Digital-Forensics-in-Cybersecurity Practice Guide 100% Pass | Latest Digital-Forensics-in-Cybersecurity Exam Certification: Digital Forensics in Cybersecurity (D431/C840) Course Exam

BTW, DOWNLOAD part of Dumpexams Digital-Forensics-in-Cybersecurity dumps from Cloud Storage: https://drive.google.com/open?id=1B2jFV6mlCTILygTiWNiOz-00BHApSJkn

By analyzing the syllabus and new trend, our Digital-Forensics-in-Cybersecurity practice engine is totally in line with this exam for your reference. So grapple with this chance, our Digital-Forensics-in-Cybersecurity learning materials will not let you down. With our Digital-Forensics-in-Cybersecurity Study Guide, not only that you can pass you exam easily and smoothly, but also you can have a wonderful study experience based on the diversed versions of our Digital-Forensics-in-Cybersecurity training prep.

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

Topic	Details
Topic 1	• 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.
Topic 2	• 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 3	• 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 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 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.

>> Digital-Forensics-in-Cybersecurity Practice Guide <<

WGU Digital-Forensics-in-Cybersecurity Exam | Digital-Forensics-in-Cybersecurity Practice Guide - Bringing Candidates Good Digital-Forensics-in-Cybersecurity Exam Certification

As a professional dumps vendors, we provide the comprehensive Digital-Forensics-in-Cybersecurity pass review that is the best helper for clearing Digital-Forensics-in-Cybersecurity actual test, and getting the professional certification quickly. It is a best choice to improve your professional skills and ability to face the challenge of Digital-Forensics-in-Cybersecurity Practice Exam with our online training. We have helped thousands of candidates to get succeed in their career by using our Digital-Forensics-in-Cybersecurity study guide.

WGU Digital Forensics in Cybersecurity (D431/C840) Course Exam Sample Questions (Q56-Q61):

NEW QUESTION # 56
While collecting digital evidence from a running computer involved in a cybercrime, the forensic investigator makes a list of items that need to be collected.
Which piece of digital evidence should be collected first?

- A. Recently accessed files
- B. Temporary Internet files
- C. Chat room logs
- D. Security logs

Answer: D

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
When collecting evidence from a running system, volatile and critical evidence such as security logs should be collected first as they are most susceptible to being overwritten or lost. Security logs may contain valuable information on unauthorized access or malicious activity.
* Chat room logs, recently accessed files, and temporary internet files are important but often less volatile or can be recovered from disk later.
* NIST SP 800-86 and SANS Incident Response Guidelines prioritize the collection of volatile logs and memory contents first.
This approach helps ensure preservation of time-sensitive data critical for forensic analysis.

NEW QUESTION # 57
An organization believes that a company-owned mobile phone has been compromised.
Which software should be used to collect an image of the phone as digital evidence?

- A. Forensic SIM Cloner
- B. Forensic Toolkit (FTK)
- C. Data Doctor
- D. PTFinder

Answer: B

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Forensic Toolkit (FTK) is a widely recognized and trusted software suite in digital forensics used to acquire and analyze forensic images of devices, including mobile phones. FTK supports the creation of bit-by-bit images of digital evidence, ensuring the integrity and admissibility of the evidence in legal contexts. This imaging process is crucial in preserving the original state of the device data without alteration.
* FTK enables forensic investigators to perform logical and physical acquisitions of mobile devices.
* It maintains the integrity of the evidence by generating cryptographic hash values (MD5, SHA-1) to prove that the image is an

exact copy.
* Other options such as PTFinder or Forensic SIM Cloner focus on specific tasks like SIM card cloning or targeted data extraction but do not provide full forensic imaging capabilities.
* Data Doctor is more aligned with data recovery rather than forensic imaging.
Reference:According to standard digital forensics methodologies outlined by NIST Special Publication 800-101(Guidelines on Mobile Device Forensics) and the SANS Institute Digital Forensics and Incident Response guides, forensic tools used to acquire mobile device images must be capable of bit-stream copying with hash verification, which FTK provides.

NEW QUESTION # 58
Which technique allows a cybercriminal to hide information?

- A. Steganalysis
- B. Steganography
- C. Encryption
- D. Cryptography

Answer: B

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Steganography is the technique of hiding information within another file, message, image, or medium to conceal the existence of the information itself. It differs from encryption in that the data is hidden, not just scrambled.
* Steganalysis is the detection or analysis of hidden data.
* Encryption and cryptography involve scrambling data but do not inherently hide its existence.
NIST and digital forensics guidelines define steganography as the art of concealed writing or data hiding, used by criminals to evade detection.

NEW QUESTION # 59
Which U.S. law protects journalists from turning over their work or sources to law enforcement before the information is shared with the public?

- A. The Privacy Protection Act (PPA)
- B. Electronic Communications Privacy Act (ECPA)
- C. Health Insurance Portability and Accountability Act (HIPAA)
- D. Communications Assistance to Law Enforcement Act (CALEA)

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
The Privacy Protection Act (PPA) protects journalists by restricting law enforcement's ability to search or seize materials intended for public dissemination unless certain exceptions apply. It safeguards journalistic sources and unpublished work from unwarranted government intrusion.
* The PPA ensures freedom of the press and protects confidential information.
* Law enforcement must comply with procedural safeguards before accessing journalistic materials.
Reference:Legal texts and digital forensic guidelines note the PPA's role in balancing investigative needs with press freedoms.

NEW QUESTION # 60
The human resources manager of a small accounting firm believes he may have been a victim of a phishing scam. The manager clicked on a link in an email message that asked him to verify the logon credentials for the firm's online bank account.
Which digital evidence should a forensic investigator collect to investigate this incident?

- A. Network traffic logs
- B. System logs
- C. Browser cache
- D. Email headers

Answer: C

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
The browser cache stores recently accessed web pages, images, and cookies, which may include phishing site content and related activity. Investigators analyzing phishing attacks collect browser cache data to reconstruct the victim's web activity and detect malicious sites.
* Cached web pages help corroborate victim statements and establish timelines.
* Browser history and cache are volatile and must be preserved promptly.
Reference:According to NIST SP 800-101 and forensic guides, browser cache is critical in investigating phishing and web-based attacks.

NEW QUESTION # 61
.....

Dumpexams's WGU Digital-Forensics-in-Cybersecurity exam training materials is the best training materials. If you are an IT staff, it will be your indispensable training materials. Do not take your future betting on tomorrow. Dumpexams's WGU Digital-Forensics-in-Cybersecurity exam training materials are absolutely trustworthy. We are dedicated to provide the materials to the world of the candidates who want to participate in IT exam. To get the WGU Digital-Forensics-in-Cybersecurity Exam Certification is the goal of many IT people & Network professionals. The pass rate of Dumpexams is incredibly high. We are committed to your success.

Digital-Forensics-in-Cybersecurity Exam Certification: https://www.dumpexams.com/Digital-Forensics-in-Cybersecurity-real-answers.html

myportal.utt.edu.tt, www.stes.tyc.edu.tw, rabonystudywork.com, Disposable vapes

BONUS!!! Download part of Dumpexams Digital-Forensics-in-Cybersecurity dumps for free: https://drive.google.com/open?id=1B2jFV6mlCTILygTiWNiOz-00BHApSJkn