

# Here's the Simple and Quick Way to Pass WGU Digital-Forensics-in-Cybersecurity Exam



P.S. Free 2026 WGU Digital-Forensics-in-Cybersecurity dumps are available on Google Drive shared by RealValidExam: <https://drive.google.com/open?id=12XIGOGzGRUzVa8A7NgVWcdz-3pHZUx7X>

RealValidExam believes in customer satisfaction and strives hard to make the entire WGU Digital-Forensics-in-Cybersecurity exam preparation process simple, smart, and successful. To achieve this objective the RealValidExam is offering the top-rated and real Digital-Forensics-in-Cybersecurity exam questions in three different Digital-Forensics-in-Cybersecurity Exam study material formats. These Digital-Forensics-in-Cybersecurity exam questions formats are WGU Digital-Forensics-in-Cybersecurity PDF dumps files, desktop practice test software, and web-based practice test software.

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

Topic	Details
Topic 1	<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>
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 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 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 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>

## TOP Reliable Digital-Forensics-in-Cybersecurity Test Prep - WGU Digital Forensics in Cybersecurity (D431/C840) Course Exam - High Pass-Rate Actual Digital-Forensics-in-Cybersecurity Test Answers

We own three versions of the Digital-Forensics-in-Cybersecurity exam torrent for you to choose. They conclude PDF version, PC version and APP online version. You can choose the most convenient version of the Digital-Forensics-in-Cybersecurity quiz torrent. The three versions of the Digital-Forensics-in-Cybersecurity test prep boost different strengths and you can find the most appropriate choice. For example, the PDF version is convenient for download and printing and is easy and convenient for review and learning. It can be printed into papers and is convenient to make notes. You can learn the Digital-Forensics-in-Cybersecurity Test Prep at any time or place and repeatedly practice.

### WGU Digital Forensics in Cybersecurity (D431/C840) Course Exam Sample Questions (Q50-Q55):

#### NEW QUESTION # 50

What is one purpose of steganography?

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

**Answer: B**

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 # 51

Which operating system creates a swap file to temporarily store information from memory on the hard drive when needed?

- A. Unix
- **B. Windows**
- C. Linux
- D. Mac

**Answer: B**

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

Windows uses a swap file (commonly calledpagefile.sys) to extend physical memory (RAM) by temporarily storing data from memory to disk when RAM is insufficient. This allows the system to handle more data than the available RAM.

\* Linux and Unix typically use dedicated swap partitions or swap files but refer to them differently and manage them in other ways.

\* Mac OS X uses a paging file system but does not typically use a "swap file" in the Windows sense; it uses dynamic paging files instead.

\* The terminology "swap file" is most commonly associated with Windows.

Reference:Microsoft Windows forensics guidelines and NIST documentation describe the page file's role in virtual memory management in Windows operating systems.

#### NEW QUESTION # 52

Which principle of evidence collection states that access to evidence must be tracked from the time it is seized through its use in court?

- A. Event log
- B. Audit log
- C. Evidence record
- **D. Chain of custody**

**Answer: D**

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

The Chain of Custody (CoC) is the documented and unbroken transfer record of evidence handling, from seizure to presentation in court. It ensures that the evidence has been preserved, controlled, and protected from tampering or alteration.

\* Evidence record documents evidence details but is less formal than CoC.

\* Event log and audit log are system-generated records and do not replace the formal CoC.

\* CoC is a fundamental forensic principle as outlined by NIST SP 800-86 and the Scientific Working Group on Digital Evidence (SWGDE) best practices, ensuring evidence admissibility and reliability in legal proceedings.

### NEW QUESTION # 53

How do forensic specialists show that digital evidence was handled in a protected, secure manner during the process of collecting and analyzing the evidence?

- A. By encrypting all evidence
- B. By deleting temporary files
- C. By performing backups
- **D. By maintaining the chain of custody**

**Answer: D**

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

The chain of custody is a documented, chronological record detailing the seizure, custody, control, transfer, analysis, and disposition of evidence. Maintaining this record proves that the evidence was protected and unaltered, which is essential for court admissibility.

\* Each transfer or access must be logged with date, time, and handler.

\* Breaks in the chain can compromise the legal validity of evidence.

Reference: According to NIST and forensic best practices, the chain of custody documentation is mandatory for reliable evidence handling.

### NEW QUESTION # 54

Which type of storage format should be transported in a special bag to reduce electrostatic interference?

- **A. Magnetic media**
- B. Solid-state drives
- C. Optical discs
- D. Flash drives

**Answer: A**

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

Magnetic media such as hard drives and magnetic tapes are sensitive to electrostatic discharge (ESD), which can damage data. They must be transported in anti-static bags or containers to reduce the risk of electrostatic interference.

\* SSDs and flash drives are less vulnerable to ESD but still benefit from proper packaging.

\* Proper handling protocols prevent unintentional data loss or corruption.

Reference: NIST SP 800-101 and forensic evidence handling standards specify anti-static packaging for magnetic storage media.

### NEW QUESTION # 55

Facing the incoming Digital-Forensics-in-Cybersecurity exam, you may feel stained and anxious, suspicious whether you could pass the exam smoothly and successfully. Actually, you must not impoverish your ambition. Our suggestions are never boggle at difficulties. It is your right time to make your mark. Preparation of exam without effective materials is just like a soldier without gun. You will be feeling be counteracted the effect of tension for our Digital-Forensics-in-Cybersecurity practice dumps can relieve you of the anxious feelings.

[illegible]

What's more, part of that RealValidExam Digital-Forensics-in-Cybersecurity dumps now are free: <https://drive.google.com/open?id=12XIGOGzGRUzVa8A7NgVWcdz-3pHZUx7X>