PassQueen
a.k.a dumpsqueen.com

Certified Cyber Intelligence Investigator ()

McAfee CCII

Version Demo

Total Demo Questions: 12

Total Premium Questions: 126

Buy Premium PDF

https://passqueen.com

support@passqueen.com

QUESTION NO: 1

A laptop is seized during an authorized investigation and transferred from the scene investigator to a forensic examiner. Select two entries that are essential to the chain-of-custody record for this transfer.

A. The identity of the person releasing and the person receiving the laptop.

B. The date, time, and purpose of the transfer.

C. A summary of the suspected offender's prior history.

D. The examiner's final opinion about the laptop's contents.

E. A list of unrelated evidence held in other cases.

ANSWER: A B

Explanation:

A chain-of-custody record must identify the evidence item and document the transfer of control. The record should include the persons releasing and receiving the device, the date and time of transfer, and the reason or purpose for the transfer. These details help demonstrate continuous accountability for the item.

A general description of the suspected offense does not establish custody. An examiner's eventual opinion belongs in an examination report, not as a substitute for recording the transfer itself.

QUESTION NO: 2

An analyst is preparing a report concerning a possible relationship between two online identities. Select three statements that appropriately communicate an analytic assessment.

A. State which observations are verified facts and which are analytical judgments.

B. Identify the indicators that support the assessed relationship.

C. Describe relevant limitations and the confidence of the assessment.

D. Present the relationship as confirmed because the identities share one username.

E. Remove source limitations so the assessment appears more decisive.

ANSWER: A B C

Explanation:

A sound assessment distinguishes established facts from analytical judgments, identifies the evidence supporting a conclusion, and states limitations or confidence where attribution remains incomplete. These practices allow a decision maker to understand both the value and the uncertainty of the intelligence.

Describing an unverified association as fact overstates the evidence. Omitting source limitations and presenting conclusions without supporting indicators makes the assessment less defensible and more difficult to review or corroborate.

QUESTION NO: 3

What resources can aid in social network investigations?

A. Data mining

B. Profile information

C. User demographics

D. Google

E. Social media monitoring services

ANSWER: A B C D E

Explanation:

Social-network investigations benefit from combining collection, enrichment, analysis, and corroboration resources. Data mining supports the discovery of meaningful patterns, relationships, repeated identifiers, and behavioral signals within large volumes of publicly available social content. Profile information supplies directly observable investigative leads, such as stated affiliations, locations, interests, account names, and posted material. User demographics provide context for assessing an account's claimed or likely audience, community, geography, and behavioral trends, while avoiding assumptions that are not supported by evidence. Google is useful for open-source research because investigators can search for usernames, quoted text, images, domains, and other indicators beyond the original social platform to identify corroborating public sources. Social media monitoring services can assist by aggregating public posts, tracking keywords or entities over time, and helping analysts identify relevant conversations or emerging activity at scale. These resources should be used together: collected information is preserved, evaluated for reliability, and corroborated before it is treated as intelligence. NIST's guidance on cyber threat information sharing emphasizes the importance of contextualizing and analyzing information before operational use, an approach that also applies to social-network-derived intelligence. See NIST SP 800-150 and the CISA information-sharing guidance.

QUESTION NO: 4

A governmental investigator prepares a preservation request to a communications provider for records connected to a suspected online fraud account. Select three details that should be included to make the request sufficiently useful and appropriately scoped.

A. The relevant account identifier, username, or email address

B. A defined date and time range for the requested preservation

C. The categories of records or evidence to be preserved

D. A demand that the provider retain all customer data permanently

E. A request for immediate disclosure without further legal authority

F. A general instruction to preserve anything related to internet fraud

ANSWER: A B C

Explanation:

A useful preservation request identifies the account or other specific identifier, defines the relevant time period, and identifies the records or evidence to be preserved. These details enable the provider to locate the material and reduce the risk of an unnecessarily broad request. The request should not demand a permanent retention period without basis, and a preservation request is not a substitute for the legal process needed to disclose protected records. A vague request for everything connected to fraud is not adequately tied to the identified investigation.

QUESTION NO: 5

A victim reports paying for electronics advertised through an online marketplace, but no goods arrived. Select two items of evidence that most directly establish the suspected non-delivery scheme.

A. Payment records showing funds sent to the seller or designated account

B. The listing and messages stating the item, price, and delivery terms

C. A screen capture of the marketplace home page

D. The victim's later purchase of similar goods from another seller

E. The seller's overall public feedback score

ANSWER: A B

Explanation:

The payment record establishes that the victim sent funds, while the listing and related communications establish what was promised, by whom, and under what delivery terms. These items directly support the essential sequence of offer, payment, and expected delivery. A general screen capture of the marketplace home page does not identify the transaction, and the victim's later purchase from another seller is unrelated. A seller's public feedback may be useful intelligence, but it does not establish the reported transaction as directly as the payment and communications evidence.

QUESTION NO: 6

Which of the following are types of Trojans?

A. Remote Access Trojans

B. Password Sending Trojans

C. Keyloggers

D. Destructive Trojans

E. Denial of Service (DoS) Attack Trojans

F. All of the Above

ANSWER: F

Explanation:

All of the Above is correct because each listed item describes a recognized Trojan category or capability. A Trojan is malware that masquerades as legitimate or desirable software in order to induce a user to run it. Once executed, its payload can provide an attacker with remote control of the affected device, collect and transmit passwords, record keystrokes, destroy data, or participate in denial-of-service activity. These categories are commonly used in malware education and incident investigation to distinguish Trojans by their primary objective and behavior. Remote-access functionality is particularly significant because it can enable command execution, surveillance, file access, and further deployment of malware. Credential theft and keylogging support account compromise, while destructive and denial-of-service payloads affect data availability and system or network operations. A single Trojan can also combine several of these functions, so classifications describe behavior rather than requiring mutually exclusive malware families. The Cybersecurity and Infrastructure Security Agency explains that Trojans use deception to get users to install malicious software and can enable unauthorized access or harmful actions. MITRE ATT&CK also documents adversary techniques for input capture, including keylogging, and for collecting credentials. See CISA's malware overview and MITRE ATT&CK: Keylogging.

QUESTION NO: 7

Ethical hacking is where a person hacks to find weaknesses in a system and then usually patches them.

A. True

B. False

ANSWER: A

Explanation:

“True” is correct because ethical hacking is an authorized security-testing activity performed to identify weaknesses before they can be exploited maliciously. An ethical hacker works with the system owner’s explicit permission and defined scope, using techniques that may resemble those of an attacker to assess networks, applications, hosts, configurations, and human-facing controls. The key purpose is risk reduction: discovered vulnerabilities are documented clearly, their potential impact is evaluated, and actionable remediation guidance is supplied so the organization can correct the weaknesses. Although the ethical hacker may not personally install every patch, ethical-hacking engagements commonly lead to patching, configuration hardening, access-control improvements, and validation testing after remediation. This makes the statement’s use of “usually patches them” appropriate as a high-level description of the process. Ethical hacking is therefore a structured, lawful practice that helps an organization improve its defensive posture rather than compromise systems for unauthorized gain. The National Institute of Standards and Technology describes penetration testing as security testing that simulates attacks to identify vulnerabilities and assess security controls. Guidance from the Cybersecurity and Infrastructure Security Agency likewise emphasizes vulnerability management and remediation as core protective activities. See NIST SP 800-115: Technical Guide to Information Security Testing and Assessment and CISA Vulnerability Management.

QUESTION NO: 8

How is a privacy policy used in social networks?

A. To protect members' information

B. To set guidelines on how information will be shared

C. All of the above

ANSWER: C

Explanation:

All of the above is correct because a social-network privacy policy serves both of the purposes stated. It is a public notice that describes how the service handles personal information supplied by members or generated through their activity, such as profile details, messages, device data, contacts, and usage information. A meaningful policy explains the organization’s practices intended to safeguard that information, including the general controls, access restrictions, retention practices, and security processes used to reduce unauthorized disclosure or misuse.

It also establishes and communicates the rules governing disclosure and sharing. Social networks commonly use privacy policies to tell members when data may be shared with other users, vendors that provide services for the platform, advertising and measurement partners, affiliated companies, researchers, law enforcement, or other parties when legally required. These disclosures help individuals understand the choices and privacy settings available to them and make informed decisions about their participation.

For example, the U.S. Federal Trade Commission emphasizes that privacy representations must accurately describe an organization’s collection, use, sharing, and protection of consumer data. Meta’s published privacy policy similarly describes categories of information it collects, how it uses that information, and the recipients with whom information may be shared. See the FTC Privacy and Security guidance and Meta Privacy Policy.

QUESTION NO: 9

An investigator receives an image file from a victim's email account and believes it may be important evidence. Select two actions that best preserve the image for later examination.

A. Retain the original received file in controlled storage.

B. Calculate and record a cryptographic hash of the original file.

C. Open the file in an editor and save it again before examination.

D. Keep only a screenshot because it shows the visible image content.

E. Delete the source email after copying the image attachment.

ANSWER: A B

Explanation:

The original received file should be retained in controlled storage, and a cryptographic hash should be calculated and recorded for the original file where feasible. These actions support later verification that the examined file is the same file that was acquired. The investigator should also preserve the email or other source record that establishes how the image was received.

Opening and saving the image through an editor can alter metadata or create a derivative file. A screenshot is useful for presentation but is not a substitute for retaining the original file and its available metadata.

QUESTION NO: 10

You can often pull metadata from images on social media sites.

A. True

B. False

ANSWER: A

Explanation:

True is correct because images shared through social-media platforms can contain or be associated with useful metadata that supports cyber-intelligence investigations. Depending on the platform, its processing settings, and whether investigators can obtain the original uploaded file, this information may include embedded EXIF/IPTC/XMP fields such as creation time, device make and model, software used to edit the file, captions, copyright information, and sometimes location data. Even when a platform removes some embedded EXIF fields from the displayed derivative image, an investigator may find useful metadata in an original download, an attachment, a linked image host, platform-provided details, or a reposted copy that underwent different processing. Metadata should therefore be collected and examined early, while preserving the source URL, download method, timestamps, and file hash so that findings can be reproduced and properly attributed. ExifTool is widely used to inspect embedded image metadata and documents the supported metadata families at https://exiftool.org/. Flickr also documents that photo metadata can be displayed and managed with a photo, illustrating that social-image services may retain and expose metadata: https://www.flickrhelp.com/hc/en-us/articles/4404064113812-Edit-photo-metadata.

QUESTION NO: 11

What is the general modus operandi for thieves selling & transporting stolen goods?

A. Many thieves had around 20-30 people and retail outlets where they felt they could "safely" sell stolen goods.

B. Fences liked to sell goods out of their houses.

C. Boosters are the best at selling counterfeit goods.

ANSWER: A

Explanation:

Many thieves had around 20-30 people and retail outlets where they felt they could "safely" sell stolen goods. This reflects the networked structure commonly associated with organized retail crime. Rather than acting solely as isolated shoplifters, these groups may divide responsibilities among individuals who obtain merchandise, coordinate its movement and storage, identify resale channels, and handle the proceeds. A seemingly legitimate retail outlet can provide a plausible setting in which stolen merchandise is blended with lawful inventory and resold with less immediate scrutiny. Group size and exact roles differ by operation, but the central modus operandi is organized acquisition followed by distribution through established resale networks. This structure enables repeated thefts, rapid movement of goods, and resale at a scale that would be difficult for an individual offender to sustain. The U.S. Department of Homeland Security describes organized retail crime as coordinated criminal activity involving the theft and resale of merchandise, while the Department of Justice identifies

organized retail theft as a significant, networked criminal concern. These sources support recognizing coordinated groups and resale outlets as characteristic features of this type of stolen-goods operation. See DHS: Organized Retail Crime and U.S. Department of Justice: Organized Retail Crime.

QUESTION NO: 12

An investigator identifies a private social-media account that may contain evidence relevant to an extortion complaint. The account holder has not consented to access, and the investigator has no legal process authorizing disclosure. What is the best immediate action?

A. Preserve public evidence and seek appropriate authority for non-public account material.

B. Use a third party's credentials to review the private account.

C. Create a deceptive account to obtain access to the private content.

D. Assume that a private profile can be accessed because it relates to a complaint.

ANSWER: A

Explanation:

The correct answer is to preserve the publicly available evidence and pursue the appropriate legal or organizational process for non-public account material. Private content is protected by access controls, and an investigator should not bypass those controls, use another person's credentials, or attempt to obtain access through deception without proper authority.

Preserving public posts, account URLs, usernames, and timestamps protects potentially volatile evidence while the investigator determines the correct process for obtaining restricted records. A preservation request may also be appropriate when records held by a provider could be subject to deletion, but preservation does not itself authorize disclosure.