

# EC-Council

## Exam Questions 312-49v10

Computer Hacking Forensic Investigator (CHFI-v10)



#### NEW QUESTION 1

- (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 2

- (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 3

- (Exam Topic 1)

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

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

**Answer:** D

#### NEW QUESTION 4

- (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 5

- (Exam Topic 1)

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

Which organization coordinates computer crimes investigations throughout the United States?

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

**Answer:** B

#### NEW QUESTION 6

- (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 7

- (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 8

- (Exam Topic 1)

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

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

**Answer:** D

#### NEW QUESTION 9

- (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 10

- (Exam Topic 1)

You are working as an independent computer forensics investigator and received a call from a systems administrator for a local school system requesting your assistance. One of the students at the local high school is suspected of downloading inappropriate images from the Internet to a PC in the Computer lab. When you arrive at the school, the systems administrator hands you a hard drive and tells you that he made a "simple backup copy" of the hard drive in the PC and put it on this drive and requests that you examine that drive for evidence of the suspected images. You inform him that a "simple backup copy" will not provide deleted files or recover file fragments.

What type of copy do you need to make to ensure that the evidence found is complete and admissible in future proceeding?

- A. Bit-stream Copy
- B. Robust Copy
- C. Full backup Copy
- D. Incremental Backup Copy

**Answer:** C

#### NEW QUESTION 10

- (Exam Topic 1)

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

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

**Answer:** B

#### NEW QUESTION 12

- (Exam Topic 2)

What technique is used by JPEGs for compression?

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

**Answer:** C

#### NEW QUESTION 14

- (Exam Topic 2)

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

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

**Answer:** A

#### NEW QUESTION 15

- (Exam Topic 2)

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

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

**Answer:** A

#### NEW QUESTION 20

- (Exam Topic 2)

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

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

**Answer:** B

#### NEW QUESTION 24

- (Exam Topic 2)

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

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

**Answer:** D

#### NEW QUESTION 25

- (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 26

- (Exam Topic 1)

From the following spam mail header, identify the host IP that sent this spam? From jie02@netvigator.com jie02@netvigator.com Tue Nov 27 17:27:11 2001  
Received: from viruswall.ie.cuhk.edu.hk (viruswall [137.189.96.52]) by eng.ie.cuhk.edu.hk (8.11.6/8.11.6) with ESMTP id fAR9RAP23061 for ; Tue, 27 Nov 2001 17:27:10 +0800 (HKT)  
Received: from mydomain.com (pcd249020.netvigator.com [203.218.39.20]) by viruswall.ie.cuhk.edu.hk (8.12.1/8.12.1) with SMTP id fAR9QXwZ018431 for ; Tue, 27 Nov 2001 17:26:36 +0800 (HKT)  
Message-Id: >200111270926.fAR9QXwZ018431@viruswall.ie.cuhk.edu.hk From: "china hotel web"  
To: "Shlam"  
Subject: SHANGHAI (HILTON HOTEL) PACKAGE  
Date: Tue, 27 Nov 2001 17:25:58 +0800 MIME-Version: 1.0  
X- Priority: 3 X-MSMail- Priority: Normal  
Reply-To: "china hotel web"

- A. 137.189.96.52
- B. 8.12.1.0
- C. 203.218.39.20
- D. 203.218.39.50

**Answer:** C

#### NEW QUESTION 30

- (Exam Topic 2)

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

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

**Answer:** B

#### NEW QUESTION 34

- (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 39

- (Exam Topic 1)

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

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

**Answer:** B

#### NEW QUESTION 43

- (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 47

- (Exam Topic 1)

What will the following command accomplish?

- A. Test ability of a router to handle over-sized packets
- B. Test the ability of a router to handle under-sized packets
- C. Test the ability of a WLAN to handle fragmented packets
- D. Test the ability of a router to handle fragmented packets

**Answer:** A

#### NEW QUESTION 51

- (Exam Topic 1)

You setup SNMP in multiple offices of your company. Your SNMP software manager is not receiving data from other offices like it is for your main office. You suspect that firewall changes are to blame. What ports should you open for SNMP to work through Firewalls? (Choose two.)

- A. 162
- B. 161
- C. 163
- D. 160

**Answer:** AB

#### NEW QUESTION 54

- (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 58**

- (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 59**

- (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 64**

- (Exam Topic 1)

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

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

**Answer:** D

**NEW QUESTION 67**

- (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 70**

- (Exam Topic 1)

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

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

**Answer:** A

**NEW QUESTION 71**

- (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 72

- (Exam Topic 1)

Item 2If you come across a sheepdip machine at your client site, what would you infer?

- A. A sheepdip coordinates several honeypots
- B. A sheepdip computer is another name for a honeypot
- C. A sheepdip computer is used only for virus-checking.
- D. A sheepdip computer defers a denial of service attack

**Answer: C**

#### NEW QUESTION 76

- (Exam Topic 1)

Study the log given below and answer the following question:

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

Precautionary measures to prevent this attack would include writing firewall rules. Of these firewall rules, which among the following would be appropriate?

- A. Disallow UDP53 in from outside to DNS server
- B. Allow UDP53 in from DNS server to outside
- C. Disallow TCP53 in from secondaries or ISP server to DNS server
- D. Block all UDP traffic

**Answer: A**

#### NEW QUESTION 78

- (Exam Topic 1)

You should make at least how many bit-stream copies of a suspect drive?

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

**Answer: B**

#### NEW QUESTION 79

- (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 84

- (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 85

- (Exam Topic 1)

Julia is a senior security analyst for Berber Consulting group. She is currently working on a contract for a small accounting firm in Florid a. They have given her permission to perform social engineering attacks on the company to see if their in-house training did any good. Julia calls the main number for the accounting firm and talks to the receptionist. Julia says that she is an IT technician from the company's main office in Iowa. She states that she needs the receptionist's network username and password to troubleshoot a problem they are having. Julia says that Bill Hammond, the CEO of the company, requested this information. After hearing the name of the CEO, the receptionist gave Julia all the information she asked for. What principal of social engineering did Julia use?

- A. Social Validation
- B. Scarcity
- C. Friendship/Liking
- D. Reciprocation

**Answer:** D

#### NEW QUESTION 90

- (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 95

- (Exam Topic 1)

You have compromised a lower-level administrator account on an Active Directory network of a small company in Dallas, Texas. You discover Domain Controllers through enumeration. You connect to one of the Domain Controllers on port 389 using ldp.exe. What are you trying to accomplish here?

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

**Answer:** D

#### NEW QUESTION 97

- (Exam Topic 1)

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

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

**Answer:** A

#### NEW QUESTION 99

- (Exam Topic 1)

The offset in a hexadecimal code is:

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

**Answer:** B

#### NEW QUESTION 104

- (Exam Topic 1)

After passively scanning the network of Department of Defense (DoD), you switch over to active scanning to identify live hosts on their network. DoD is a large organization and should respond to any number of scans. You start an ICMP ping sweep by sending an IP packet to the broadcast address. Only five hosts respond to your ICMP pings; definitely not the number of hosts you were expecting. Why did this ping sweep only produce a few responses?

- A. Only IBM AS/400 will reply to this scan
- B. Only Windows systems will reply to this scan
- C. A switched network will not respond to packets sent to the broadcast address
- D. Only Unix and Unix-like systems will reply to this scan

**Answer:** D

#### NEW QUESTION 108

- (Exam Topic 1)

James is testing the ability of his routers to withstand DoS attacks. James sends ICMP ECHO requests to the broadcast address of his network. What type of DoS attack is James testing against his network?

- A. Smurf
- B. Trinoo
- C. Fraggle
- D. SYN flood



**Answer:** A

**NEW QUESTION 110**

- (Exam Topic 1)

Why are Linux/Unix based computers better to use than Windows computers for idle scanning?

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

**Answer:** C

**NEW QUESTION 113**

- (Exam Topic 1)

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

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

**Answer:** D

**NEW QUESTION 116**

- (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 117**

- (Exam Topic 1)

What is the following command trying to accomplish?

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

**Answer:** A

**NEW QUESTION 122**

- (Exam Topic 1)

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

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

**Answer:** ACDE

**NEW QUESTION 124**

- (Exam Topic 1)

In Linux, what is the smallest possible shellcode?

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

**Answer:** A

**NEW QUESTION 125**

- (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 126

- (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 131

- (Exam Topic 1)

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

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

**Answer:** D

#### NEW QUESTION 132

- (Exam Topic 1)

What is the target host IP in the following command?

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

**Answer:** A

#### NEW QUESTION 135

- (Exam Topic 1)

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

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

**Answer:** C

#### NEW QUESTION 139

- (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 143

- (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 144

- (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 147

- (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 149

- (Exam Topic 1)

This is original file structure database that Microsoft originally designed for floppy disks. It is written to the outermost track of a disk and contains information about each file stored on the drive.

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

**Answer:** C

#### NEW QUESTION 152

- (Exam Topic 1)

Sectors in hard disks typically contain how many bytes?

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

**Answer:** B

#### NEW QUESTION 153

- (Exam Topic 1)

Jim performed a vulnerability analysis on his network and found no potential problems. He runs another utility that executes exploits against his system to verify the results of the vulnerability test.

The second utility executes five known exploits against his network in which the vulnerability analysis said were not exploitable. What kind of results did Jim receive from his vulnerability analysis?

- A. False negatives
- B. False positives
- C. True negatives
- D. True positives

**Answer:** A

#### NEW QUESTION 155

- (Exam Topic 1)

When obtaining a warrant, it is important to:

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

**Answer:** A

#### NEW QUESTION 156

- (Exam Topic 1)

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

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

**Answer: B**

#### NEW QUESTION 159

- (Exam Topic 1)

An Expert witness give an opinion if:

- A. The Opinion, inferences or conclusions depend on special knowledge, skill or training not within the ordinary experience of lay jurors
- B. To define the issues of the case for determination by the finder of fact
- C. To stimulate discussion between the consulting expert and the expert witness
- D. To deter the witness from expanding the scope of his or her investigation beyond the requirements of the case

**Answer: A**

#### NEW QUESTION 161

- (Exam Topic 4)

When Investigating a system, the forensics analyst discovers that malicious scripts were Injected Into benign and trusted websites. The attacker used a web application to send malicious code. In the form of a browser side script, to a different end-user. What attack was performed here?

- A. Brute-force attack
- B. Cookie poisoning attack
- C. Cross-site scripting attack
- D. SQL injection attack

**Answer: C**

#### NEW QUESTION 166

- (Exam Topic 4)

Which Federal Rule of Evidence speaks about the Hearsay exception where the availability of the declarant Is immaterial and certain characteristics of the declarant such as present sense Impression, excited utterance, and recorded recollection are also observed while giving their testimony?

- A. Rule 801
- B. Rule 802
- C. Rule 804
- D. Rule 803

**Answer: D**

#### NEW QUESTION 171

- (Exam Topic 4)

"No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court" - this principle Is advocated by which of the following?

- A. The Association of Chief Police Officers (ACPO) Principles of Digital Evidence
- B. Locard's exchange principle
- C. Scientific Working Group on Imaging Technology (SWGIT)
- D. FBI Cyber Division

**Answer: A**

#### NEW QUESTION 175

- (Exam Topic 4)

This is a statement, other than one made by the declarant while testifying at the trial or hearing, offered in evidence to prove the truth of the matter asserted. Which among the following is suitable for the above statement?

- A. Testimony by the accused
- B. Limited admissibility
- C. Hearsay rule
- D. Rule 1001

**Answer: C**

#### NEW QUESTION 177

- (Exam Topic 4)

A forensic analyst has been tasked with investigating unusual network activity Inside a retail company's network. Employees complain of not being able to access services, frequent rebooting, and anomalies In log files. The Investigator requested log files from the IT administrator and after carefully reviewing them, he finds the following log entry:

```
12:34:35 192.2.3.4 HEAD GET /login.asp?username=blah" or 1=1 - 12:34:35 192.2.3.4 HEAD GET  
/login.asp?username=blah" or )1=1 (-- 12:34:35 192.2.3.4 HEAD GET  
/login.asp?username+blah" or exec master..xp_cmdshell 'net user test testpass - -
```

What type of attack was performed on the companies' web application?

- A. Directory transversal
- B. Unvalidated input
- C. Log tampering
- D. SQL injection

**Answer:** D

#### NEW QUESTION 181

- (Exam Topic 4)

The working of the Tor browser is based on which of the following concepts?

- A. Both static and default routing
- B. Default routing
- C. Static routing
- D. Onion routing

**Answer:** D

#### NEW QUESTION 183

- (Exam Topic 4)

An investigator seized a notebook device installed with a Microsoft Windows OS. Which type of files would support an investigation of the data size and structure in the device?

- A. Ext2 and Ext4
- B. APFSandHFS
- C. HFS and GNUC
- D. NTFSandFAT

**Answer:** D

#### NEW QUESTION 187

- (Exam Topic 4)

In Java, when multiple applications are launched, multiple Dalvik Virtual Machine instances occur that consume memory and time. To avoid that. Android Implements a process that enables low memory consumption and quick start-up time. What is the process called?

- A. init
- B. Media server
- C. Zygote
- D. Daemon

**Answer:** C

#### NEW QUESTION 188

- (Exam Topic 4)

Web browsers can store relevant information from user activities. Forensic investigators may retrieve files, lists, access history, cookies, among other digital footprints. Which tool can contribute to this task?

- A. Most Recently Used (MRU) list
- B. MZCacheView
- C. Google Chrome Recovery Utility
- D. Task Manager

**Answer:** B

#### NEW QUESTION 193

- (Exam Topic 4)

Simona has written a regular expression for the detection of web application-specific attack attempt that reads as `/((\%3C)|<K(\%2F)|V)*[a-zA-Z0-9\%I*(\%3E)|>)/lx`. Which of the following does the part `(\%3E)|>` look for?

- A. Alphanumeric string or its hex equivalent
- B. Opening angle bracket or its hex equivalent
- C. Closing angle bracket or its hex equivalent
- D. Forward slash for a closing tag or its hex equivalent

**Answer:** D

#### NEW QUESTION 198

- (Exam Topic 4)

Which of the following malware targets Android mobile devices and installs a backdoor that remotely installs applications from an attacker-controlled server?

- A. Felix
- B. XcodeGhost
- C. xHelper
- D. Unflod

**Answer:** C

#### NEW QUESTION 199

- (Exam Topic 4)

Jeff is a forensics investigator for a government agency's cyber security office. Jeff is tasked with acquiring a memory dump of a Windows 10 computer that was involved in a DDoS attack on the government agency's web application. Jeff is onsite to collect the memory. What tool could Jeff use?

- A. Volatility
- B. Autopsy
- C. RAM Mapper
- D. Memcheck

**Answer:** A

#### NEW QUESTION 204

- (Exam Topic 4)

Which of the following statements pertaining to First Response is true?

- A. First Response is a part of the investigation phase
- B. First Response is a part of the post-investigation phase
- C. First Response is a part of the pre-investigation phase
- D. First Response is neither a part of pre-investigation phase nor a part of investigation phase
- E. It only involves attending to a crime scene first and taking measures that assist forensic investigators in executing their tasks in the investigation phase more efficiently

**Answer:** A

#### NEW QUESTION 208

- (Exam Topic 4)

Ronald, a forensic investigator, has been hired by a financial services organization to investigate an attack on their MySQL database server, which is hosted on a Windows machine named WIN-DTRAI83202X. Ronald wants to retrieve information on the changes that have been made to the database. Which of the following files should Ronald examine for this task?

- A. relay-log.info
- B. WIN-DTRAI83202Xrelay-bin.index
- C. WIN-DTRAI83202Xslow.log
- D. WIN-DTRAI83202X-bin.nnnnnn

**Answer:** C

#### NEW QUESTION 210

- (Exam Topic 4)

What happens to the header of the file once it is deleted from the Windows OS file systems?

- A. The OS replaces the first letter of a deleted file name with a hex byte code: E5h
- B. The OS replaces the entire hex byte coding of the file.
- C. The hex byte coding of the file remains the same, but the file location differs
- D. The OS replaces the second letter of a deleted file name with a hex byte code: Eh5

**Answer:** A

#### NEW QUESTION 212

- (Exam Topic 4)

The information security manager at a national legal firm has received several alerts from the intrusion detection system that a known attack signature was detected against the organization's file server. What should the information security manager do first?

- A. Report the incident to senior management
- B. Update the anti-virus definitions on the file server
- C. Disconnect the file server from the network
- D. Manually investigate to verify that an incident has occurred

**Answer:** C

#### NEW QUESTION 213

- (Exam Topic 4)

A file requires 10 KB space to be saved on a hard disk partition. An entire cluster of 32 KB has been allocated for this file. The remaining, unused space of 22 KB on this cluster will be identified as .

- A. Swap space
- B. Cluster space
- C. Slack space
- D. Sector space

**Answer:** D

#### NEW QUESTION 218

- (Exam Topic 4)

What is the extension used by Windows OS for shortcut files present on the machine?



- A. .log
- B. .pf
- C. .lnk
- D. .dat

**Answer:** C

#### NEW QUESTION 222

- (Exam Topic 4)

A call detail record (CDR) provides metadata about calls made over a phone service. From the following data fields, which one is not contained in a CDR.

- A. The call duration
- B. A unique sequence number identifying the record
- C. The language of the call
- D. Phone number receiving the call

**Answer:** C

#### NEW QUESTION 224

- (Exam Topic 4)

Derrick, a forensic specialist, was investigating an active computer that was executing various processes. Derrick wanted to check whether this system was used in an incident that occurred earlier. He started inspecting and gathering the contents of RAM, cache, and DLLs to identify incident signatures. Identify the data acquisition method employed by Derrick in the above scenario.

- A. Dead data acquisition
- B. Static data acquisition
- C. Non-volatile data acquisition
- D. Live data acquisition

**Answer:** C

#### NEW QUESTION 229

- (Exam Topic 4)

Cybercriminals sometimes use compromised computers to commit other crimes, which may involve using computers or networks to spread malware or illegal information. Which type of cybercrime stops users from using a device or network, or prevents a company from providing a software service to its customers?

- A. Denial-of-Service (DoS) attack
- B. Malware attack
- C. Ransomware attack
- D. Phishing

**Answer:** C

#### NEW QUESTION 233

- (Exam Topic 4)

Which of the following directory contains the binary files or executables required for system maintenance and administrative tasks on a Linux system?

- A. /sbin
- B. /bin
- C. /usr
- D. /lib

**Answer:** A

#### NEW QUESTION 237

- (Exam Topic 4)

William is examining a log entry that reads 192.168.0.1 - - [18/Jun/2020:12:42:29 +0000] "GET / HTTP/1.1" 200 1861. Which of the following logs does the log entry belong to?

- A. The combined log format of Apache access log
- B. The common log format of Apache access log
- C. Apache error log
- D. IIS log

**Answer:** A

#### NEW QUESTION 238

- (Exam Topic 4)

Assume there is a file named myfile.txt in C: drive that contains hidden data streams. Which of the following commands would you issue to display the contents of a data stream?

- A. echo text > program: source\_file
- B. myfile.dat: stream 1
- C. C:\MORE < myfile.txt:stream1
- D. C:\>ECHO text\_message > myfile.txt:stream1

**Answer:** A

#### NEW QUESTION 240

- (Exam Topic 4)

Fred, a cybercrime Investigator for the FBI, finished storing a solid-state drive in a static resistant bag and filled out the chain of custody form. Two days later, John grabbed the solid-state drive and created a clone of it (with write blockers enabled) in order to investigate the drive. He did not document the chain of custody though. When John was finished, he put the solid-state drive back in the static resistant and placed it back in the evidence locker. A day later, the court trial began and upon presenting the evidence and the supporting documents, the chief Justice outright rejected them. Which of the following statements strongly support the reason for rejecting the evidence?

- A. Block clones cannot be created with solid-state drives
- B. Write blockers were used while cloning the evidence
- C. John did not document the chain of custody
- D. John investigated the clone instead of the original evidence itself

**Answer: C**

#### NEW QUESTION 241

- (Exam Topic 4)

Which following forensic tool allows investigator to detect and extract hidden streams on NTFS drive?

- A. Stream Detector
- B. TimeStomp
- C. Autopsy
- D. analyzeMFT

**Answer: A**

#### NEW QUESTION 246

- (Exam Topic 4)

Harry has collected a suspicious executable file from an infected system and seeks to reverse its machine code to instructions written in assembly language. Which tool should he use for this purpose?

- A. Ollydbg
- B. oledump
- C. HashCalc
- D. BinText

**Answer: A**

#### NEW QUESTION 247

- (Exam Topic 4)

An investigator wants to extract passwords from SAM and System Files. Which tool can the investigator use to obtain a list of users, passwords, and their hashes in this case?

- A. PWdump7
- B. HashKey
- C. Ntlix
- D. FileMerlin

**Answer: A**

#### NEW QUESTION 249

- (Exam Topic 4)

A cybercriminal is attempting to remove evidence from a Windows computer. He deletes the file evidence1.doc, sending it to Windows Recycle Bin. The cybercriminal then empties the Recycle Bin. After having been removed from the Recycle Bin, what will happen to the data?

- A. The data will remain in its original clusters until it is overwritten
- B. The data will be moved to new clusters in unallocated space
- C. The data will become corrupted, making it unrecoverable
- D. The data will be overwritten with zeroes

**Answer: A**

#### NEW QUESTION 252

- (Exam Topic 4)

Jack is reviewing file headers to verify the file format and hopefully find more information of the file. After a careful review of the data chunks through a hex editor, Jack finds the binary value 0xffd8ff. Based on the above information, what type of format is the file/image saved as?

- A. BMP
- B. GIF
- C. ASCII
- D. JPEG

**Answer: D**

#### NEW QUESTION 255

- (Exam Topic 4)

Cloud forensic investigations impose challenges related to multi-jurisdiction and multi-tenancy aspects. To have a better understanding of the roles and responsibilities between the cloud service provider (CSP) and the client, which document should the forensic investigator review?

- A. Service level agreement
- B. Service level management
- C. National and local regulation
- D. Key performance indicator

**Answer:** A

#### NEW QUESTION 256

- (Exam Topic 4)

Donald made an OS disk snapshot of a compromised Azure VM under a resource group being used by the affected company as a part of forensic analysis process. He then created a vhd file out of the snapshot and stored it in a file share and as a page blob as backup in a storage account under different region. What is the next thing he should do as a security measure?

- A. Recommend changing the access policies followed by the company
- B. Delete the snapshot from the source resource group
- C. Delete the OS disk of the affected VM altogether
- D. Create another VM by using the snapshot

**Answer:** C

#### NEW QUESTION 258

- (Exam Topic 4)

A breach resulted from a malware attack that evaded detection and compromised the machine memory without installing any software or accessing the hard drive. What technique did the adversaries use to deliver the attack?

- A. Fileless
- B. Trojan
- C. JavaScript
- D. Spyware

**Answer:** A

#### NEW QUESTION 263

- (Exam Topic 4)

For the purpose of preserving the evidentiary chain of custody, which of the following labels is not appropriate?

- A. Relevant circumstances surrounding the collection
- B. General description of the evidence
- C. Exact location the evidence was collected from
- D. SSN of the person collecting the evidence

**Answer:** D

#### NEW QUESTION 265

- (Exam Topic 4)

Which of the following Windows event logs record events related to device drives and hardware changes?

- A. Forwarded events log
- B. System log
- C. Application log
- D. Security log

**Answer:** B

#### NEW QUESTION 267

- (Exam Topic 4)

Recently, an Internal web app that a government agency utilizes has become unresponsive, Betty, a network engineer for the government agency, has been tasked to determine the cause of the web application's unresponsiveness. Betty launches Wireshark and begins capturing the traffic on the local network. While analyzing the results, Betty noticed that a syn flood attack was underway. How did Betty know a syn flood attack was occurring?

- A. Wireshark capture shows multiple ACK requests and SYN responses from single/multiple IP address(es)
- B. Wireshark capture does not show anything unusual and the issue is related to the web application
- C. Wireshark capture shows multiple SYN requests and RST responses from single/multiple IP address(es)
- D. Wireshark capture shows multiple SYN requests and ACK responses from single/multiple IP address(es)

**Answer:** C

#### NEW QUESTION 270

- (Exam Topic 4)

Robert needs to copy an OS disk snapshot of a compromised VM to a storage account in different region for further investigation. Which of the following should he use in this scenario?

- A. Azure CLI
- B. Azure Monitor

- C. Azure Active Directory
- D. Azure Portal

**Answer:** D

**NEW QUESTION 271**

- (Exam Topic 4)

Which of the following tools is used to dump the memory of a running process, either immediately or when an error condition occurs?

- A. FATKit
- B. Coreography
- C. Belkasoft Live RAM Capturer
- D. CacheInf

**Answer:** C

**NEW QUESTION 276**

- (Exam Topic 4)

Matthew has been assigned the task of analyzing a suspicious MS Office document via static analysis over an Ubuntu-based forensic machine. He wants to see what type of document it is, whether it is encrypted, or contains any flash objects/VBA macros. Which of the following python-based script should he run to get relevant information?

- A. oleform.py
- B. oleid.py
- C. oledir.py
- D. pdfid.py

**Answer:** B

**NEW QUESTION 279**

- (Exam Topic 4)

An Investigator is checking a Cisco firewall log that reads as follows:

Aug 21 2019 09:16:44: %ASA-1-106021: Deny ICMP reverse path check from 10.0.0.44 to 10.0.0.33 on Interface outside

What does %ASA-1-106021 denote?

- A. Mnemonic message
- B. Type of traffic
- C. Firewall action
- D. Type of request

**Answer:** C

**NEW QUESTION 281**

- (Exam Topic 4)

"In exceptional circumstances, where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to explain his/her actions and the impact of those actions on the evidence, in the court." Which ACPO principle states this?

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

**Answer:** D

**NEW QUESTION 285**

- (Exam Topic 4)

allows a forensic investigator to identify the missing links during investigation.

- A. Evidence preservation
- B. Chain of custody
- C. Evidence reconstruction
- D. Exhibit numbering

**Answer:** C

**NEW QUESTION 286**

- (Exam Topic 4)

Debbie has obtained a warrant to search a known pedophile's house. Debbie went to the house and executed the search warrant to seize digital devices that have been recorded as being used for downloading illicit images. She seized all digital devices except a digital camera. Why did she not collect the digital camera?

- A. The digital camera was not listed as one of the digital devices in the warrant
- B. The vehicle Debbie was using to transport the evidence was already full and could not carry more items
- C. Debbie overlooked the digital camera because it is not a computer system
- D. The digital camera was old
- E. had a cracked screen, and did not have batteries
- F. Therefore, it could not have been used in a crime.

**Answer:** A

**NEW QUESTION 291**

- (Exam Topic 4)

Malware analysis can be conducted in various manners. An investigator gathers a suspicious executable file and uploads it to VirusTotal in order to confirm whether the file is malicious, provide information about its functionality, and provide information that will allow to produce simple network signatures. What type of malware analysis was performed here?

- A. Static
- B. Volatile
- C. Dynamic
- D. Hybrid

**Answer:** D

**NEW QUESTION 292**

- (Exam Topic 3)

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

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

**Answer:** A

**NEW QUESTION 296**

- (Exam Topic 3)

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

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

**Answer:** C

**NEW QUESTION 299**

- (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 302**

- (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 307**

- (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 310**

- (Exam Topic 3)

Which of the following processes is part of the dynamic malware analysis?

- A. Process Monitoring
- B. Malware disassembly
- C. Searching for the strings
- D. File fingerprinting

**Answer:** A

**NEW QUESTION 314**

- (Exam Topic 3)

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

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

**Answer:** D

**NEW QUESTION 318**

- (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 321**

- (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 326**

- (Exam Topic 3)

What does the bytes 0x0B-0x53 represent in the boot sector of NTFS volume on Windows 2000?

- A. Jump instruction and the OEM ID
- B. BIOS Parameter Block (BPB) and the OEM ID
- C. BIOS Parameter Block (BPB) and the extended BPB
- D. Bootstrap code and the end of the sector marker

**Answer:** C

**NEW QUESTION 329**

- (Exam Topic 3)

What is cold boot (hard boot)?

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

**Answer:** D

**NEW QUESTION 331**

- (Exam Topic 3)

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




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

**Answer:** A

**NEW QUESTION 334**

- (Exam Topic 3)

What document does the screenshot represent?



The screenshot shows a form for evidence collection. It has several fields with folder icons: 'Laboratory or Agency Name', 'Case Number', 'Received from (Name and Title)', 'Address and Telephone Number', 'Location from where Evidence Obtained', 'Reason Evidence Was Obtained', and 'Date and Time Evidence Was Obtained'. Below these fields is a table with three columns: 'Item Number', 'Quantity', and 'Description of Item'.

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

**Answer:** D

**NEW QUESTION 337**

- (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 340**

- (Exam Topic 3)

Which of the following web browser uses the Extensible Storage Engine (ESE) database format to store browsing records, including history, cache, and cookies?

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

**Answer:** C

**NEW QUESTION 341**

- (Exam Topic 3)

What is the purpose of using Obfuscator in malware?

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

**Answer:** C

**NEW QUESTION 342**

- (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 343**

- (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 346**

- (Exam Topic 3)

An investigator has extracted the device descriptor for a 1GB thumb drive that looks like: Disk&Ven\_Best\_Buy&Prod\_Geek\_Squad\_U3&Rev\_6.15. What does the “Geek\_Squad” part represent?

- A. Product description
- B. Manufacturer Details
- C. Developer description
- D. Software or OS used

**Answer:** A

**NEW QUESTION 350**

- (Exam Topic 3)

Which type of attack is possible when attackers know some credible information about the victim's password, such as the password length, algorithms involved, or the strings and characters used in its creation?

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

**Answer:** A

**NEW QUESTION 355**

- (Exam Topic 3)

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

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

**Answer:** B

**NEW QUESTION 359**

- (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 362**

- (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 364

- (Exam Topic 3)

You are asked to build a forensic lab and your manager has specifically informed you to use copper for lining the walls, ceilings, and floor. What is the main purpose of lining the walls, ceilings, and floor with copper?

- A. To control the room temperature
- B. To strengthen the walls, ceilings, and floor
- C. To avoid electromagnetic emanations
- D. To make the lab sound proof

**Answer:** D

#### NEW QUESTION 366

- (Exam Topic 3)

Which of the following tool can reverse machine code to assembly language?

- A. PEiD
- B. RAM Capturer
- C. IDA Pro
- D. Deep Log Analyzer

**Answer:** C

#### NEW QUESTION 371

- (Exam Topic 3)

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

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

**Answer:** D

#### NEW QUESTION 376

- (Exam Topic 3)

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

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

**Answer:** C

#### NEW QUESTION 379

- (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 384

- (Exam Topic 3)

POP3 is an Internet protocol, which is used to retrieve emails from a mail server. Through which port does an email client connect with a POP3 server?

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

**Answer:** A

#### NEW QUESTION 387

- (Exam Topic 3)

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

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

**Answer:** D

**NEW QUESTION 390**

- (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 394**

- (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 395**

- (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 396**

- (Exam Topic 3)

Which of the following setups should a tester choose to analyze malware behavior?

- A. A virtual system with internet connection
- B. A normal system without internet connect
- C. A normal system with internet connection
- D. A virtual system with network simulation for internet connection

**Answer:** D

**NEW QUESTION 401**

- (Exam Topic 3)

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

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

**Answer:** D

**NEW QUESTION 403**

- (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 405**

- (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 406**

- (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 408**

- (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 410**

- (Exam Topic 3)

Which of the following protocols allows non-ASCII files, such as video, graphics, and audio, to be sent through the email messages?

- A. MIME
- B. BINHEX
- C. UT-16
- D. UUCODE

**Answer:** A

**NEW QUESTION 411**

- (Exam Topic 3)

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

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

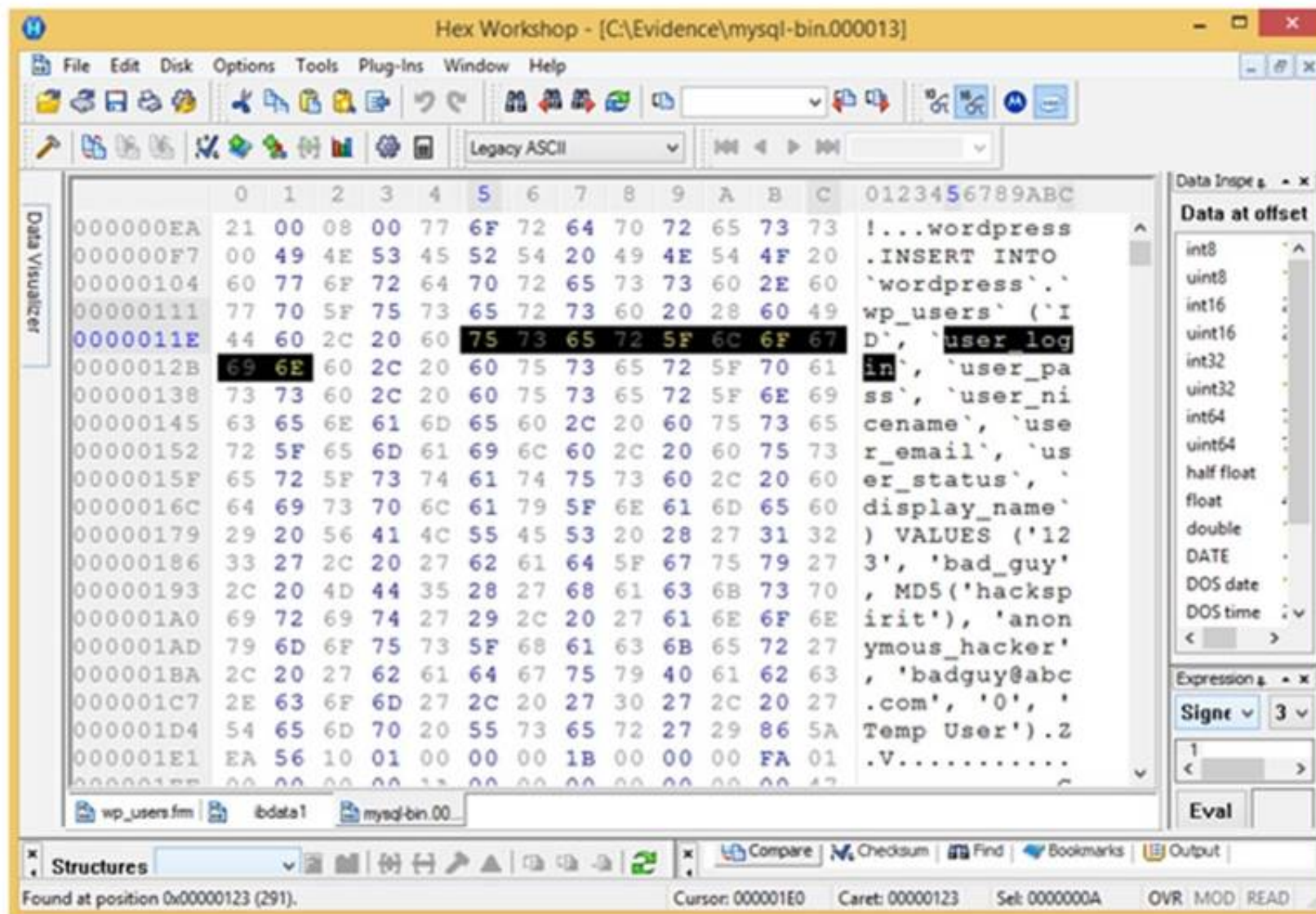
**Answer:** C

**NEW QUESTION 414**

- (Exam Topic 3)

Analyze the hex representation of mysql-bin.000013 file in the screenshot below. Which of the following will be an inference from this analysis?





- A. A user with username bad\_guy has logged into the WordPress web application
- B. A WordPress user has been created with the username anonymous\_hacker
- C. An attacker with name anonymous\_hacker has replaced a user bad\_guy in the WordPress database
- D. A WordPress user has been created with the username bad\_guy

**Answer: D**

#### NEW QUESTION 415

- (Exam Topic 3)

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

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

**Answer: D**

#### NEW QUESTION 420

- (Exam Topic 3)

What is the role of Alloc.c in Apache core?

- A. It handles allocation of resource pools
- B. It is useful for reading and handling of the configuration files
- C. It takes care of all the data exchange and socket connections between the client and the server
- D. It handles server start-ups and timeouts

**Answer: A**

#### NEW QUESTION 425

- (Exam Topic 3)

Robert, a cloud architect, received a huge bill from the cloud service provider, which usually doesn't happen. After analyzing the bill, he found that the cloud resource consumption was very high. He then examined the cloud server and discovered that a malicious code was running on the server, which was generating huge but harmless traffic from the server. This means that the server has been compromised by an attacker with the sole intention to hurt the cloud customer financially. Which attack is described in the above scenario?

- A. XSS Attack
- B. DDoS Attack (Distributed Denial of Service)
- C. Man-in-the-cloud Attack
- D. EDoS Attack (Economic Denial of Service)



**Answer:** B

**NEW QUESTION 429**

- (Exam Topic 3)

Which among the following web application threats is resulted when developers expose various internal implementation objects, such as files, directories, database records, or key-through references?

- A. Remote File Inclusion
- B. Cross Site Scripting
- C. Insecure Direct Object References
- D. Cross Site Request Forgery

**Answer:** C

**NEW QUESTION 433**

- (Exam Topic 3)

In which of these attacks will a steganalyst use a random message to generate a stego-object by using some steganography tool, to find the steganography algorithm used to hide the information?

- A. Chosen-message attack
- B. Known-cover attack
- C. Known-message attack
- D. Known-stego attack

**Answer:** A

**NEW QUESTION 438**

- (Exam Topic 3)

CAN-SPAM act requires that you:

- A. Don't use deceptive subject lines
- B. Don't tell the recipients where you are located
- C. Don't identify the message as an ad
- D. Don't use true header information

**Answer:** A

**NEW QUESTION 442**

- (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 446**

- (Exam Topic 3)

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

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

**Answer:** B

**NEW QUESTION 449**

- (Exam Topic 3)

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

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

**Answer:** D

**NEW QUESTION 452**

- (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 455**

- (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 460**

- (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 464**

- (Exam Topic 3)

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

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

**Answer:** D

**NEW QUESTION 468**

- (Exam Topic 3)

What is the investigator trying to analyze if the system gives the following image as output?



```

Administrator: Command Prompt
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32\C:\Users\Admin\Desktop\logonSessions\logonsessions.exe

Logonsessions v1.3
Copyright (C) 2004-2015 Mark Russinovich
Sysinternals - www.sysinternals.com

[0] Logon session 00000000:000003e7:
  User name:      WORKGROUP\RD-006$
  Auth package:   NTLM
  Logon type:     (none)
  Session:        0
  Sid:            S-1-5-18
  Logon time:     3/10/2016 3:32:46 AM
  Logon server:
  DNS Domain:
  UPN:

[1] Logon session 00000000:00000209:
  User name:
  Auth package:   NTLM
  Logon type:     (none)
  Session:        0
  Sid:            (none)
  Logon time:     3/10/2016 3:32:46 AM
  Logon server:
  DNS Domain:
  UPN:

[2] Logon session 00000000:000003e4:
  User name:      WORKGROUP\RD-006$
  Auth package:   Negotiate
  Logon type:     Service
  Session:        0
  Sid:            S-1-5-20
  Logon time:     3/10/2016 3:32:46 AM
  Logon server:
  DNS Domain:
  UPN:
  
```

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

**Answer: B**

#### NEW QUESTION 473

- (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 476

- (Exam Topic 3)

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

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

**Answer: C**

#### NEW QUESTION 481

- (Exam Topic 3)

Lynne receives the following email:

Dear lynne@gmail.com! We are sorry to inform you that your ID has been temporarily frozen due to incorrect or missing information saved at 2016/11/10 20:40:24  
 You have 24 hours to fix this problem or risk to be closed permanently! To proceed Please Connect >> My Apple ID

Thank You The link to My Apple ID shows <http://byggarbetsplatsen.se/backup/signon/> What type of attack is this?

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

**Answer: B**

#### NEW QUESTION 482

- (Exam Topic 3)

What does the command “C:\>wevtutil gl <log name>” display?

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

**Answer: A**

#### NEW QUESTION 483

- (Exam Topic 3)

As a part of the investigation, Caroline, a forensic expert, was assigned the task to examine the transaction logs pertaining to a database named Transfers. She used SQL Server Management Studio to collect the active transaction log files of the database. Caroline wants to extract detailed information on the logs, including AllocUnitId, page id, slot id, etc. Which of the following commands does she need to execute in order to extract the desired information?

- A. DBCC LOG(Transfers, 1)
- B. DBCC LOG(Transfers, 3)
- C. DBCC LOG(Transfers, 0)
- D. DBCC LOG(Transfers, 2)

**Answer: D**

#### NEW QUESTION 484

- (Exam Topic 3)

Which of these ISO standards define the file system for optical storage media, such as CD-ROM and DVD-ROM?

- A. ISO 9660
- B. ISO 13346
- C. ISO 9960
- D. ISO 13490

**Answer: A**

#### NEW QUESTION 488

- (Exam Topic 3)

Identify the file system that uses \$BitMap file to keep track of all used and unused clusters on a volume.

- A. NTFS
- B. FAT
- C. EXT
- D. FAT32

**Answer: A**

#### NEW QUESTION 491

- (Exam Topic 3)

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

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

**Answer: C**

#### NEW QUESTION 495

- (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 497**

- (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 498

- (Exam Topic 3)

The Apache server saves diagnostic information and error messages that it encounters while processing requests. The default path of this file is `usr/local/apache/logs/error.log` in Linux. Identify the Apache error log from the following logs.

- A. <http://victim.com/scripts/..%c0%af../..%c0%af../..%c0%af../..%c0%af../..%c0%af../..%c0%af../..%c0%af../..%c0%af../winnt/system32/cmd.exe?/c+dir+C:\Winnt\system32\Logfiles\W3SVC1>  
B. [Wed Oct 11 14:32:52 2000] [error] [client 127.0.0.1] client denied by server configuration:/export/home/live/ap/htdocs/test  
C. 127.0.0.1 - frank [10/Oct/2000:13:55:36 -0700]"GET /apache\_pb.gif HTTP/1.0" 200 2326  
D. 127.0.0.1 - - [10/Apr/2007:10:39:11 +0300] ] [error] "GET /apache\_pb.gif HTTP/1.0" 200 2326

**Answer: B**

**NEW QUESTION 501**

- (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 506**

- (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 509**

- (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 512**

- (Exam Topic 3)

An attacker successfully gained access to a remote Windows system and plans to install persistent backdoors on it. Before that, to avoid getting detected in future, he wants to cover his tracks by disabling the last-accessed timestamps of the machine. What would he do to achieve this?

- A. Set the registry value of HKLM\SYSTEM\CurrentControlSet\Control\FileSystem\NtfsDisableLastAccessUpdate to 0  
B. Run the command fsutil behavior set disablelastaccess 0  
C. Set the registry value of HKLM\SYSTEM\CurrentControlSet\Control\FileSystem\NtfsDisableLastAccessUpdate to 1  
D. Run the command fsutil behavior set enablelastaccess 0

**Answer: C**

## NEW QUESTION 516

- (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 518

- (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 519

- (Exam Topic 2)

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

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

**Answer:** B

#### NEW QUESTION 522

- (Exam Topic 2)

To which phase of the Computer Forensics Investigation Process does the Planning and Budgeting of a Forensics Lab belong?

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

**Answer:** C

#### NEW QUESTION 523

- (Exam Topic 2)

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

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

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

**Answer:** C

#### NEW QUESTION 527

- (Exam Topic 2)

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

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

**Answer:** C



#### NEW QUESTION 528

- (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 530

- (Exam Topic 2)

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

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

**Answer: A**

#### NEW QUESTION 532

- (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 536

- (Exam Topic 2)

How will you categorize a cybercrime that took place within a CSP's cloud environment?

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

**Answer: D**

#### NEW QUESTION 540

- (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 545

- (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 546

- (Exam Topic 2)

Which program is the bootloader when Windows XP starts up?

- A. KERNEL.EXE
- B. NTLDR

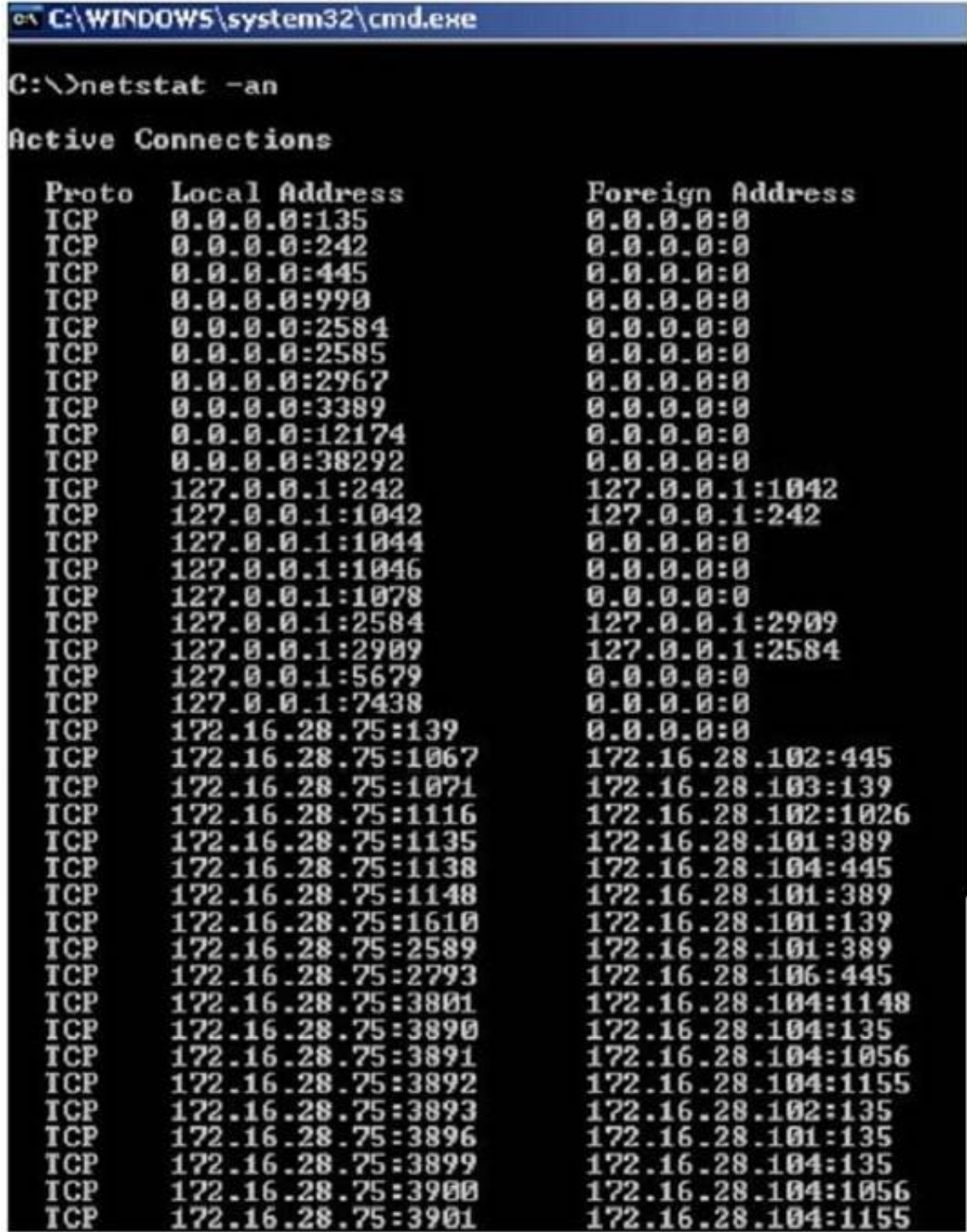
- C. LOADER
- D. LILO

Answer: B

NEW QUESTION 547

- (Exam Topic 2)

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



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

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

Answer: B

NEW QUESTION 551

- (Exam Topic 2)

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

Answer: B

NEW QUESTION 554

- (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 559

- (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 564

- (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=10.130.9.3 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=10.120.10.123 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=14937
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=70.185.198.247 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=10.120.10.123 src_port=48392 d
2007-06-14 23:59:09 192.168.254.1 action=Permit sent=12219 rcvd=140495 src=70.185.198.247 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=10.130.9.3 dst=224.0.0.2 src_port=49415 dst_port=49
2007-06-14 23:59:09 192.168.254.1 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 23:59:10 192.168.254.1 action=Permit sent=3018 rcvd=34134 src=70.185.198.247 dst=10.120.10.122 src_port=4480
2007-06-14 18:34:04 192.168.254.1 action=Permit sent=799 rcvd=6686 src=70.185.198.247 dst=10.120.10.122 src_port=46344
2007-06-14 18:34:05 192.168.254.1 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 18:34:07 192.168.254.1 action=Permit sent=2094 rcvd=23180 src=70.185.198.247 dst=10.120.10.122 src_port=4685
2007-06-14 18:34:09 192.168.254.1 action=Permit sent=2612 rcvd=68608 src=70.185.198.247 dst=10.120.10.122 src_port=4711
2007-06-14 18:34:11 192.168.254.1 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=70.185.198.247 dst=10.120.10.123 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=10.130.9.3 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=379
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=461 src=24.119.169.162 dst=10.120.10.123 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=10.130.9.3 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=10.130.9.3 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=10.130.9.3 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 568

- (Exam Topic 2)

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

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

**Answer: C**

#### NEW QUESTION 571

- (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 573

- (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 575**

- (Exam Topic 2)

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

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

**Answer:** A

**NEW QUESTION 578**

- (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 579**

- (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 583**

- (Exam Topic 2)

Which file is a sequence of bytes organized into blocks understandable by the system's linker?

- A. executable file
- B. source file
- C. Object file
- D. None of these

**Answer:** C

**NEW QUESTION 585**

- (Exam Topic 2)

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

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

**Answer:** D

**NEW QUESTION 588**

- (Exam Topic 2)

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

- A. Proxify.net
- B. Dnsstuff.com
- C. Samspace.org
- D. Archive.org

**Answer:** D

**NEW QUESTION 589**

- (Exam Topic 2)

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

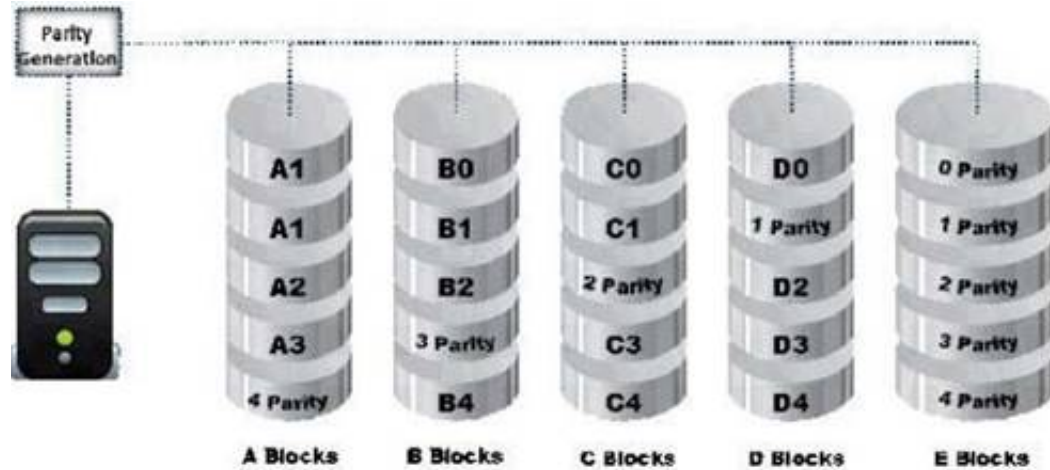
- A. Net sessions
- B. Net config
- C. Net share
- D. Net use

**Answer: D**

#### NEW QUESTION 592

- (Exam Topic 2)

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



What RAID level is represented here?

- A. RAID Level 0
- B. RAID Level 5
- C. RAID Level 3
- D. RAID Level 1

**Answer: B**

#### NEW QUESTION 596

- (Exam Topic 2)

Ivanovich, a forensics investigator, is trying to extract complete information about running processes from a system. Where should he look apart from the RAM and virtual memory?

- A. Swap space
- B. Application data
- C. Files and documents
- D. Slack space

**Answer: A**

#### NEW QUESTION 598

- (Exam Topic 2)

What method of copying should always be performed first before carrying out an investigation?

- A. Parity-bit copy
- B. Bit-stream copy
- C. MS-DOS disc copy
- D. System level copy

**Answer: B**

#### NEW QUESTION 599

- (Exam Topic 2)

Which of the following options will help users to enable or disable the last access time on a system running Windows 10 OS?

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

**Answer: C**

#### NEW QUESTION 602

- (Exam Topic 2)

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

- A. Searching for evidence themselves would not have any ill effects

- B. Searching could possibly crash the machine or device
- C. Searching creates cache files, which would hinder the investigation
- D. Searching can change date/time stamps

**Answer:** D

**NEW QUESTION 606**

- (Exam Topic 2)

What does the 63.78.199.4(161) denotes in a Cisco router log?

Mar 14 22:57:53.425 EST: %SEC-6-IPACCESSLOGP: list internet-inbound denied udp 66.56.16.77(1029) -> 63.78.199.4(161), 1 packet

- A. Destination IP address
- B. Source IP address
- C. Login IP address
- D. None of the above

**Answer:** A

**NEW QUESTION 607**

- (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 610**

- (Exam Topic 2)

Sectors are pie-shaped regions on a hard disk that store data. Which of the following parts of a hard disk do not contribute in determining the addresses of data?

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

**Answer:** B

**NEW QUESTION 614**

- (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 615**

- (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 619**

- (Exam Topic 2)

Which of the following data structures stores attributes of a process, as well as pointers to other attributes and data structures?

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

**Answer:** D

**NEW QUESTION 621**

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

**Answer:** D

#### NEW QUESTION 623

- (Exam Topic 2)

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

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

**Answer:** B

#### NEW QUESTION 626

- (Exam Topic 2)

In Steganalysis, which of the following describes a Known-stego attack?

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

**Answer:** C

#### NEW QUESTION 629

- (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 634

- (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 636

- (Exam Topic 2)

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

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

**Answer:** D

#### NEW QUESTION 639

- (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 643

- (Exam Topic 2)

What is the default IIS log location?

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

**Answer:** B

#### NEW QUESTION 644

- (Exam Topic 2)

What type of attack sends spoofed UDP packets (instead of ping packets) with a fake source address to the IP broadcast address of a large network?

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

**Answer:** A

#### NEW QUESTION 645

- (Exam Topic 2)

Paul is a computer forensics investigator working for Tyler & Company Consultants. Paul has been called upon to help investigate a computer hacking ring broken up by the local police. Paul begins to inventory the PCs found in the hackers hideout. Paul then comes across a PDA left by them that is attached to a number of different peripheral devices. What is the first step that Paul must take with the PDA to ensure the integrity of the investigation?

- A. Place PDA, including all devices, in an antistatic bag
- B. Unplug all connected devices
- C. Power off all devices if currently on
- D. Photograph and document the peripheral devices

**Answer:** D

#### NEW QUESTION 648

- (Exam Topic 2)

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

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

**Answer:** C

#### NEW QUESTION 649

- (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 654

- (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 655

- (Exam Topic 2)

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

```
#Software: Microsoft Internet Information Services 6.0
#version: 1.0
#date: 2007-01-22 15:42:36
#Fields: date time s-sitename s-ip cs-method cs-uri-stem cs-uri-query s-port cs-user
2007-01-22 15:42:36 w3svc1 172.16.28.102 GET /index.html - 80 - 172.16.28.80
Mozilla/4.0+(compatible;+MSIE+6.0;+windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 w3svc1 172.16.28.102 GET /Development/index.asp - 80 - 172.16.28
Mozilla/4.0+(compatible;+MSIE+6.0;+windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 w3svc1 172.16.28.102 GET /Development/css/olcstyle.css - 80 - 17
Mozilla/4.0+(compatible;+MSIE+6.0;+windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 w3svc1 172.16.28.102 GET /favicon.ico - 80 - 172.16.28.80 Avant+
2007-01-22 15:42:36 w3svc1 172.16.28.102 GET /Development/css/dhtml_horiz.css - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 w3svc1 172.16.28.102 GET /Development/images/index_01.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 w3svc1 172.16.28.102 GET /Development/images/index_02.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 w3svc1 172.16.28.102 GET /Development/images/index_03.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 w3svc1 172.16.28.102 GET /Development/images/index_04.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 w3svc1 172.16.28.102 GET /Development/images/index_06.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 w3svc1 172.16.28.102 GET /Development/images/index_07.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 w3svc1 172.16.28.102 GET /Development/images/index_08.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 w3svc1 172.16.28.102 GET /Development/script/dhtml.js - 80 - 172
Mozilla/4.0+(compatible;+MSIE+6.0;+windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 w3svc1 172.16.28.102 GET /Development/images/greenArraw.jpg - 80
Mozilla/4.0+(compatible;+MSIE+6.0;+windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 w3svc1 172.16.28.102 GET /Development/images/board_01.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 w3svc1 172.16.28.102 GET /Development/images/board_02.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 w3svc1 172.16.28.102 GET /Development/images/board_03.jpg - 80 -
```

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

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

**Answer: A**

#### NEW QUESTION 656

- (Exam Topic 2)

Where are files temporarily written in Unix when printing?

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

**Answer: D**

#### NEW QUESTION 659

- (Exam Topic 2)

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

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

**Answer: B**

#### NEW QUESTION 660

- (Exam Topic 2)

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

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

**Answer: C**

#### NEW QUESTION 662

- (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 667**

- (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 668**

- (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 670**

- (Exam Topic 2)

Madison is on trial for allegedly breaking into her university's internal network. The police raided her dorm room and seized all of her computer equipment.

Madison's lawyer is trying to convince the judge that the seizure was unfounded and baseless. Under which US Amendment is Madison's lawyer trying to prove the police violated?

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

**Answer:** A

**NEW QUESTION 675**

- (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 679**

- (Exam Topic 2)

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

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

**Answer:** D

**NEW QUESTION 681**

- (Exam Topic 2)

While looking through the IIS log file of a web server, you find the following entries:

```
2007-01-23 14:18:39 W3SVC1 172.16.28.102 GET /Development/index.asp
2007-01-23 14:18:39 W3SVC1 172.16.28.102 GET /login.asp?username=if {(select user)='sa' OR (select user)='dbo')}
select 1 else select 1/0
2007-01-23 14:18:39 W3SVC1 172.16.28.102 GET /Developments/index_02.jpg
2007-01-23 14:18:39 W3SVC1 172.16.28.102 GET /Development/index_04.jpg
```

What is evident from this log file?

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

**Answer:** D

**NEW QUESTION 684**

- (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 686**

- (Exam Topic 2)

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

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

**Answer: C**

**NEW QUESTION 687**

- (Exam Topic 2)

Using Linux to carry out a forensics investigation, what would the following command accomplish? `dd if=/usr/home/partition.image of=/dev/sdb2 bs=4096 conv=notrunc,noerror`

- A. Search for disk errors within an image file
- B. Backup a disk to an image file
- C. Copy a partition to an image file
- D. Restore a disk from an image file

**Answer: D**

**NEW QUESTION 688**

.....



## 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](#)**