312-49v8_formatted

Number: 000-000
Passing Score: 800
Time Limit: 120 min
File Version: 1.0

ECCouncil 312-49v8

ECCouncil Computer Hacking Forensic Investigator

mail : etest.tw@gmail.com

Exam A

QUESTION 1
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 2
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 3
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
Section: (none)

Explanation/Reference:

QUESTION 4
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 5
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 6
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
Section: (none)

Explanation/Reference:
Explanation:

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

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

Answer: A
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 8
Email archiving is a systematic approach to save and protect the data contained in emails so that it can tie easily accessed at a later date.

A. True
B. False

Answer: A
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 9
Which of the following commands shows you the NetBIOS name table each?

A. Option A
B. Option B
C. Option C
D. Option D

Answer: A
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 10
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 11
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 12
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 13
Network forensics allows Investigators 10 inspect network traffic and logs to identify and locate the attack system

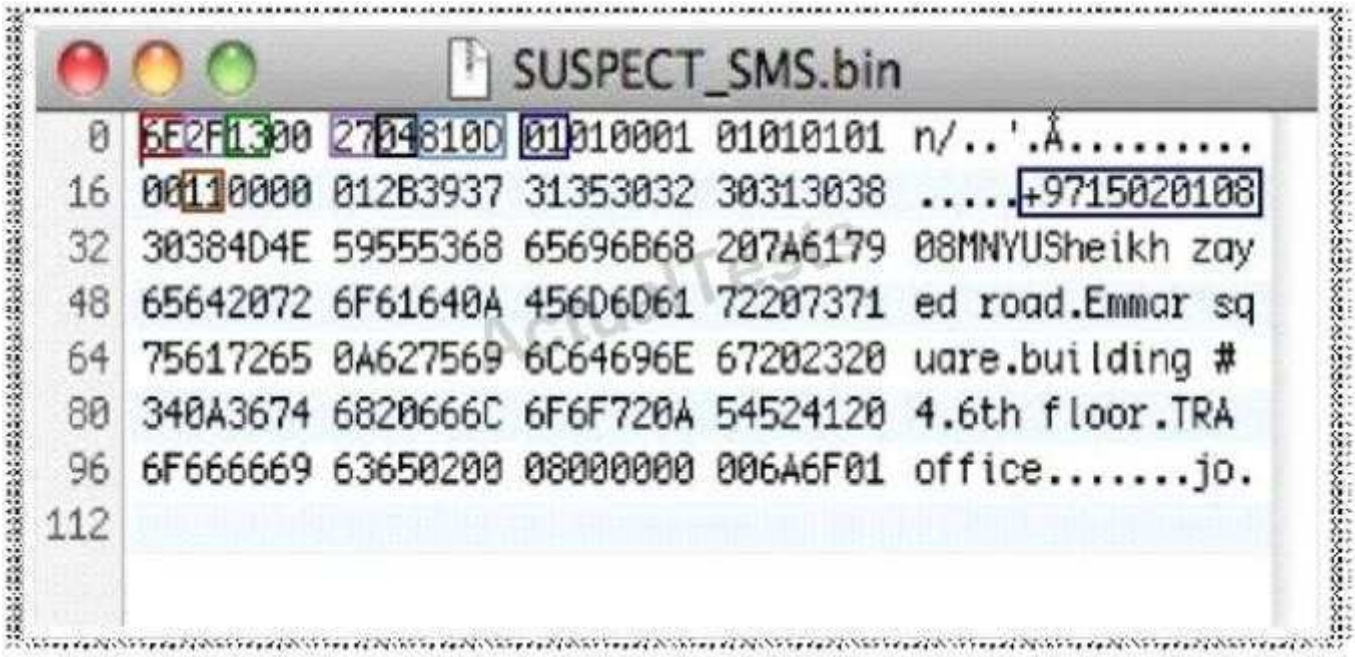
Network forensics can reveal: (Select three answers)

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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 14
Determine the message length from following hex viewer record:



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

Answer: D
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 15
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 16
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 17
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 18
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
Section: (none)

Explanation/Reference:

QUESTION 19
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 20
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 21
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
Section: (none)

Explanation/Reference:

QUESTION 22
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 23
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 24
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
Section: (none)

Explanation/Reference:

QUESTION 25
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 26
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 27

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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 28
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 29
During the seizure of digital evidence, the suspect can be allowed touch the computer system.

A. True
B. False

Answer: B
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 30
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 31
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 32
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 33
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 34
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. Option A
B. Option B
C. Option C
D. Option D

Answer: A
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 35
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 36
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 37

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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 38
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 39
Which Is a Linux journaling file system?

A. Ext3
B. HFS
C. FAT
D. BFS

Answer: A
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 40
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 41
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 42
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 43
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
Section: (none)

Explanation/Reference:

QUESTION 44
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 Z 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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 45
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. Verily 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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 46
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
Section: (none)

Explanation/Reference:

QUESTION 47
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 48
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 49
Data files from original evidence should be used for forensics analysis

A. True
B. False

Answer: B
Section: (none)

Explanation/Reference:

QUESTION 50
Attackers can manipulate variables that reference files with "dot-dot-slash (./)" sequences and their variations such as http://www.juggyDoy.corn/GET/process.php././././././././etc/passwd.

Identify the attack referred.

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

Answer: A
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 51
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
Section: (none)

Explanation/Reference:

QUESTION 52
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 53
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 54
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 55
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 56
P0P3 (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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 57
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 58
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 59
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 60
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 61
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 62
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 63
Recovery of the deleted partition is the process by which the investigator evaluates and extracts the deleted partitions.

A. True
B. False

Answer: A
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 64
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 65
Which one of the following is not a consideration in a forensic readiness planning checklist?

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

Answer: D
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 66
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
Section: (none)

Explanation/Reference:
Explanation:

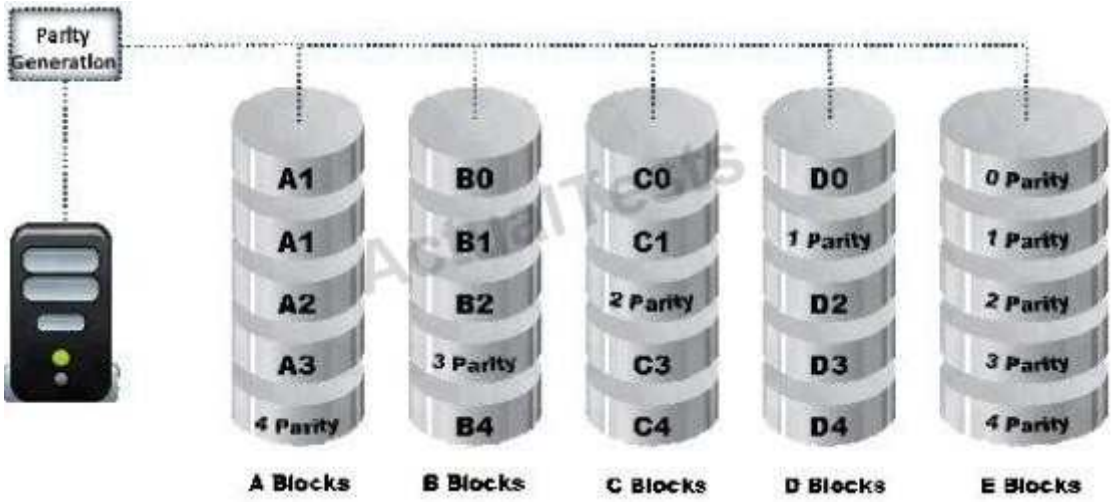
QUESTION 67
What is a chain of custody?

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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 68
Data is striped at a byte level across multiple drives and parity information is distributed among all member drives.



What RAID level is represented here?

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

Answer: D
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 69
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 70
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 71
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 72
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 73
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 74
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 75
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 76
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 77
Physical security recommendations: There should be only one entrance to a forensics lab

A. True
B. False

Answer: A
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 78
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 79
You should always work with original evidence

A. True
B. False

Answer: B
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 80
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 81
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 82
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 83
Digital evidence is not fragile in nature.

A. True
B. False

Answer: B
Section: (none)

Explanation/Reference:

QUESTION 84
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 85
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 86
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
Section: (none)

Explanation/Reference:

QUESTION 87
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 88
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 89
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 90
Depending upon the Jurisdictional areas, different laws apply to different incidents. Which of the following law is related to fraud and related activity in connection with computers?

A. 18 USC 7029
B. 18 USC 7030
C. 18 USC 7361
D. 18 USC 7371

Answer: B
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 91
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 92
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 93
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 94
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 95
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 96
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 97
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 98

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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 99
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 100
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
Section: (none)

Explanation/Reference:

QUESTION 101
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 102
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 103
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 104
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 105
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 106
Cyber-crime is defined as any Illegal act involving a gun, ammunition, or its applications.

A. True
B. False

Answer: B
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 107
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 108
A computer forensic report is a report which provides detailed information on the complete forensics investigation process.

A. True
B. False

Answer: A
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 109
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 110
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 111
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 112
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 113
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 114
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
Section: (none)

Explanation/Reference:

QUESTION 115
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 116
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 117
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 118
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 119
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 120
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 121
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 122
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
Section: (none)

Explanation/Reference:

QUESTION 123
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 124
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 125
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
Section: (none)

Explanation/Reference:

QUESTION 126
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 127
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 128
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 129
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 130
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 131
What is the smallest allocation unit of a hard disk?

A. Cluster
B. Spinning tracks
C. Disk platters
D. Slack space

Answer: A
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 132
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 133
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 134
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 2326
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./../winnt/system32/cmd.exe?/c+di r+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 2326

Answer: B
Section: (none)

Explanation/Reference:
Explanation:

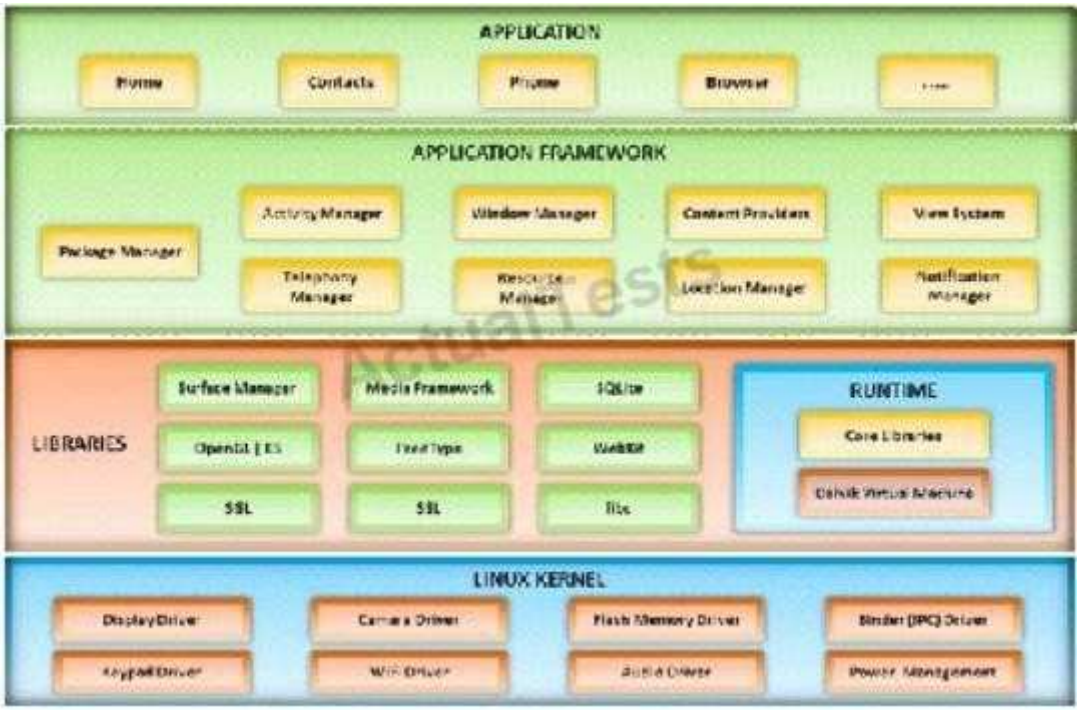
QUESTION 135
Operating System logs are most beneficial for Identifying or Investigating suspicious activities involving a particular host. Which of the following Operating System logs contains information about operational actions performed by OS components?

A. Event logs
B. Audit logs
C. Firewall logs
D. IDS logs

Answer: A
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 136
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 137
All the Information about the user activity on the network, like details about login and logoff attempts, is collected in the security log of the computer. When a user's login is successful, successful audits generate an entry whereas unsuccessful audits generate an entry for failed login attempts in the logon event ID table.

In the logon event ID table, which event ID entry (number) represents a successful logging on to a computer?

A. 528
B. 529
C. 530
D. 531

Answer: A
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 138
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 139
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 140
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
Section: (none)

Explanation/Reference:

QUESTION 141
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 142
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 143
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 disciple to deal with the legal processes

Answer: A
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 144
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 145
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 146
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 147
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 148
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 149
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 150
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 151
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
Section: (none)

Explanation/Reference:

QUESTION 152
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 153
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
Section: (none)

Explanation/Reference:

Explanation:

QUESTION 154
Mobile phone forensics is the science of recovering digital evidence from a mobile phone under forensically sound conditions.

A. True
B. False

Answer: A
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 155
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 156
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 157
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
Section: (none)

Explanation/Reference:
Explanation:

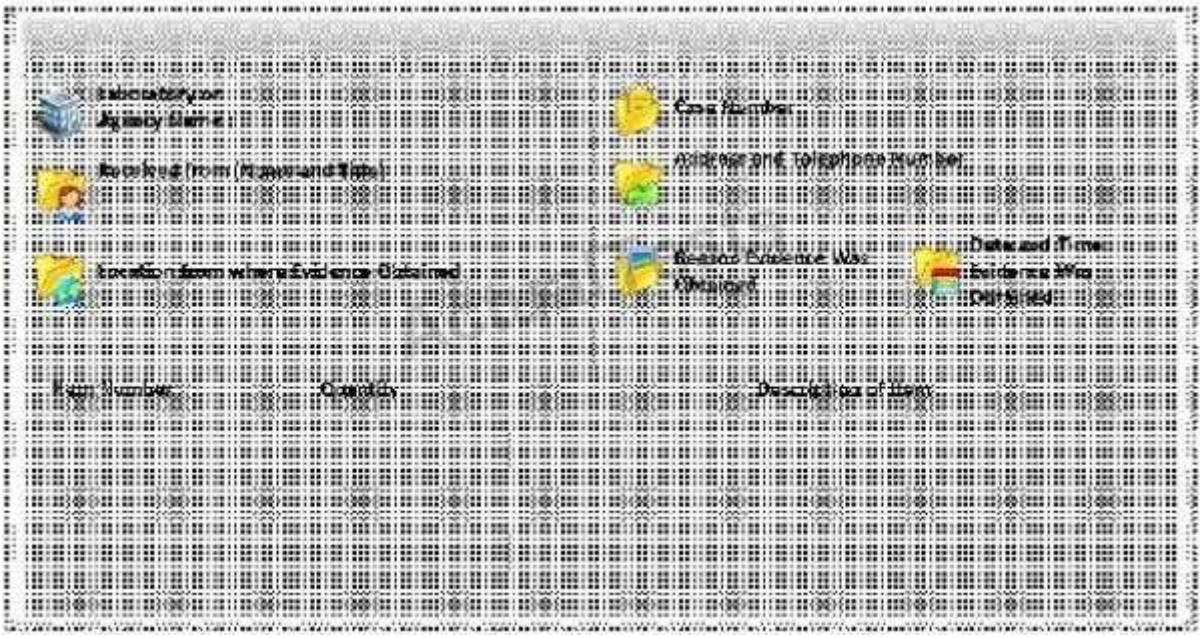
QUESTION 158
A forensic investigator is a person who handles the complete Investigation process, that is, the preservation, identification, extraction, and documentation of the evidence. The investigator has many roles and responsibilities relating to the cybercrime analysis. The role of the forensic 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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 159
What document does the screenshot represent?



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

Answer: A
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 160
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 161
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 162
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 Thunderoird
D. Eudora

Answer: B
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 163
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 164
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 165

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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 166
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 167
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 168

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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 169
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 170
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
Section: (none)

Explanation/Reference:

QUESTION 171
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 172
International Mobile Equipment Identifier (IMEI) is a 15-dlgit number that indicates the manufacturer, model type, and country of approval for GSM devices. The first eight digits of an IMEI number that provide information about the model and origin of the mobile device is also known as:

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

Answer: A
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 173
The IIS log file format is a fixed (cannot be customized) ASCII text-based format. The IIS format includes basic items, such as client IP address, user name, date and time, service and instance, server name and IP address, request type, target of operation, etc. Identify the service status code from the following IIS log.

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

A. W3SVC2
B. 4210
C. 3524

D. 100

Answer: D
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 174
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 175
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
Section: (none)

Explanation/Reference:

QUESTION 176
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 177
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 178
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 179
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
Section: (none)

Explanation/Reference:
Explanation:

QUESTION 180

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
Section: (none)

Explanation/Reference: