Certification WGU Digital-Forensics-in-Cybersecurity Exam | Digital-Forensics-in-Cybersecurity Download Pdf

BTW, DOWNLOAD part of Lead1Pass Digital-Forensics-in-Cybersecurity dumps from Cloud Storage: https://drive.google.com/open?id=1EtJQSLmWdmAhJDB_SD0LmbuP_-7r2xl9

The modern WGU world is changing its dynamics at a fast pace. To stay and compete in this challenging market, you have to learn and enhance your in-demand skills. Fortunately, with the Digital Forensics in Cybersecurity (D431/C840) Course Exam (Digital-Forensics-in-Cybersecurity) certification exam you can do this job nicely and quickly. To do this you just need to enroll in the WGU Digital-Forensics-in-Cybersecurity Certification Exam and put all your efforts to pass the Digital Forensics in Cybersecurity (D431/C840) Course Exam (Digital-Forensics-in-Cybersecurity) certification exam.

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 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 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 5	• 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.

Pass Guaranteed Quiz Digital-Forensics-in-Cybersecurity - Digital Forensics in Cybersecurity (D431/C840) Course Exam –Professional Certification Exam

WGU Digital-Forensics-in-Cybersecurity exam torrent is famous for instant download. You will receive downloading link and password within ten minutes, and if you don't receive, just contact us, we will check for you. In addition, Digital-Forensics-in-Cybersecurity Exam Materials are high quality, it covers major knowledge points for the exam, you can have an easy study if you choose us.

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

NEW QUESTION # 56
How should a forensic scientist obtain the network configuration from a Windows PC before seizing it from a crime scene?

- A. By opening the Network and Sharing Center
- B. By rebooting the computer into safe mode
- C. By checking the system properties
- D. By using the ipconfig command from a command prompt on the computer

Answer: D

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
The ipconfig command executed at a Windows command prompt displays detailed network configuration information such as IP addresses, subnet masks, and default gateways. Collecting this information prior to seizure preserves volatile evidence relevant to the investigation.
* Documenting network settings supports the understanding of the suspect system's connectivity at the time of seizure.
* NIST recommends capturing volatile data (including network configuration) before shutting down or disconnecting a suspect machine.
Reference:NIST SP 800-86 and forensic best practices recommend gathering volatile evidence using system commands like ipconfig.

NEW QUESTION # 57
How is the Windows swap file, also known as page file, used?

- A. Primarily for security
- B. Augments the RAM
- C. Reserved for system files
- D. Replaces bad sectors

Answer: B

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:
The Windows swap file, or page file, is a system file used to extend physical memory by storing data that cannot fit into the RAM. When RAM is full, the OS swaps inactive data pages to this file, thus augmenting RAM capacity.
* It does not replace bad sectors; that function is for disk management utilities.
* It is not primarily for security but for memory management.
* It is not reserved exclusively for system files but is used dynamically for memory paging.
Reference:Microsoft's official documentation and forensic guides like NIST SP 800-86 describe the page file' s role in virtual memory management and its importance in forensic analysis because it may contain fragments of memory and sensitive information.

NEW QUESTION # 58
What is one purpose of steganography?

- A. To deliver information secretly
- B. To delete files securely
- C. To encrypt data for security
- D. To compress large files

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Steganography is used to conceal information within other seemingly innocuous data, such as embedding messages inside image files, allowing secret delivery of information without detection.
* Unlike encryption, steganography hides the existence of the message itself.
* It is an anti-forensic technique used to evade detection.
Reference:NIST and digital forensics literature describe steganography as covert communication methodology.

NEW QUESTION # 59
Which United States law defines requirements for record keeping and destruction of electronic records for publicly traded companies?

- A. Computer Security Act
- B. Telecommunications Act
- C. USA PATRIOT Act
- D. Sarbanes-Oxley Act

Answer: D

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
The Sarbanes-Oxley Act (SOX) establishes strict requirements for the creation, retention, protection, and destruction of electronic business records for publicly traded companies. The law was enacted to prevent corporate fraud and mandates secure handling of digital documents, email, and logs.
* SOX requires auditing controls that ensure electronic records remain unaltered.
* Section 802 specifically defines criminal penalties for altering, destroying, or falsifying electronic records.
* Forensic investigators must ensure evidence from publicly traded companies is retained in compliance with SOX requirements.
Reference:Digital Forensics and legal compliance guides cite SOX as the primary U.S. law governing electronic record retention and destruction procedures for publicly traded organizations.

NEW QUESTION # 60
Which technique allows a cybercriminal to hide information?

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

Answer: A

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 # 61
.....

Disposable vapes

P.S. Free 2026 WGU Digital-Forensics-in-Cybersecurity dumps are available on Google Drive shared by Lead1Pass: https://drive.google.com/open?id=1EtJQSLmWdmAhJDB_SD0LmbuP_-7r2xl9