dst=224.0.0.2 src_port=49415 dst_port=49
2007-06-14 21:48:10 192.168.254.1 action=Permit sent=407 rcvd=0 src=192.168.254.14 dst=204.61.5.130 src_port=260 dst_po
2007-06-14 21:48:13 192.168.254.1 action=Permit sent=1040 rcvd=0 src=192.168.254.14 dst=204.61.5.130 src_port=41216 dst
2007-06-14 21:48:15 192.168.254.1 action=Deny sent=0 rcvd=12288 src=10.130.9.3 dst=224.0.0.2 src_port=49415 dst_port=49
2007-06-14 21:48:16 192.168.254.1 action=Deny sent=0 rcvd=12264 src=10.130.9.3 dst=224.0.0.2 src_port=49415 dst_port=49

```

What can the investigator infer from the screenshot seen below?

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

**Answer: C**

**NEW QUESTION 239**

- (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 241**

- (Exam Topic 2)

Which of the following is a database in which information about every file and directory on an NT File System (NTFS) volume is stored?

- A. Volume Boot Record
- B. Master Boot Record
- C. GUID Partition Table
- D. Master File Table

**Answer: D**

**NEW QUESTION 243**

- (Exam Topic 2)

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

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

**Answer:** D

**NEW QUESTION 244**

- (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 246**

- (Exam Topic 2)

Bob works as information security analyst for a big finance company. One day, the anomaly-based intrusion detection system alerted that a volumetric DDOS targeting the main IP of the main web server was occurring. What kind of attack is it?

- A. IDS attack
- B. APT
- C. Web application attack
- D. Network attack

**Answer:** D

**NEW QUESTION 249**

- (Exam Topic 2)

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

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

**Answer:** A

**NEW QUESTION 250**

- (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 255**

- (Exam Topic 2)

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

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

**Answer:** C

**NEW QUESTION 259**

- (Exam Topic 2)

What must an investigator do before disconnecting an iPod from any type of computer?

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

**Answer:** A

**NEW QUESTION 260**

- (Exam Topic 2)

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

- A. Net config
- B. Net file
- C. Net share
- D. Net sessions

**Answer: B**

#### NEW QUESTION 265

- (Exam Topic 2)

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

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

**Answer: D**

#### NEW QUESTION 270

- (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 273

- (Exam Topic 2)

Pagefile.sys is a virtual memory file used to expand the physical memory of a computer. Select the registry path for the page file:

- A. HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management
- B. HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\System Management
- C. HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Device Management
- D. HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\PrefetchParameters

**Answer: A**

#### NEW QUESTION 274

- (Exam Topic 2)

Which of the following refers to the process of the witness being questioned by the attorney who called the latter to the stand?

- A. Witness Authentication
- B. Direct Examination
- C. Expert Witness
- D. Cross Questioning

**Answer: B**

#### NEW QUESTION 279

- (Exam Topic 2)

When investigating a wireless attack, what information can be obtained from the DHCP logs?

- A. The operating system of the attacker and victim computers
- B. IP traffic between the attacker and the victim
- C. MAC address of the attacker
- D. If any computers on the network are running in promiscuous mode

**Answer: C**

#### NEW QUESTION 284

- (Exam Topic 2)

When marking evidence that has been collected with the aa/ddmmyy/nnnn/zz format, what does the nnn denote?

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

**Answer: D**

**NEW QUESTION 286**

- (Exam Topic 2)

Which of the following files stores information about local Dropbox installation and account, email IDs linked with the account, current version/build for the local application, the host\_id, and local path information?

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

**Answer: C**

**NEW QUESTION 290**

- (Exam Topic 2)

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

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

**Answer: B**

**NEW QUESTION 291**

- (Exam Topic 2)

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

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

**Answer: A**

**NEW QUESTION 294**

- (Exam Topic 2)

In Windows Security Event Log, what does an event id of 530 imply?

- A. Logon Failure – Unknown user name or bad password
- B. Logon Failure – User not allowed to logon at this computer
- C. Logon Failure – Account logon time restriction violation
- D. Logon Failure – Account currently disabled

**Answer: C**

**NEW QUESTION 297**

- (Exam Topic 2)

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

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

**Answer: B**

**NEW QUESTION 301**

- (Exam Topic 2)

Which MySQL log file contains information on server start and stop?

- A. Slow query log file
- B. General query log file
- C. Binary log
- D. Error log file

**Answer: D**

**NEW QUESTION 306**

- (Exam Topic 2)

When carrying out a forensics investigation, why should you never delete a partition on a dynamic disk?

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

Answer: C

**NEW QUESTION 309**

- (Exam Topic 2)

Which network attack is described by the following statement?

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

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

Answer: A

**NEW QUESTION 312**

- (Exam Topic 2)

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

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

Answer: D

**NEW QUESTION 315**

- (Exam Topic 2)

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

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

Answer: C

**NEW QUESTION 316**

- (Exam Topic 2)

What is one method of bypassing a system BIOS password?

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

Answer: B

**NEW QUESTION 318**

- (Exam Topic 2)

Where is the startup configuration located on a router?

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

Answer: C

**NEW QUESTION 322**

- (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 326**

- (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 330**

- (Exam Topic 2)

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

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

**Answer: A**

**NEW QUESTION 335**

- (Exam Topic 2)

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

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

**Answer: B**

**NEW QUESTION 336**

- (Exam Topic 2)

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

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

**Answer: C**

**NEW QUESTION 337**

- (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 339**

- (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 were 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 341**

- (Exam Topic 2)

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

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

D. Written Informal Report

**Answer: B**

**NEW QUESTION 344**

- (Exam Topic 2)

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

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

**Answer: C**

**NEW QUESTION 349**

- (Exam Topic 2)

Annie is searching for certain deleted files on a system running Windows XP OS. Where will she find the files if they were not completely deleted from the system?

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

**Answer: B**

**NEW QUESTION 353**

- (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 356**

- (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 358**

- (Exam Topic 2)

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

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

**Answer: D**

**NEW QUESTION 363**

- (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 368**

- (Exam Topic 2)

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 371**

- (Exam Topic 2)

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

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

**Answer: A**

**NEW QUESTION 373**

- (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 377**

- (Exam Topic 2)

Which of the following file contains the traces of the applications installed, run, or uninstalled from a system?

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

**Answer: A**

**NEW QUESTION 379**

- (Exam Topic 2)

NTFS has reduced slack space than FAT, thus having lesser potential to hide data in the slack space. This is because:

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

**Answer: C**

**NEW QUESTION 380**

- (Exam Topic 2)

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

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

**Answer: A**

**NEW QUESTION 384**

- (Exam Topic 2)

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

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

D. Cryptanalysis

**Answer: B**

**NEW QUESTION 387**

- (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 389**

- (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 393**

- (Exam Topic 2)

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

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

**Answer: A**

**NEW QUESTION 395**

- (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 399**

- (Exam Topic 2)

Which of the following files stores information about a local Google Drive installation such as User email ID, Local Sync Root Path, and Client version installed?

- A. filecache.db
- B. config.db
- C. sigstore.db
- D. Sync\_config.db

**Answer: D**

**NEW QUESTION 402**

- (Exam Topic 2)

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

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

**Answer: A**

**NEW QUESTION 407**

- (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 411**

- (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 412**

- (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 416**

- (Exam Topic 2)

When using an iPod and the host computer is running Windows, what file system will be used?

- A. iPod+
- B. HFS
- C. FAT16
- D. FAT32

**Answer: D**

**NEW QUESTION 417**

- (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 420**

- (Exam Topic 2)

Watson, a forensic investigator, is examining a copy of an ISO file stored in CDFS format. What type of evidence is this?

- A. Data from a CD copied using Windows
- B. Data from a CD copied using Mac-based system
- C. Data from a DVD copied using Windows system
- D. Data from a CD copied using Linux system

**Answer: A**

**NEW QUESTION 424**

- (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 427**

- (Exam Topic 2)

Under confession, an accused criminal admitted to encrypting child pornography pictures and then hiding them within other pictures. What technique did the accused criminal employ?

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

**Answer: D**

**NEW QUESTION 430**

- (Exam Topic 2)

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

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

**Answer: B**

**NEW QUESTION 432**

- (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 435**

- (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 440**

- (Exam Topic 1)

Why is it a good idea to perform a penetration test from the inside?

- A. It is never a good idea to perform a penetration test from the inside
- B. Because 70% of attacks are from inside the organization
- C. To attack a network from a hacker's perspective
- D. It is easier to hack from the inside

**Answer: B**

**NEW QUESTION 443**

- (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 446**

- (Exam Topic 1)

What will the following command produce on a website login page? `SELECT email, passwd, login_id, full_name FROM members WHERE email = 'someone@somehwere.com'; DROP TABLE members; --'`

- A. Deletes the entire members table

- B. Inserts the Error! Reference source not found.email address into the members table
- C. Retrieves the password for the first user in the members table
- D. This command will not produce anything since the syntax is incorrect

**Answer:** A

**NEW QUESTION 448**

- (Exam Topic 1)

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

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

**Answer:** C

**NEW QUESTION 453**

- (Exam Topic 1)

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

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

**Answer:** A

**NEW QUESTION 458**

- (Exam Topic 1)

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

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

**Answer:** B

**NEW QUESTION 462**

- (Exam Topic 1)

Which of the following should a computer forensics lab used for investigations have?

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

**Answer:** B

**NEW QUESTION 467**

- (Exam Topic 1)

George is a senior security analyst working for a state agency in Florida. His state's congress just passed a bill mandating every state agency to undergo a security audit annually. After learning what will be required, George needs to implement an IDS as soon as possible before the first audit occurs. The state bill requires that an IDS with a "time-based induction machine" be used.

What IDS feature must George implement to meet this requirement?

- A. Signature-based anomaly detection
- B. Pattern matching
- C. Real-time anomaly detection
- D. Statistical-based anomaly detection

**Answer:** C

**NEW QUESTION 470**

- (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 471**

- (Exam Topic 1)

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

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

Answer: D

**NEW QUESTION 472**

- (Exam Topic 1)

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

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

Answer: A

**NEW QUESTION 475**

- (Exam Topic 1)

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

Answer: D

**NEW QUESTION 478**

- (Exam Topic 1)

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

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

Answer: A

**NEW QUESTION 479**

- (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 480**

- (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 485**

- (Exam Topic 1)

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

- A. EME

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

**Answer:** C

**NEW QUESTION 486**

- (Exam Topic 1)

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

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

**Answer:** A

**NEW QUESTION 489**

- (Exam Topic 1)

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

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

**Answer:** B

**NEW QUESTION 494**

- (Exam Topic 1)

An Employee is suspected of stealing proprietary information belonging to your company that he had no rights to possess. The information was stored on the Employees Computer that was protected with the NTFS Encrypted File System (EFS) and you had observed him copy the files to a floppy disk just before leaving work for the weekend. You detain the Employee before he leaves the building and recover the floppy disks and secure his computer. Will you be able to break the encryption so that you can verify that that the employee was in possession of the proprietary information?

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

**Answer:** B

**NEW QUESTION 498**

- (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 503**

- (Exam Topic 1)

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

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

**Answer:** C

**NEW QUESTION 504**

- (Exam Topic 1)

Paul's company is in the process of undergoing a complete security audit including logical and physical security testing. After all logical tests were performed; it is now time for the physical round to begin. None of the employees are made aware of this round of testing. The security-auditing firm sends in a technician dressed as an electrician. He waits outside in the lobby for some employees to get to work and follows behind them when they access the restricted areas. After entering the main office, he is able to get into the server room telling the IT manager that there is a problem with the outlets in that room. What type of attack has the technician performed?

- A. Tailgating
- B. Backtrapping
- C. Man trap attack
- D. Fuzzing

**Answer:** A

**NEW QUESTION 509**

- (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 514**

- (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 518**

- (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 519**

- (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 521**

- (Exam Topic 1)

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

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

**Answer:** D

**NEW QUESTION 526**

- (Exam Topic 1)

Terri works for a security consulting firm that is currently performing a penetration test on First National Bank in Tokyo. Terri's duties include bypassing firewalls and switches to gain access to the network. Terri sends an IP packet to one of the company's switches with ACK bit and the source address of her machine set. What is Terri trying to accomplish by sending this IP packet?

- A. Trick the switch into thinking it already has a session with Terri's computer
- B. Poison the switch's MAC address table by flooding it with ACK bits
- C. Crash the switch with a DoS attack since switches cannot send ACK bits
- D. Enable tunneling feature on the switch

Answer: A

**NEW QUESTION 530**

- (Exam Topic 1)

You are a computer forensics investigator working with local police department and you are called to assist in an investigation of threatening emails. The complainant has printer out 27 email messages from the suspect and gives the printouts to you. You inform her that you will need to examine her computer because you need access to the \_\_\_\_\_ in order to track the emails back to the suspect.

- A. Routing Table
- B. Firewall log
- C. Configuration files
- D. Email Header

Answer: D

**NEW QUESTION 534**

- (Exam Topic 1)

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

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

Answer: B

**NEW QUESTION 537**

- (Exam Topic 1)

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

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

Answer: A

**NEW QUESTION 538**

- (Exam Topic 1)

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

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

Answer: A

**NEW QUESTION 542**

- (Exam Topic 1)

The newer Macintosh Operating System is based on:

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

Answer: B

**NEW QUESTION 546**

- (Exam Topic 1)

You are called in to assist the police in an investigation involving a suspected drug dealer. The suspects house was searched by the police after a warrant was obtained and they located a floppy disk in the suspects 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 can 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 548

- (Exam Topic 1)

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

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

**Answer: C**

#### NEW QUESTION 553

- (Exam Topic 1)

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

- A. Refer the reporter to the attorney that retained you
- B. Say, "no comment"
- C. Answer all the reporter's questions as completely as possible
- D. Answer only the questions that help your case

**Answer: A**

#### NEW QUESTION 555

- (Exam Topic 1)

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

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

**Answer: B**

#### NEW QUESTION 558

- (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 559

- (Exam Topic 1)

The MD5 program is used to:

- A. wipe magnetic media before recycling it
- B. make directories on an evidence disk
- C. view graphics files on an evidence drive
- D. verify that a disk is not altered when you examine it

**Answer: D**

#### NEW QUESTION 564

- (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 566**

- (Exam Topic 1)

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

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

Answer: C

**NEW QUESTION 568**

- (Exam Topic 1)

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

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

Answer: C

**NEW QUESTION 570**

- (Exam Topic 1)

Bill is the accounting manager for Grummon and Sons LLC in Chicago. On a regular basis, he needs to send PDF documents containing sensitive information through E-mail to his customers.

Bill protects the PDF documents with a password and sends them to their intended recipients. Why PDF passwords do not offer maximum protection?

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

Answer: A

**NEW QUESTION 571**

- (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 575**

- (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 577**

- (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 579

- (Exam Topic 1)

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

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

Answer: A

#### NEW QUESTION 582

- (Exam Topic 1)

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\_pwd[12509]: (login) session opened for user simple by (uid=0)

Apr 26 06:44:36 victim7 PAM\_pwd[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 587

- (Exam Topic 1)

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

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

Answer: D

#### NEW QUESTION 588

- (Exam Topic 1)

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

Answer: A

#### NEW QUESTION 593

- (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 594

- (Exam Topic 1)

A state department site was recently attacked and all the servers had their disks erased. The incident response team sealed the area and commenced

investigation. During evidence collection they came across a zip disks that did not have the standard labeling on it. The incident team ran the disk on an isolated system and found that the system disk was accidentally erased. They decided to call in the FBI for further investigation. Meanwhile, they short listed possible suspects including three summer interns. Where did the incident team go wrong?

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

**Answer: C**

**NEW QUESTION 599**

- (Exam Topic 1)

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

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

**Answer: A**

**NEW QUESTION 602**

- (Exam Topic 1)

When a file is deleted by Windows Explorer or through the MS-DOS delete command, the operating system inserts \_\_\_\_\_ in the first letter position of the filename in the FAT database.

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

**Answer: D**

**NEW QUESTION 607**

- (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 608**

- (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 611**

- (Exam Topic 1)

This organization maintains a database of hash signatures for known software.

- A. International Standards Organization
- B. Institute of Electrical and Electronics Engineers
- C. National Software Reference Library
- D. American National standards Institute

**Answer: C**

**NEW QUESTION 615**

- (Exam Topic 1)

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

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

**Answer: A**

#### **NEW QUESTION 618**

- (Exam Topic 1)

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

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

**Answer: A**

#### **NEW QUESTION 619**

- (Exam Topic 1)

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

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

**Answer: D**

#### **NEW QUESTION 624**

- (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 625**

- (Exam Topic 1)

Before you are called to testify as an expert, what must an attorney do first?

- A. engage in damage control
- B. prove that the tools you used to conduct your examination are perfect
- C. read your curriculum vitae to the jury
- D. qualify you as an expert witness

**Answer: D**

#### **NEW QUESTION 630**

- (Exam Topic 1)

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

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

**Answer: C**

#### **NEW QUESTION 633**

- (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 635

- (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 640

- (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 644

- (Exam Topic 1)

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 648

- (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 649

- (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 652

- (Exam Topic 1)

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

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

**Answer:** A

#### NEW QUESTION 654

- (Exam Topic 1)

In what way do the procedures for dealing with evidence in a criminal case differ from the procedures for dealing with evidence in a civil case?

- A. evidence must be handled in the same way regardless of the type of case

- B. evidence procedures are not important unless you work for a law enforcement agency
- C. evidence in a criminal case must be secured more tightly than in a civil case
- D. evidence in a civil case must be secured more tightly than in a criminal case

**Answer: C**

**NEW QUESTION 656**

- (Exam Topic 1)

With Regard to using an Antivirus scanner during a computer forensics investigation, You should:

- A. Scan the suspect hard drive before beginning an investigation
- B. Never run a scan on your forensics workstation because it could change your systems configuration
- C. Scan your forensics workstation at intervals of no more than once every five minutes during an investigation
- D. Scan your Forensics workstation before beginning an investigation

**Answer: D**

**NEW QUESTION 660**

.....

## **Thank You for Trying Our Product**

### **We offer two products:**

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

2nd - Questions and Answers in PDF Format

### **312-49v10 Practice Exam Features:**

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

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