DUMPSBOSS.

Certified Cybersecurity Technician (CCT)

ECCouncil 212-82

Version Demo

Total Demo Questions: 19

Total Premium Questions: 190

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, Information Security Fundamentals	53
Topic 2, Networking Fundamentals	11
Topic 3, Security Operations	19
Topic 4, Application Security	9
Topic 5, Network Security	32
Topic 6, Endpoint Security	8
Topic 7, Cloud Security	8
Topic 8, Penetration Testing	18
Topic 9, Digital Forensics	23
Topic 10, Incident Response	9
Total	190

QUESTION NO: 1

Marcus, a security architect, was instructed to adopt a Zero Trust security model for the organization's hybrid environment. The organization wants to reduce implicit trust for users, devices, applications, and network locations.

Which of the following principles should Marcus apply? (Choose three.)

A. Verify explicitly

B. Use least-privilege access

C. Assume breach

D. Trust devices on the internal network by default

E. Grant permanent administrator permissions to remote users

ANSWER: A B C

Explanation:

Explicit verification requires access decisions to use all available relevant signals, such as user identity, device condition, location, and workload context. **Least-privilege access** limits users and processes to only the permissions required for authorized tasks. **Assuming breach** encourages segmentation, continuous monitoring, and limiting the blast radius of a possible compromise.

Automatically trusting a device because it is on the internal network contradicts Zero Trust principles. Permanent broad permissions also increase risk and are inconsistent with least privilege. NIST explains Zero Trust architecture and its core concepts in NIST SP 800-207.

QUESTION NO: 2

As the director of cybersecurity for a prominent financial Institution, you oversee the security protocols for a vast array of digital operations. The institution recently transitioned to a new core banking platform that integrates an artificial intelligence (AI)-based fraud detection system. This system monitors real-time transactions, leveraging pattern recognition and behavioral analytics.

A week post-transition, you are alerted to abnormal behavior patterns in the AI system. On closer examination, the system is mistakenly flagging genuine transactions as fraudulent, causing a surge in false positives. This not only disrupts the customers' banking experience but also strains the manual review team. Preliminary investigations suggest subtle data poisoning attacks aiming to compromise the AI's training data, skewing its decision-making ability. To safeguard the AI-based fraud detection system and maintain the integrity of your financial data, which of the following steps should be your primary focus?

A. Collaborate with the AI development team to retrain the model using only verified transaction data and implement real time monitoring to detect data poisoning attempts.

B. Migrate back to the legacy banking platform until the new system is thoroughly vetted and all potential vulnerabilities are addressed.

C. Liaise with third-party cybersecurity firms to conduct an exhaustive penetration test on the entire core banking platform, focusing on potential data breach points.

D. Engage in extensive customer outreach programs, urging them to report any discrepancies in their transaction records, and manually verifying flagged transactions.

ANSWER: A

Explanation:

Collaborate with the AI development team to retrain the model using only verified transaction data and implement real time monitoring to detect data poisoning attempts. This directly addresses the suspected attack mechanism: data poisoning degrades a model by introducing manipulated, mislabeled, or otherwise untrustworthy data into its training or feedback

pipeline. Before retraining, the institution should preserve relevant evidence, identify the affected datasets and ingestion paths, validate data provenance and labels, and exclude untrusted records. Retraining with verified, representative transaction data restores the fraud model's decision boundary based on trustworthy evidence, helping reduce erroneous fraud alerts while maintaining detection capability.

Ongoing monitoring is equally important because fraud-detection systems commonly receive fresh transaction and outcome data. Controls should therefore monitor data-quality distributions, label integrity, unusual shifts in feature values, training-data provenance, and changes in false-positive rates. Alerts and review workflows enable the security and machine-learning teams to investigate suspicious changes before contaminated data is promoted into a production model. NIST's AI Risk Management Framework emphasizes managing AI risks throughout the system lifecycle, while NIST's adversarial-machine-learning guidance specifically identifies poisoning as a threat requiring appropriate mitigations. See the NIST AI Risk Management Framework and NIST Adversarial Machine Learning guidance.

QUESTION NO: 3

Steve, a network engineer, was tasked with troubleshooting a network issue that is causing unexpected packet drops. For this purpose, he employed a network troubleshooting utility to capture the ICMP echo request packets sent to the server. He identified that certain packets are dropped at the gateway due to poor network connection.

Identify the network troubleshooting utility employed by Steve in the above scenario.

A. dnsenurn

B. arp

C. traceroute

D. ipconfig

ANSWER: C

Explanation:

traceroute is the appropriate utility because it traces the path that traffic follows from a source system to a destination and reports the intermediate routing devices, including a gateway at which loss or nonresponse is observed. It works by sending probe packets with progressively increasing Time To Live values. Each router that expires a probe's TTL returns a response, allowing the tool to identify that hop and measure the round-trip time. Implementations can use ICMP-based probes; notably, Windows `tracert` sends ICMP Echo Request messages, which matches the scenario's reference to ICMP echo requests. Repeated probes at each hop make it possible to recognize intermittent loss or connectivity degradation associated with a particular gateway, rather than merely confirming that the final server is reachable. This hop-by-hop visibility is why traceroute is a standard diagnostic utility when unexpected packet drops are suspected along a network path. The Linux traceroute documentation describes its TTL-based route-discovery behavior at man7.org traceroute manual, and Microsoft documents the ICMP Echo Request behavior of `tracert` at Microsoft Learn: tracert.

QUESTION NO: 4

Ryleigh, a system administrator, was instructed to perform a full back up of organizational data on a regular basis. For this purpose, she used a backup technique on a fixed date when the employees are not accessing the system i.e., when a service-level down time is allowed a full backup is taken.

Identify the backup technique utilized by Ryleigh in the above scenario.

A. Nearline backup

B. Cold backup

C. Hot backup

D. Warm backup

ANSWER: B

Explanation:

Cold backup is the appropriate technique because it is performed while the relevant system, application, or database is offline and users are not accessing it. In this scenario, Ryleigh schedules a full backup for a fixed maintenance period in which service-level downtime is permitted. Taking the backup during that inactive window helps ensure that the backed-up data is in a stable, internally consistent state, since no active user transactions or updates are being written while the copy is made. This approach is commonly used when an organization can tolerate a planned interruption and wants a straightforward full backup process without needing the application to remain available during the operation. Scheduled downtime also allows administrators to coordinate the backup with maintenance controls, verify successful completion, and reduce the likelihood of capturing partially completed changes. NIST describes backups as copies of data maintained to enable restoration following loss or corruption and emphasizes establishing procedures appropriate to operational requirements. Oracle documentation likewise describes offline backups as backups made after the database has been shut down, which reflects the defining characteristic of a cold backup. See NIST SP 800-34 Rev. 1 and Oracle Database Backup and Recovery User's Guide.

QUESTION NO: 5

Adeline, a physical security manager, was instructed to strengthen protection for the organization's data center. She must implement controls that restrict unauthorized entry, record access activity, and allow security personnel to observe activity around the facility.

Which of the following controls should Adeline implement? (Choose three.)

A. Mantrap

B. Access-control logs

C. Closed-circuit television (CCTV)

D. Public visitor Wi-Fi

E. Unescorted visitor badges

ANSWER: A B C

Explanation:

A **mantrap** restricts entry by requiring an individual to pass through two interlocking doors, helping prevent tailgating and piggybacking. **Access-control logs** provide a record of badge, biometric, or other access attempts that can be reviewed during investigations. **Closed-circuit television (CCTV)** enables security personnel to observe and record activity around entrances and sensitive areas.

These controls work together as preventive and detective safeguards for a data center. A visitor badge alone does not necessarily prevent unauthorized access unless it is tied to authorization and monitored access procedures. NIST describes physical access controls and monitoring requirements in NIST SP 800-53 Rev. 5.

QUESTION NO: 6

Mark, a security analyst, was tasked with performing threat hunting to detect imminent threats in an organization's network. He generated a hypothesis based on the observations in the initial step and started the threat hunting process using existing data collected from DNS and proxy logs.

Identify the type of threat hunting method employed by Mark in the above scenario.

A. Entity-driven hunting

B. TTP-driven hunting

C. Data-driven hunting

D. Hybrid hunting

ANSWER: C

Explanation:

Data-driven hunting is correct because the investigation begins with telemetry that the organization has already collected: DNS and proxy logs. This hunting approach uses available security data sources to identify suspicious patterns, anomalies, indicators, and relationships that may support or refine an initial hypothesis. DNS records can reveal suspicious lookups, newly observed domains, tunneling-like query patterns, or command-and-control infrastructure. Proxy logs add web-request, destination, user, device, and traffic context that helps an analyst investigate potentially malicious communications. The hypothesis gives the activity a focused investigative direction, while the existing log data is the primary basis for discovering and validating evidence of a threat. This aligns with established threat-hunting practice, in which analysts query and correlate endpoint, network, identity, and other telemetry to proactively uncover adversary activity that may not have generated an alert. MITRE describes the use of data sources and telemetry for detecting adversary techniques in its Data Sources knowledge base. Microsoft also describes proactive hunting as using collected data to investigate hypotheses through queries and analysis in its advanced hunting overview.

QUESTION NO: 7

The IH&R team in an organization was handling a recent malware attack on one of the hosts connected to the organization's network. Edwin, a member of the IH&R team, was involved in reinstating lost data from the backup media. Before performing this step, Edwin ensured that the backup does not have any traces of malware.

Identify the IH&R step performed by Edwin in the above scenario.

A. Eradication

B. Incident containment

C. Notification

D. Recovery

ANSWER: D

Explanation:

Recovery is the correct incident handling and response step because Edwin is restoring lost data from backup media after a malware incident. Recovery focuses on safely returning affected systems, services, and information to normal operation after the threat has been contained and removed. A critical recovery activity is validating that restoration sources, including backups, are clean and trustworthy before they are used. Restoring from an infected backup could reintroduce the malware, undo remediation work, and create a recurring incident. By checking that the backup contains no traces of malware before reinstating the lost data, Edwin is applying a core recovery safeguard: restore only verified, uncompromised data to the environment. Recovery also commonly includes validating the restored system's integrity and functionality, applying necessary security updates or configuration corrections, and monitoring for signs that the incident reappears. This activity aligns with NIST incident-response guidance, which identifies recovery as the phase in which organizations restore systems and data and confirm normal operations can resume safely. See the NIST SP 800-61 Rev. 2 Computer Security Incident Handling Guide and the CISA Incident Response guidance.

QUESTION NO: 8

Harper, a forensic officer, collected a laptop as evidence during an internal investigation. She must preserve a defensible chain of custody from collection through examination and reporting.

Which of the following activities should Harper perform to maintain the chain of custody? (Choose three.)

A. Record the date, time, location, and person who collected the evidence

B. Document every transfer between authorized individuals

C. Store the evidence in a secured location with restricted access

D. Use the original laptop for routine analysis

E. Leave the evidence unattended in an open work area

ANSWER: A B C

Explanation:

Harper should **record the date, time, location, and person who collected the evidence**, **document every transfer of the evidence between authorized individuals**, and **store the evidence in a secured location with restricted access**. These actions establish who possessed the item, when possession changed, where it was maintained, and how it was protected from unauthorized access or alteration. Complete custody records support the credibility and authenticity of the evidence during an investigation or legal proceeding.

Using the original laptop for routine analysis risks changing data and damaging evidentiary integrity. A forensic examiner should normally create and validate a forensic image, then perform examination on the copy while preserving the original. Leaving the evidence unattended in an open location also breaks physical security and makes the custody history difficult to defend. See NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response and the NIJ Electronic Crime Scene Investigation guide.

QUESTION NO: 9

Grace, an online shopping enthusiast, purchased a smart TV using her debit card. During online payment. Grace's browser redirected her from the e-commerce website to a third-party payment gateway, where she provided her debit card details and the OTP received on her registered mobile phone. After completing the transaction, Grace logged Into her online bank account and verified the current balance in her savings account, identify the state of data being processed between the e-commerce website and payment gateway in the above scenario.

A. Data in inactive

B. Data in transit

C. Data in use

D. Data at rest

ANSWER: B

Explanation:

Data in transit is correct because the payment-related information is being communicated across a network between separate systems: the e-commerce site, Grace’s browser, and the payment gateway. Information such as card details, transaction identifiers, authorization requests, and payment responses is in motion while it travels through internet connections and supporting network infrastructure. This state is commonly called data in transit, or data in motion.

Protecting this data state is essential for online purchases because payment information must remain confidential and resistant to alteration while it is transmitted. Secure web connections using Transport Layer Security protect communications between the browser and web services, helping provide encryption, integrity protection, and server authentication. Payment workflows also commonly use additional controls, including authenticated application programming interfaces, tokenization, and secure session handling, to reduce exposure of sensitive account data during transfer. The National Institute of Standards and Technology describes cryptographic mechanisms for protecting sensitive information during communications in its guidance on transport-layer security, available through NIST SP 800-52 Revision 2. The PCI Security Standards Council likewise identifies protection of cardholder data transmitted over open, public networks as a core security requirement: PCI DSS document library.

QUESTION NO: 10

Shawn, a forensic officer, was appointed to investigate a crime scene that had occurred at a coffee shop. As a part of investigation, Shawn collected the mobile device from the victim, which may contain potential evidence to identify the culprits.

Which of the following points must Shawn follow while preserving the digital evidence? (Choose three.)

A. Never record the screen display of the device

B. Turn the device ON if it is OFF

C. Do not leave the device as it is if it is ON

D. Make sure that the device is charged

E. Immediately isolate the device from cellular, Wi-Fi, Bluetooth, and other networks.

F. Document and photograph the device, including its screen display and physical condition.

ANSWER: D E F

Explanation:

Mobile-device evidence preservation focuses on preventing alteration, loss of volatile data, remote access, and remote wiping while maintaining a defensible record of the device's condition. "Make sure that the device is charged" is appropriate because an unexpected loss of power can change the device's state and may make access to volatile evidence more difficult. Investigators should use an appropriate power source while avoiding unnecessary interaction with the device. "Immediately isolate the device from cellular, Wi-Fi, Bluetooth, and other networks" protects evidence from remote commands, synchronization, deletion, or modification. Isolation should be performed in a way that preserves the device's current state, such as placing it in a suitable radio-frequency-shielding container when appropriate. "Document and photograph the device, including its screen display and physical condition" establishes the initial condition of the evidence and supports chain-of-custody records. Documentation should capture visible notifications, time, battery level, network indicators, damage, and identifying details before further forensic handling. These practices align with the general forensic principle of preserving evidence integrity and maintaining complete documentation. See the NIST Guide to Mobile Device Forensics and NIJ Electronic Crime Scene Investigation guide.

QUESTION NO: 11

Kason, a forensic officer, was appointed to investigate a case where a threat actor has bullied certain children online. Before proceeding legally with the case, Kason has documented all the supporting documents, including source of the evidence and its relevance to the case, before presenting it in front of the jury.

Which of the following rules of evidence was discussed in the above scenario?

A. Authentic

B. Understandable

C. Reliable

D. Admissible

ANSWER: D

Explanation:

Admissible is correct because the scenario focuses on preparing evidence for legal presentation by documenting its source and explaining its relevance to the case. Admissibility is the threshold concept governing whether evidence may be presented to a judge or jury. For digital forensic material, the investigator must be able to show that the material bears on a fact that matters in the case and that there is an adequate foundation for introducing it in court. Recording where the evidence came from, how it was obtained, and why it is connected to the alleged online bullying helps establish that foundation and supports its use during legal proceedings.

In particular, relevance is a core requirement for admissibility: evidence must tend to make a consequential fact more or less probable. The documented source also supports the foundation needed to introduce digital evidence properly. These requirements are reflected in Rule 401 and Rule 901 of the U.S. Federal Rules of Evidence, which address relevance and authentication of evidence. See Federal Rule of Evidence 401 and Federal Rule of Evidence 901.

QUESTION NO: 12

Chase, a DevSecOps engineer, was instructed to improve the security of containerized applications deployed by the organization. He must reduce the attack surface of containers and prevent applications from receiving unnecessary privileges.

Which of the following measures should Chase implement? (Choose three.)

A. Use minimal trusted base images

B. Run containers as a non-root user

C. Scan images for known vulnerabilities

D. Run every container in privileged mode

E. Store production passwords inside container images

ANSWER: A B C

Explanation:

Using **minimal trusted base images** reduces unnecessary packages and services that may contain vulnerabilities. Running containers as a **non-root user** limits the privileges available to a compromised application. Scanning container images for **known vulnerabilities** helps identify insecure dependencies and operating-system packages before deployment.

Using privileged containers unnecessarily weakens isolation and can expose host resources. Embedding passwords or API keys in container images creates a risk because images can be copied, inspected, and retained in registries. Docker provides container-security guidance in its Docker Engine security documentation, and NIST discusses container security in NIST SP 800-190.

QUESTION NO: 13

Elijah, an email security administrator, was instructed to reduce the risk of domain spoofing and fraudulent messages sent using the organization's domain name. He plans to implement email-authentication technologies that enable receiving mail servers to validate authorized senders and apply a policy when authentication checks fail.

Which of the following technologies should Elijah implement? (Choose three.)

A. Sender Policy Framework (SPF)

B. DomainKeys Identified Mail (DKIM)

C. Domain-based Message Authentication, Reporting, and Conformance (DMARC)

D. Transport Layer Security (TLS)

E. Post Office Protocol version 3 (POP3)

ANSWER: A B C

Explanation:

SPF, **DKIM**, and **DMARC** are the appropriate email-authentication technologies. Sender Policy Framework (SPF) publishes authorized sending hosts for a domain in DNS. DomainKeys Identified Mail (DKIM) adds a cryptographic signature that a receiving server can validate using the public key published in DNS. Domain-based Message Authentication, Reporting, and

Conformance (DMARC) uses SPF and DKIM alignment and allows the domain owner to publish a policy such as none, quarantine, or reject for messages that fail validation.

TLS protects the confidentiality and integrity of an email transport connection when supported by both communicating servers, but it does not establish whether a sender is authorized to use a particular domain. POP3 is a mail-retrieval protocol and does not provide domain-spoofing protection. See RFC 7208: Sender Policy Framework, RFC 6376: DKIM Signatures, and RFC 7489: DMARC.

QUESTION NO: 14

Arabella, a forensic officer, documented all the evidence related to the case in a standard forensic investigation report template. She filled different sections of the report covering all the details of the crime along with the daily progress of the investigation process.

In which of the following sections of the forensic investigation report did Arabella record the "nature of the claim and information provided to the officers"?

A. Investigation process

B. Investigation objectives

C. Evidence information

D. Evaluation and analysis process

ANSWER: C

Explanation:

Evidence information is the appropriate section because it records the case-specific information supplied to forensic personnel, including the nature of the claim or allegation and the information initially provided to the officers. This information establishes the context for the evidence examination: it identifies what was reported, what potential incident or offense is being investigated, and what material or circumstances prompted the forensic work. Recording this context alongside the evidence details helps ensure that the examination is traceable to the reported claim and that the resulting report clearly distinguishes information received from subsequent forensic findings. A well-documented evidence-information section also supports repeatability and review by preserving the initial evidentiary context available to the investigative team. NIST's guidance on integrating forensic techniques emphasizes documenting collected information, examination activities, and findings in a manner that supports the investigation and later reporting. Similarly, SWGDE guidance stresses complete documentation to preserve the context, handling, and interpretation of digital evidence. See NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response and SWGDE Published Documents.

QUESTION NO: 15

Ariana, a network security administrator, was instructed to protect the organization's switched network from ARP spoofing attacks. She must implement controls that validate ARP traffic and prevent unauthorized systems from associating fraudulent MAC addresses with valid IP addresses.

Which of the following controls can help Ariana mitigate ARP spoofing? (Choose three.)

A. Dynamic ARP Inspection (DAI)

B. DHCP snooping

C. Static ARP entries

D. Port mirroring

E. Virtual private network (VPN)

ANSWER: A B C

Explanation:

Dynamic ARP Inspection (DAI), **DHCP snooping**, and **static ARP entries** are appropriate controls. DAI inspects ARP packets on untrusted switch ports and validates IP-to-MAC address bindings before permitting ARP traffic. DHCP snooping builds a trusted binding database from legitimate DHCP exchanges, which DAI can use to verify ARP messages. Static ARP entries can also prevent unauthorized ARP updates for selected critical hosts by defining a fixed IP-to-MAC mapping.

ARP spoofing occurs when an attacker sends forged ARP messages to associate the attacker's MAC address with another device's IP address, such as a default gateway. This can enable interception or disruption of local network traffic. Port mirroring is used to copy traffic for monitoring and does not validate ARP mappings. A virtual private network protects traffic confidentiality across an untrusted network but does not itself stop forged ARP messages on a local segment. See Cisco documentation on Dynamic ARP Inspection and DHCP snooping.

QUESTION NO: 16

Paul, a computer user, has shared information with his colleague using an online application. The online application used by Paul has been incorporated with the latest encryption mechanism. This mechanism encrypts data by using a sequence of photons that have a spinning trait while traveling from one end to another, and these photons keep changing their shapes during their course through filters: vertical, horizontal, forward slash, and backslash.

Identify the encryption mechanism demonstrated in the above scenario.

A. Quantum cryptography

B. Homomorphic encryption

C. Rivest Shamir Adleman encryption

D. Elliptic curve cryptography

ANSWER: A

Explanation:

Quantum cryptography is correct because the scenario describes the use of individual photons and their polarization states to establish secure cryptographic key material. Vertical and horizontal polarization represent one measurement basis, while forward-slash and backslash polarization represent a second, diagonal basis. A sender encodes bits by selecting photon polarization states, and the receiver measures them using randomly selected filters. After transmission, the parties compare the bases they used over a conventional authenticated channel and retain only measurements made with matching bases. This is the core principle of quantum key distribution, commonly illustrated by the BB84 protocol.

The security benefit comes from quantum-mechanical measurement: observing an unknown photon state can disturb that state. Consequently, an attempted interception introduces detectable errors into the exchanged key, allowing the communicating parties to discard a compromised session. The resulting shared secret can then be used with conventional symmetric encryption to protect the actual information sent through the online application. NIST describes quantum key distribution as a method that uses quantum properties to establish secret keys and can reveal eavesdropping attempts. See the NIST definition of quantum key distribution and the NIST overview of quantum key distribution technology.

QUESTION NO: 17

Calvin spotted blazing flames originating from a physical file storage location in his organization because of a Short circuit. In response to the incident, he used a fire suppression system that helped curb the incident in the initial stage and prevented it from spreading over a large area. Which of the following firefighting systems did Calvin use in this scenario?

A. Fire detection system

B. Sprinkler system

C. Smoke detectors

D. Fire extinguisher

ANSWER: D

Explanation:

Fire extinguisher is correct because it is a portable, first-response fire-suppression device intended to control or extinguish an incipient-stage fire before it grows beyond the capacity of available equipment and personnel. Calvin directly observed flames and used a system that curbed the fire at its initial stage, which describes the practical use of a portable extinguisher. In a location containing physical files, the selected extinguisher must be appropriate for the materials involved and for the possibility that electrical equipment remains energized following a short circuit. Personnel should only attempt to use an extinguisher when they have been trained, the fire is still small and contained, they have a safe exit route, and emergency response procedures have been activated as required. The U.S. Occupational Safety and Health Administration defines portable fire extinguishers as equipment for use by employees to fight incipient-stage fires and requires employers to provide education regarding extinguisher use where applicable. OSHA's requirements and guidance are available at 29 CFR 1910.157, Portable Fire Extinguishers. Additional workplace fire-safety guidance is available from OSHA Fire Prevention.

QUESTION NO: 18

Ryder, an identity and access management administrator, was instructed to deploy multifactor authentication for remote users. The solution must require users to provide credentials from different authentication-factor categories before access is granted.

Which of the following combinations satisfy the multifactor authentication requirement? (Choose three.)

A. Password and hardware token

B. PIN and fingerprint

C. Smart card and facial recognition

D. Password and security question

E. PIN and password

ANSWER: A B C

Explanation:

A password combined with a hardware token uses a knowledge factor and a possession factor. A PIN combined with a fingerprint uses a knowledge factor and an inherence factor. A smart card combined with facial recognition uses a possession factor and an inherence factor. Each combination therefore contains two distinct factor categories.

Using two passwords does not provide multifactor authentication because both are knowledge factors. Likewise, answering two security questions uses only knowledge-based authentication. NIST defines authentication factors and describes multifactor authentication in NIST SP 800-63B.

QUESTION NO: 19

Shawn, a forensic officer, was appointed to investigate a crime scene that had occurred at a coffee shop. As a part of investigation, Shawn collected the mobile device from the victim, which may contain potential evidence to identify the culprits.

Which of the following points must Shawn follow while preserving the digital evidence? (Choose three.)

A. Never record the screen display of the device

B. Turn the device ON if it is OFF

C. Do not leave the device as it is if it is ON

D. Make sure that the device is charged

E. If the device is powered off, leave it off.

ANSWER: C D E

Explanation:

For mobile-device evidence, preservation must minimize changes to the device while preventing loss of volatile data and remote alteration. “If the device is powered off, leave it off” is essential because booting a seized device can modify system artifacts, initiate synchronization, trigger security controls, or otherwise alter potential evidence. The device’s powered state should be documented as found, along with visible notifications and other observable conditions.

When a device is already powered on, it should not simply be left unprotected. The examiner should maintain its current state, document the display, and promptly isolate it from cellular, Wi-Fi, Bluetooth, and other radio communications using appropriate methods such as a Faraday enclosure. This limits the risk of remote wiping, new message delivery, synchronization, or other external changes. Ensuring that an operating device remains charged helps avoid an unplanned shutdown, which could cause loss of volatile information or make later access more difficult. These actions must be performed under documented evidence-handling procedures that preserve chain of custody and integrity. NIST’s mobile-device forensic guidance discusses preserving device state, preventing network communications, and maintaining power where appropriate: NIST SP 800-101 Rev. 1. Additional incident-handling and evidence-preservation guidance is available from NIST.