Quiz 2026 Digital-Forensics-in-Cybersecurity: Reliable Clear Digital Forensics in Cybersecurity (D431/C840) Course Exam Exam

WGU D431 Final Exam Review (New Update) Digital Forensics in Cybersecurity| Qs & As| Grade A 100% Correct (Verified A nswers)

QUESTION
What is Internet Forensics?

Answer:
The process of piecing together where and when a user has been on the internet.

QUESTION
What is The Wireless Communications and Public Safety Act of 1999

Answer:
Allows for collection and use of "empty" communications, which means nonverbal and nontext communications, such as GPS information.

QUESTION
What is The Sarbanes-Oxley Act of 2002

Answer:
Contains many provisions about recordkeeping and destruction of electronic records relating to t he management and operation of publicly held companies

QUESTION
Are warrants needed when evidence in plain sight?

P.S. Free 2026 WGU Digital-Forensics-in-Cybersecurity dumps are available on Google Drive shared by VCETorrent: https://drive.google.com/open?id=1X8fwYFT7zQSGH5RunM2NBDqKAsXI7FhD

Another great way to assess readiness is the WGU Digital-Forensics-in-Cybersecurity web-based practice test. This is one of the trusted online WGU Digital-Forensics-in-Cybersecurity prep materials to strengthen your concepts. All specs of the desktop software are present in the web-based WGU Digital-Forensics-in-Cybersecurity Practice Exam.

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

Topic	Details
Topic 1	• 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 2	• 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 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 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.

Digital-Forensics-in-Cybersecurity Valid Exam Notes & Digital-Forensics-in-Cybersecurity Brain Exam

This format is for candidates who do not have the time or energy to use a computer or laptop for preparation. The WGU Digital-Forensics-in-Cybersecurity PDF file includes real WGU Digital-Forensics-in-Cybersecurity questions, and they can be easily printed and studied at any time. VCETorrent regularly updates its PDF file to ensure that its readers have access to the updated questions.

WGU Digital Forensics in Cybersecurity (D431/C840) Course Exam Sample Questions (Q39-Q44):

NEW QUESTION # 39
Which universal principle must be observed when handling digital evidence?

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

Answer: A

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 # 40
The chief information officer of an accounting firm believes sensitive data is being exposed on the local network.
Which tool should the IT staff use to gather digital evidence about this security vulnerability?

- A. Firewall
- B. Antivirus
- C. Sniffer
- D. Packet filter

Answer: C

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
A sniffer, also known as a packet analyzer, captures network traffic in real time and allows IT staff to monitor and analyze data packets passing through the network. This is crucial when investigating potential data leaks or network vulnerabilities. Using a sniffer helps identify unauthorized transmissions of sensitive data and trace suspicious activity at the packet level.
* Sniffers collect raw network data which can be analyzed for patterns or anomalies.
* According to NIST guidelines on network forensics, packet capture tools (sniffers) are essential in gathering digital evidence related to network security incidents.
Reference:NIST Special Publication 800-86 (Guide to Integrating Forensic Techniques into Incident Response) highlights the importance of sniffers in network-based investigations.

NEW QUESTION # 41
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. Temporary Internet files
- B. Chat room logs
- C. Recently accessed files
- 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 # 42
Which law is related to the disclosure of personally identifiable protected health information (PHI)?

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

Answer: B

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
HIPAA establishes standards to protect sensitive patient health information (PHI) and regulates the use and disclosure of such information. Forensic investigators dealing with health data must comply with HIPAA to avoid legal violations.
* HIPAA compliance is critical when handling medical records in investigations.
* Breach of PHI privacy can result in civil and criminal penalties.
Reference:HIPAA is widely referenced in cybersecurity and forensic policies relating to healthcare data protection.

NEW QUESTION # 43
Which tool identifies the presence of steganography?

- A. Forensic Toolkit (FTK)
- B. Disk Investigator
- C. ComputerCOP
- D. DiskDigger

Answer: B

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Disk Investigator is a forensic tool that can analyze disk images and file systems to identify hidden data, including the presence of steganography by examining slack space, hidden files, and embedded data.
* DiskDigger is mainly a data recovery tool.
* FTK is a comprehensive forensic suite but does not specialize in steganography detection.
* ComputerCOP is a parental control software, not a forensic tool.
Digital forensic best practices recognize Disk Investigator as useful for detecting steganographic content in files and disk areas.

NEW QUESTION # 44
......

The VCETorrent team regularly updates the Digital-Forensics-in-Cybersecurity exam pdf format to make sure that applicants receive the most up-to-date WGU Digital-Forensics-in-Cybersecurity exam questions. Additionally, our Digital-Forensics-in-Cybersecurity PDF is designed to be user-friendly and accessible on any smart device, which means that students can prepare for the Digital-Forensics-in-Cybersecurity from anywhere, at any time.

www.pdfvce.com □ □Digital-Forensics-in-Cybersecurity Valid Test Sample

- Digital-Forensics-in-Cybersecurity Reliable Cram Materials ♣ Digital-Forensics-in-Cybersecurity Latest Exam □ Digital-Forensics-in-Cybersecurity Valid Test Prep □ Search for ✔ Digital-Forensics-in-Cybersecurity □✔□ and download it for free immediately on □ www.verifieddumps.com □ □Digital-Forensics-in-Cybersecurity Latest Exam
- www.stes.tyc.edu.tw, study.stcs.edu.np, www.stes.tyc.edu.tw, www.upskillonline.org, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, samerawad.com, github.com, www.stes.tyc.edu.tw, Disposable vapes

P.S. Free & New Digital-Forensics-in-Cybersecurity dumps are available on Google Drive shared by VCETorrent: https://drive.google.com/open?id=1X8fwYFT7zQSGH5RunM2NBDqKAsXI7FhD