Exam Digital-Forensics-in-Cybersecurity Reference, Digital-Forensics-in-Cybersecurity Reliable Test Sims

The Digital Forensics in Cybersecurity (D431/C840) Course Exam (Digital-Forensics-in-Cybersecurity) practice questions have a close resemblance with the actual Digital Forensics in Cybersecurity (D431/C840) Course Exam (Digital-Forensics-in-Cybersecurity) exam. Our WGU Digital-Forensics-in-Cybersecurity exam dumps give help to give you an idea about the actual Digital Forensics in Cybersecurity (D431/C840) Course Exam (Digital-Forensics-in-Cybersecurity) exam. You can attempt multiple Digital Forensics in Cybersecurity (D431/C840) Course Exam (Digital-Forensics-in-Cybersecurity) exam questions on the software to improve your performance.

WGU Digital-Forensics-in-Cybersecurity Exam Syllabus Topics:

Topic	Details
Topic 1	• Domain Legal and Procedural Requirements in Digital Forensics: This domain measures the skills of Digital Forensics Technicians and focuses on laws, rules, and standards that guide forensic work. It includes identifying regulatory requirements, organizational procedures, and accepted best practices that ensure an investigation is defensible and properly executed.

Topic 2	• Domain Incident Reporting and Communication: This domain measures the skills of Cybersecurity Analysts and focuses on writing incident reports that present findings from a forensic investigation. It includes documenting evidence, summarizing conclusions, and communicating outcomes to organizational stakeholders in a clear and structured way.
Topic 3	• Domain Evidence Analysis with Forensic Tools: This domain measures skills of Cybersecurity technicians and focuses on analyzing collected evidence using standard forensic tools. It includes reviewing disks, file systems, logs, and system data while following approved investigation processes that ensure accuracy and integrity.
Topic 4	• Domain Recovery of Deleted Files and Artifacts: This domain measures the skills of Digital Forensics Technicians and focuses on collecting evidence from deleted files, hidden data, and system artifacts. It includes identifying relevant remnants, restoring accessible information, and understanding where digital traces are stored within different systems.
Topic 5	• Domain Digital Forensics in Cybersecurity: This domain measures the skills of Cybersecurity technicians and focuses on the core purpose of digital forensics in a security environment. It covers the techniques used to investigate cyber incidents, examine digital evidence, and understand how findings support legal and organizational actions.

>> Exam Digital-Forensics-in-Cybersecurity Reference <<

Digital-Forensics-in-Cybersecurity Reliable Test Sims, Passing Digital-Forensics-in-Cybersecurity Score

We always learned then forget, how to solve this problem, the answer is to have a good memory method, our Digital-Forensics-in-Cybersecurity exam question will do well on this point. Our Digital-Forensics-in-Cybersecurity real exam materials have their own unique learning method, abandon the traditional rote learning, adopt diversified memory patterns, such as the combination of text and graphics memory method, to distinguish between the memory of knowledge. Our Digital-Forensics-in-Cybersecurity learning reference files are so scientific and reasonable that you can buy them safely.

WGU Digital Forensics in Cybersecurity (D431/C840) Course Exam Sample Questions (Q79-Q84):

NEW QUESTION # 79
A forensic investigator suspects that spyware has been installed to a Mac OS X computer by way of an update.
Which Mac OS X log or folder stores information about system and software updates?

- A. /var/log/daily.out
- B. /Library/Receipts
- C. /var/spool/cups
- D. /var/vm

Answer: B

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
The/Library/Receiptsfolder on Mac OS X contains receipts that track software installation and updates, including system and application updates. This folder helps forensic investigators determine which updates were installed and when, useful for detecting suspicious or unauthorized software installations like spyware.
* /var/spool/cupsis related to printer spooling.
* /var/log/daily.outcontains daily system log summaries but not detailed update records.
* /var/vmcontains virtual memory files.
NIST and Apple forensics documentation indicate that/Library/Receiptsis a key location for examining software installation history.

NEW QUESTION # 80
Susan was looking at her credit report and noticed that several new credit cards had been opened lately in her name. Susan has not opened any of the credit card accounts herself.
Which type of cybercrime has been perpetrated against Susan?

- A. SQL injection
- B. Identity theft
- C. Cyberstalking
- D. Malware

Answer: B

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Identity theft occurs when an attacker unlawfully obtains and uses another person's personal information to open accounts, access credit, or commit fraud. The opening of credit cards without the victim's consent is a classic example.
* SQL injection is a web application attack method that does not directly relate to this case.
* Cyberstalking involves harassment via digital means and is unrelated.
* Malware is malicious software and may be used to facilitate identity theft but is not the crime itself.
Reference:According to the U.S. Federal Trade Commission (FTC) definitions and NIST Cybersecurity Framework, identity theft is defined as the unauthorized use of someone's personal information for fraudulent purposes, perfectly matching Susan's situation.

NEW QUESTION # 81
Which Windows 7 operating system log stores events collected from remote computers?

- A. Application
- B. Security
- C. System
- D. ForwardedEvents

Answer: D

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
TheForwardedEventslog in Windows 7 is specifically designed to store events collected from remote computers via event forwarding. This log is part of the Windows Event Forwarding feature used in enterprise environments to centralize event monitoring.
* TheSystemandApplicationlogs store local system and application events.
* TheSecuritylog stores local security-related events.
* ForwardedEventscollects and stores events forwarded from other machines.
Microsoft documentation and NIST SP 800-86 mention the use of ForwardedEvents for centralized event log collection in investigations.

NEW QUESTION # 82
Which principle of evidence collection states that access to evidence must be tracked from the time it is seized through its use in court?

- A. Chain of custody
- B. Audit log
- C. Evidence record
- D. Event log

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
The Chain of Custody (CoC) is the documented and unbroken transfer record of evidence handling, from seizure to presentation in court. It ensures that the evidence has been preserved, controlled, and protected from tampering or alteration.
* Evidence record documents evidence details but is less formal than CoC.
* Event log and audit log are system-generated records and do not replace the formal CoC.

* CoC is a fundamental forensic principle as outlined by NIST SP 800-86 and the Scientific Working Group on Digital Evidence (SWGDE) best practices, ensuring evidence admissibility and reliability in legal proceedings.

NEW QUESTION # 83

Which universal principle must be observed when handling digital evidence?

- A. Keep the evidence in a plastic bag
- B. Make a copy and analyze the original
- C. Get the signatures of two witnesses
- D. Avoid making changes to the evidence

Answer: D

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
The foremost principle in digital forensics isnever altering the original evidence. This ensures integrity, authenticity, and admissibility in court.
* Investigators analyze forensic copies, not originals.
* Write-blockers and hashing are used to prevent changes.
* Any alteration-intentional or accidental-can invalidate evidence.
Reference:NIST SP 800-86 and SP 800-101 define the unaltered preservation of evidence as the first and most essential forensic rule.

NEW QUESTION # 84

......

If you still have a trace of enterprise, you really want to start working hard! Digital-Forensics-in-Cybersecurity exam questions are the most effective helpers on your path. By using Digital-Forensics-in-Cybersecurity study engine, your abilities will improve and your mindset will change. Who does not want to be a positive person? This is all supported by strength! In any case, a lot of people have improved their strength through Digital-Forensics-in-Cybersecurity Exam simulating. They now have the opportunity they want. Whether to join the camp of the successful ones, purchase Digital-Forensics-in-Cybersecurity study engine, you decide for yourself!

Digital-Forensics-in-Cybersecurity Reliable Test Sims: https://www.briandumpsprep.com/Digital-Forensics-in-Cybersecurity-prep-exam-braindumps.html

- Professional Exam Digital-Forensics-in-Cybersecurity Reference Covers the Entire Syllabus of Digital-Forensics-in-Cybersecurity 🎯 Search for ➡ Digital-Forensics-in-Cybersecurity 🎯🎯🎯 and obtain a free download on 🎯 www.examcollectionpass.com 🎯 🎯Valid Digital-Forensics-in-Cybersecurity Test Notes
- Pdfvce Digital-Forensics-in-Cybersecurity Digital Forensics in Cybersecurity (D431/C840) Course Exam Exam Questions are Available in Three Different Formats 🎯 Open ⇒ www.pdfvce.com ⇐ and search for （ Digital-Forensics-in-Cybersecurity ） to download exam materials for free 🎯Digital-Forensics-in-Cybersecurity Frequent Updates
- Pass Guaranteed Marvelous WGU Digital-Forensics-in-Cybersecurity - Exam Digital Forensics in Cybersecurity (D431/C840) Course Exam Reference 🎯 Open [www.prep4away.com] enter { Digital-Forensics-in-Cybersecurity } and obtain a free download 🎯Digital-Forensics-in-Cybersecurity Free Updates
- www.stes.tyc.edu.tw, myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, xaxucytu.obsidianportal.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes

What's more, part of that BraindumpsPrep Digital-Forensics-in-Cybersecurity dumps now are free: https://drive.google.com/open?id=1BloTh2rsX-iKZO_mbyBa57KxPONCiQw1