

# Digital-Forensics-in-Cybersecurity Valid Real Exam & Digital-Forensics-in-Cybersecurity Latest Test Report

## WGU - D431 DIGITAL FORENSICS IN CYBERSECURITY EXAM 2024 WITH 100% CORRECT ANSWERS

Which law requires both parties to consent to the recording of a conversation?

- A. Electronic Communications Privacy (ECPA)
- B. Communications Assistance to Law Enforcement Act (CALEA)
- C. USA Patriot Act
- D. Health Insurance Portability and Accountability Act (HIPAA) Answer ✓✓ - A. Electronic Communication Privacy (ECPA)

Which law is related to the disclosure of personally identifiable protected health information (PHI)?

- A. Federal Privacy Act of 1974
- B. Electronic Communication Privacy Act
- C. Health Insurance Portability and Accountability Act (HIPAA)
- D. CAN-SPAM Act Answer ✓✓ - C. Health Insurance Portability and Accountability Act (HIPAA)

Which U.S. law criminalizes the act of knowingly using misleading domain name with the intent to deceive a minor into viewing harmful materials?

- A. 18 U.S.C. 2252B
- B. CAN-SPAM Act
- C. Children's Online Privacy Protection Act (COPPA)
- D. Communication Decency Act Answer ✓✓ - A. 18 U.S.C. 2252B

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

P.S. Free 2026 WGU Digital-Forensics-in-Cybersecurity dumps are available on Google Drive shared by TestPDF:  
<https://drive.google.com/open?id=1nd6PPWNPFOoNQbBLqkWK10UqHRMjffVk>

As old saying goes, god will help those who help themselves. So you must keep inspiring yourself no matter what happens. At present, our Digital-Forensics-in-Cybersecurity exam materials are able to motivate you a lot. Our products will help you overcome your laziness. And you will become what you want to be with the help of our Digital-Forensics-in-Cybersecurity learning questions. You can realize and reach your dream. Also, you will have a pleasant learning of our Digital-Forensics-in-Cybersecurity study quiz.

Under the hatchet of fast-paced development, we must always be cognizant of social long term goals and the direction of the development of science and technology. Adapt to the network society, otherwise, we will take the risk of being obsoleted. Our Digital-Forensics-in-Cybersecurity Test Torrent keep a look out for new ways to help you approach challenges and succeed in passing the Digital Forensics in Cybersecurity (D431/C840) Course Exam exam. An ancient Chinese proverb states that "The journey of a thousand miles starts with a single step". To be recognized as the leading international exam bank in the world through our excellent performance, our Digital Forensics in Cybersecurity (D431/C840) Course Exam qualification test are being concentrated on for a long time and have accumulated mass resources and experience in designing study materials.

>> Digital-Forensics-in-Cybersecurity Valid Real Exam <<

**Digital Forensics in Cybersecurity (D431/C840) Course Exam prep**

# material & Digital-Forensics-in-Cybersecurity useful exam pdf & Digital Forensics in Cybersecurity (D431/C840) Course Exam exam practice questions

TestPDF offers a full refund if you cannot pass Digital-Forensics-in-Cybersecurity certification on your first try. This is a risk-free guarantee currently enjoyed by our more than 90,000 clients. We can assure you that you can always count on our braindumps material. We are proud to say that our Digital-Forensics-in-Cybersecurity Exam Dumps material to reduce your chances of failing the Digital-Forensics-in-Cybersecurity certification. Therefore, you are not only saving a lot of time but money as well.

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

Topic	Details
Topic 1	<ul style="list-style-type: none"><li>• 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.</li></ul>
Topic 2	<ul style="list-style-type: none"><li>• 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.</li></ul>
Topic 3	<ul style="list-style-type: none"><li>• 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.</li></ul>
Topic 4	<ul style="list-style-type: none"><li>• 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.</li></ul>
Topic 5	<ul style="list-style-type: none"><li>• 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.</li></ul>

## WGU Digital Forensics in Cybersecurity (D431/C840) Course Exam Sample Questions (Q64-Q69):

### NEW QUESTION # 64

What is a reason to use steganography?

- A. To erase secret data
- B. To save secret data
- C. To highlight secret data
- D. To delete secret data

**Answer: B**

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

Steganography is used to save or embed secret data within another file or medium, allowing covert communication without alerting observers to the presence of the data.

\* The goal is to conceal, not highlight or delete data.

\* It does not erase or delete secret data; instead, it hides it.

This aligns with standard definitions in cybersecurity and forensic literature including NIST's cybersecurity frameworks.

### NEW QUESTION # 65

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

#### Answer: A

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 # 66

A victim of Internet fraud fell for an online offer after using a search engine to find a deal on an expensive software purchase. Once the victim learned about the fraud, he contacted a forensic investigator for help.

Which digital evidence should the investigator collect?

- A. Computer logs
- B. Whois records
- C. Email headers
- D. Virus signatures

#### Answer: A

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

In Internet fraud investigations, computer logs are critical because they provide a record of user activity, including browsing history, downloads, and system events. These logs can help establish a timeline, identify malicious access, and confirm fraudulent transactions.

\* Computer logs may include browser history, system event logs, and application logs that document the victim's interaction with the fraudulent offer.

\* Whois records help identify domain registration details but are secondary evidence.

\* Email headers are relevant if communication via email was part of the fraud but less critical than logs that show direct interaction.

\* Virus signatures are used in malware investigations, not directly relevant to fraud evidence collection.

Reference:According to guidelines by the International Journal of Digital Crime and Forensics and the SANS Institute, capturing logs is essential in building a case for Internet fraud as it provides objective data about the victim's system and activities.

### NEW QUESTION # 67

Which policy is included in the CAN-SPAM Act?

- A. Email sender must provide a method for recipients to opt out of future emails without charge
- B. Email sender must verify the recipient's consent before sending
- C. Email sender must include recipient IP address in the email header
- D. Email sender must encrypt all outgoing emails

#### Answer: A

Explanation:

#### Comprehensive and Detailed Explanation From Exact Extract:

The CAN-SPAM Act requires that commercial emails include a clear and conspicuous mechanism allowing recipients to opt out of receiving future emails. This opt-out method cannot require payment or additional steps that would discourage recipients.

\* The act aims to reduce unsolicited commercial emails and spam.

\* Compliance is critical for lawful email marketing and forensic investigations involving email misuse.

Reference: U.S. federal law and cybersecurity policies reference CAN-SPAM provisions for email communications.

#### NEW QUESTION # 68

Which directory contains the system's configuration files on a computer running Mac OS X?

- A. /cfg
- B. /bin
- C. /etc
- D. /var

**Answer: C**

Explanation:

#### Comprehensive and Detailed Explanation From Exact Extract:

The /etc directory on Unix-based systems, including macOS, contains important system configuration files and scripts. It is the standard location for system-wide configuration data.

\* /var contains variable data like logs and spool files.

\* /bin contains essential binary executables.

\* /cfg is not a standard directory in macOS.

This is standard Unix/Linux directory structure knowledge and is reflected in NIST and forensic references for macOS.

#### NEW QUESTION # 69

.....

Under coordinated synergy of all staff, our Digital-Forensics-in-Cybersecurity guide materials achieved to a higher level of perfection by keeping close attention with the trend of dynamic market. They eliminated stereotypical content from our Digital-Forensics-in-Cybersecurity practice materials. And if you download our Digital-Forensics-in-Cybersecurity study quiz this time, we will send free updates for you one year long since we promise that our customers can enjoy free updates for one year.

**Digital-Forensics-in-Cybersecurity Latest Test Report:** <https://www.testpdf.com/Digital-Forensics-in-Cybersecurity-exam-braindumps.html>

- Exam Digital-Forensics-in-Cybersecurity Materials □ Dumps Digital-Forensics-in-Cybersecurity Download □ Free Sample Digital-Forensics-in-Cybersecurity Questions □ Go to website ↗ www.prepawayexam.com □ ↗ open and search for ➡ Digital-Forensics-in-Cybersecurity □ to download for free □ Prep Digital-Forensics-in-Cybersecurity Guide
- 2026 WGU Digital-Forensics-in-Cybersecurity: Authoritative Digital Forensics in Cybersecurity (D431/C840) Course Exam Valid Real Exam □ Download [ Digital-Forensics-in-Cybersecurity ] for free by simply searching on □ www.pdfvce.com □ ↗ Digital-Forensics-in-Cybersecurity Valid Dumps Sheet
- 2026 WGU Digital-Forensics-in-Cybersecurity: Authoritative Digital Forensics in Cybersecurity (D431/C840) Course Exam Valid Real Exam □ Download [ Digital-Forensics-in-Cybersecurity ] for free by simply entering ✓ www.validtorrent.com □ ✓ □ website □ ↗ Digital-Forensics-in-Cybersecurity Valid Exam Tips
- Digital-Forensics-in-Cybersecurity Reliable Dumps Book □ Free Sample Digital-Forensics-in-Cybersecurity Questions □ □ Prep Digital-Forensics-in-Cybersecurity Guide □ ➡ www.pdfvce.com ↳ is best website to obtain ➡ Digital-Forensics-in-Cybersecurity □ for free download □ Latest Digital-Forensics-in-Cybersecurity Study Materials
- Digital-Forensics-in-Cybersecurity Practice Questions □ Prep Digital-Forensics-in-Cybersecurity Guide □ Digital-Forensics-in-Cybersecurity Reasonable Exam Price □ Open ➡ www.prep4sures.top □ enter ➡ Digital-Forensics-in-Cybersecurity □ and obtain a free download □ Reliable Digital-Forensics-in-Cybersecurity Study Guide
- 2026 Perfect 100% Free Digital-Forensics-in-Cybersecurity – 100% Free Valid Real Exam | Digital-Forensics-in-Cybersecurity Latest Test Report □ Download ➡ Digital-Forensics-in-Cybersecurity ↳ for free by simply entering ↳ www.pdfvce.com ↳ website □ Latest Digital-Forensics-in-Cybersecurity Test Dumps
- Authoritative Digital-Forensics-in-Cybersecurity Valid Real Exam | Digital-Forensics-in-Cybersecurity 100% Free Latest Test Report □ Search for “Digital-Forensics-in-Cybersecurity” and download exam materials for free through ➡ www.examcollectionpass.com □ ↗ ➡ Latest Digital-Forensics-in-Cybersecurity Test Dumps

P.S. Free 2026 WGU Digital-Forensics-in-Cybersecurity dumps are available on Google Drive shared by TestPDF: <https://drive.google.com/open?id=1nd6PPWNPFOoNQbBLqkWK10UqHRMjfVk>