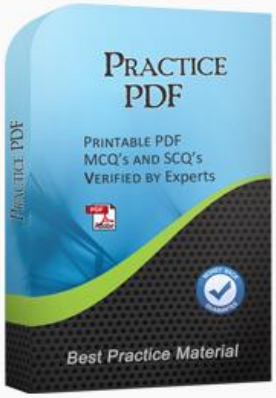
BraindumpQuiz

# BraindumpQuiz


- Online Tool, Convenient, easy to study.
- Instant Online Access
- Supports All Web Browsers
- Practice Online Anytime
- Test History and Performance Review
- Supports Windows / Mac / Android / iOS, etc.


- Installable Software Application
- Simulates Real Exam Environment
- Builds Exam Confidence
- Supports MS Operating System
- Two Modes For Practice
- Practice Offline Anytime




- Printable PDF Format
- Prepared by IT Experts
- Instant Access to Download
- Study Anywhere, Anytime
- 365 Days Free Updates
- Free PDF Demo Available

### Security & Privacy

We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.

### 365 Days Free Updates

Free update is available within 365 days after your purchase. After 365 days, you will get 50% discounts for updating.

### Money Back Guarantee

Full refund if you fail the corresponding exam in 90 days after purchasing. And Free get any another product.

### Instant Download

After Payment, our system will send you the products you purchase in mailbox in a minute after payment. If not received within 2 hours, please contact us.

**Exam** : **CCII**

**Title** : Certified Cyber Intelligence Investigator (CCII)

**Vendor** : McAfee

**Version** : DEMO

**NO.1** What technique can be used totrack cryptocurrency transactionsin cybercrime investigations?
**A.** Blockchain analysis
**B.** Reverse IP lookup
**C.** Dark web forums
**D.** Phishing attacks
***Answer:*** A
Explanation:
Comprehensive and Detailed In-Depth Explanation:Blockchain analysishelps track cryptocurrency transactions by:
* Following transaction history using blockchain explorers(e.g., Bitcoin, Ethereum).
* Identifying wallets and linking them to known entities.
* Detecting laundering patterns used in illicit activities(e.g., mixing services).
Whiledark web forums and phishingare methods usedto obtain private keys, blockchain analysis is a forensically sound techniqueused bylaw enforcement.
References:McAfee Institute CCII Cryptocurrency Investigations, Cybercrime Encyclopedia.

**NO.2** In Rosenberg v. Collins, the court held that if the computer output is used in the regular course of business, the evidence shall be admitted.
**A.** True
**B.** False
***Answer:*** A
Explanation:
InRosenberg v. Collins, the court established thatcomputer-generated records regularly used in business operationsareadmissibleas evidenceunder the business records exceptionto the hearsay rule. Investigators rely onmetadata, server logs, and financial recordsfor cyber investigations.
References:
U.S. Court Rulings on Digital Evidence
Federal Rules of Evidence for Cyber Investigations
McAfee Institute Legal Framework for Digital Evidence

**NO.3** Which technique is used for profiling individuals during an investigation?
**A.** Social Media Analysis
**B.** IP Tracking
**C.** Facial Recognition
**D.** All of the above
***Answer:*** D
Explanation:
Investigatorsuse multiple techniquesto build profiles on suspects:
Social Media Analysis- Reviewing posts, connections, and activities.
IP Tracking- Identifying locations and internet usage patterns.
Facial Recognition- Matching images to known identities in databases.
These techniques help incybercrime investigations, fraud detection, and counterterrorism. However, privacy laws govern theirethical and legal use.
References:McAfee Institute CCII Cyber Intelligence Guide, OSINT Handbook.

**NO.4** Prevention involves gaining or developing information related to threats of crime or terrorism and using it to apprehend offenders, harden targets, and use strategies that will eliminate or mitigate the threats.

**A.** True

**B.** False

***Answer:*** A

Explanation:

Prevention is acore function of intelligence and law enforcement operations. It involves:

Collecting intelligence on potential threatsbefore they materialize.

Identifying criminal or terrorist activitiesthrough surveillance and OSINT.

Hardened security measuresfor potential targets (e.g., increasing cybersecurity, bordersecurity).

Taking legal actionagainst identified offenders (e.g., arrests, asset seizures).Byusing proactive intelligence gathering, agencies candisrupt crime networks, prevent terrorist attacks, and reduce financial fraud.

References:McAfee Institute CCII Threat Prevention Module, Cyber Crime Investigator's Field Guide.

**NO.5** Auction fraud patterns typically involve trends and medians in the cost structure.

**A.** True

**B.** False

***Answer:*** A

Explanation:

Investigators analyzeprice fluctuations, listing patterns, and bidding historyto detectauction fraud. Unusual trends, such asrepeated low-price listings or last-minute bidding wars, indicate fraudulent activities.

References:McAfee Institute CCII Auction Fraud Analysis, Cyber Crime Investigator's Field Guide.

**NO.6** What are the top steps that will help you document an incident and assist federal, state, and local law enforcement agencies in their investigation?

**A.** Preserve the state of the computer at the time of the incident by making a backup copy of logs

**B.** If the incident is in progress, activate auditing software and consider implementing a keystroke monitoring system

**C.** Document the losses suffered by your organization as a result of the incident

**D.** Contact law enforcement

**E.** All of the above

***Answer:*** E

Explanation:

Incident documentation iscriticalin cyber investigations. Best practices include:

Data Preservation:Creatingforensic copiesof digital evidence.

Active Monitoring:Usingkeystroke logging and network traffic analysis.

Loss Documentation:Quantifyingfinancial and operational damage.

Legal Reporting:Contactinglaw enforcement and relevant regulatory bodies.

Following these steps ensuresevidence is admissible in court.

References:

McAfee Institute Cybercrime Reporting Guide

U.S. Department of Justice Digital Forensics Manual

Chain of Custody in Digital Evidence Collection

**NO.7** You can access the profile of a subject if they are represented by legal counsel.
**A.** True
**B.** False
***Answer:*** B
Explanation:
Accessing a subject's profile when they are represented by legal counselmay violate legal and ethical boundaries. Investigators must ensure compliance withlegal regulationsto avoid infringement on privacy rights. Unauthorized access could result inlegal liabilitiesunder variouscybercrime laws and ethical guidelinesfor digital investigations.
References:
McAfee Institute Cybercrime Investigator's Field Guide
OSINT Handbook
Federal Digital Privacy Laws

**NO.8** Investigators should always rely on screenshots as primary evidence in cyber investigations.
**A.** True
**B.** False
***Answer:*** B
Explanation:
Screenshots arenot considered primary evidencebecause they can beeasily altered or fabricated. Digital forensic practices require:
Website archive tools (e.g., Wayback Machine).
Metadata analysisfor verification.
Log extractionsfrom web servers.
References:McAfee Institute CCII OSINT Techniques, Cyber Crime Investigator's Field Guide.

**NO.9** What is Organized Retail Crime (ORC)?
**A.** The sale of stolen merchandise online
**B.** The stealing of retail merchandise, by multiple perpetrators
**C.** The act of stealing merchandise for profit
**D.** All of the above
***Answer:*** D
Explanation:
Organized Retail Crime (ORC)refers tocoordinated theft ringsthat steal merchandise in bulk and resell iton online platforms, black markets, and dark web marketplaces. These crimescause billions in lossesfor retailers annually.
References:McAfee Institute CCII Retail Crime Training, Cybercrime Encyclopedia.

**NO.10** Thieves, in general, are motivated to steal and sell goods because they can quickly convert them for money.
**A.** True
**B.** False
***Answer:*** A

Explanation:
The primarymotivation behind theftis the ability toquickly convert stolen goods into cash. This is seen in:
Pawn shop transactions
Online marketplaces (e.g., eBay, Facebook Marketplace)
Dark web black markets
Selling through fences (middlemen who resell stolen goods)Quick conversion reduces the chance oflaw enforcement tracking the stolen goodsand makestheft an attractive, high-profit crimefor criminals.
References:McAfee Institute CCII Financial Crime Guide, Cyber Crime Investigator's Field Guide.

**NO.11** Just like a hostname can be changed, a MAC address can also be changed through a process called MAC Spoofing.
**A.** True
**B.** False
***Answer:*** A
Explanation:
MAC spoofingallows attackers tochange their network identity, making tracking harder.Cybercriminals use it to:
Bypass network security measures(e.g., MAC filtering).
Evade law enforcement trackingin cyber investigations.
Appear as another devicein network logs.
References:McAfee Institute CCII Cyber Threat Guide, The Hitchhiker's Guide to Online Anonymity.

**NO.12** Direct evidence is called to eliminate a specific act.
**A.** True
**B.** False
***Answer:*** B
Explanation:
Direct evidencerefers tofirsthand accounts, recordings, or eyewitness testimonythat directly proves a fact.
However, it doesnot necessarily eliminateother possible explanations for an act. Examples include:
Surveillance footagecapturing a suspect at a crime scene.
Witness statementsconfirming actions.
While direct evidence is compelling, investigatorsstill assess additional evidence to support conclusions.
References:
McAfee Institute Digital Evidence Handbook
U.S. Court Evidence Rules
Federal Investigation Techniques Manual

**NO.13** If you have no luck identifying a subject on a social network, try adjusting your regional settings and change your location. Sometimes, the user's privacy settings are set to only show their profile to users in the same geographical location.
**A.** True

**B.** False

***Answer:*** A

Explanation:

Many social media platformsrestrict visibilitybased on geographic settings. ChangingVPN locationsor utilizingregional search engines(e.g., Yandex for Russia, Baidu for China) increases the chances of discovering hidden profiles.

References:

McAfee Institute Social Media OSINT Guide

Regional Privacy and Cybersecurity Laws

VPN Usage in Cyber Investigations