Digital-Forensics-in-Cybersecurity Reliable Exam Registration | Digital-Forensics-in-Cybersecurity Latest Braindumps Free

DOWNLOAD the newest DumpsFree Digital-Forensics-in-Cybersecurity PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1ByBRPj0o7baihgcb8B0fJqQ0DELxRdJ6

All these three WGU Digital-Forensics-in-Cybersecurity exam questions formats contain the real, valid, and error-free Digital Forensics in Cybersecurity (D431/C840) Course Exam (Digital-Forensics-in-Cybersecurity) exam practice test questions that are ideal study material for quick WGU Digital-Forensics-in-Cybersecurity Exam Preparation. Just choose the right DumpsFree Digital Forensics in Cybersecurity (D431/C840) Course Exam Questions formats and download quickly and start Digital Forensics in Cybersecurity (D431/C840) Course Exam (Digital-Forensics-in-Cybersecurity) exam preparation without wasting further time.

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 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 4	• 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 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.

Digital-Forensics-in-Cybersecurity Latest Braindumps Free - Valid Digital-Forensics-in-Cybersecurity Exam Format

Sometimes, you may worry about too much on the Digital-Forensics-in-Cybersecurity exam and doubt a lot on the Digital-Forensics-in-Cybersecurity exam questions. But if your friends or other familiar people passed the exam, you may be more confident in his evaluation. In any case, our common goal is to let you pass the exam in the shortest possible time! And we can proudly claim that if you study with our Digital-Forensics-in-Cybersecurity Training Materials for 20 to 30 hours, then you can pass the exam with ease. And it is the data provided and tested by our worthy customers!

WGU Digital Forensics in Cybersecurity (D431/C840) Course Exam Sample Questions (Q80-Q85):

NEW QUESTION # 80
A forensic scientist is examining a computer for possible evidence of a cybercrime.
Why should the forensic scientist copy files at the bit level instead of the OS level when copying files from the computer to a forensic computer?

- A. Copying files at the OS level changes the timestamp of the files.
- B. Copying files at the OS level takes too long to be practical.
- C. Copying files at the OS level will copy extra information that is unnecessary.
- D. Copying files at the OS level fails to copy deleted files or slack space.

Answer: D

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Bit-level (or bit-stream) copying captures every bit on the storage media, including files, deleted files, slack space (unused space within a cluster), and unallocated space. This ensures all digital evidence, including artifacts not visible at the OS level, is preserved for analysis.
* Copying at the OS level captures only allocated files visible in the file system, missing deleted files and slack space.
* Bit-level copying is a cornerstone of forensic best practices as specified in NIST SP 800-86 and SWGDE guidelines.
* Timestamp changes and unnecessary information issues are secondary concerns compared to the completeness of evidence.

NEW QUESTION # 81
A forensic investigator needs to identify where email messages are stored on a Microsoft Exchange server.
Which file extension is used by Exchange email servers to store the mailbox database?

- A. .mail
- B. .edb
- C. .nsf
- D. .db

Answer: B

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Microsoft Exchange Server uses the.edbfile extension for its Extensible Storage Engine (ESE) database files.
These.edbfiles contain the mailbox data including emails, calendar items, and contacts.
* .nsfis used by IBM Lotus Notes.
* .mailand.dbare generic extensions but not standard for Exchange.
* The.edbfile is the primary data store for Exchange mailboxes.
Reference:According to Microsoft technical documentation and forensic manuals, the Exchange mailbox database is stored in.edbfiles, which forensic examiners analyze to recover email evidence.

NEW QUESTION # 82
Which characteristic applies to magnetic drives compared to solid-state drives (SSDs)?

- A. Higher cost
- B. Faster read/write speeds
- C. Less susceptible to damage
- D. Lower cost

Answer: D

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Magnetic hard drives generally have a lower cost per gigabyte compared to solid-state drives (SSDs).
However, they are more susceptible to mechanical damage and slower in data access.
* SSDs have no moving parts and provide better durability and speed but at a higher price.
* Forensics practitioners consider these differences during evidence acquisition.
Reference:Digital forensics texts and hardware overviews describe magnetic drives as cost-effective but fragile compared to SSDs.

NEW QUESTION # 83
Which file stores local Windows passwords in the Windows\System32\ directory and is subject to being cracked by using a live CD?

- A. Ntidr
- B. IPSec
- C. HAL
- D. SAM

Answer: D

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
The SAM (Security Account Manager) file located in theWindows\System32\configdirectory stores hashed local user account passwords. It can be accessed and extracted using a live CD or bootable forensic tool, which allows the forensic investigator to bypass the running operating system and avoid altering the evidence.
* IPSec is related to network security policies, not password storage.
* HAL (Hardware Abstraction Layer) is a system file managing hardware interaction.
* Ntidr is a boot loader file in Windows NT systems.
Cracking password hashes extracted from the SAM file is a common forensic practice to recover user passwords during investigations.
Reference:NIST Special Publication 800-86 and Windows forensic textbooks confirm that the SAM file is the repository of local password hashes accessible via forensic live CDs or imaging.

NEW QUESTION # 84
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/spool/cups
- B. /Library/Receipts
- C. /var/log/daily.out
- 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 # 85
.....

Digital-Forensics-in-Cybersecurity exam dumps provided by DumpsFree are tested through practice, and are the most correct and the newest practical Digital-Forensics-in-Cybersecurity test dumps. Our DumpsFree can provide accurate Digital-Forensics-in-Cybersecurity certification training questions based on extensive research and the experience of real world to make you pass Digital-Forensics-in-Cybersecurity Certification Exam in a short time. If you purchase our Digital-Forensics-in-Cybersecurity exam dumps, we will offer free update service within one year.