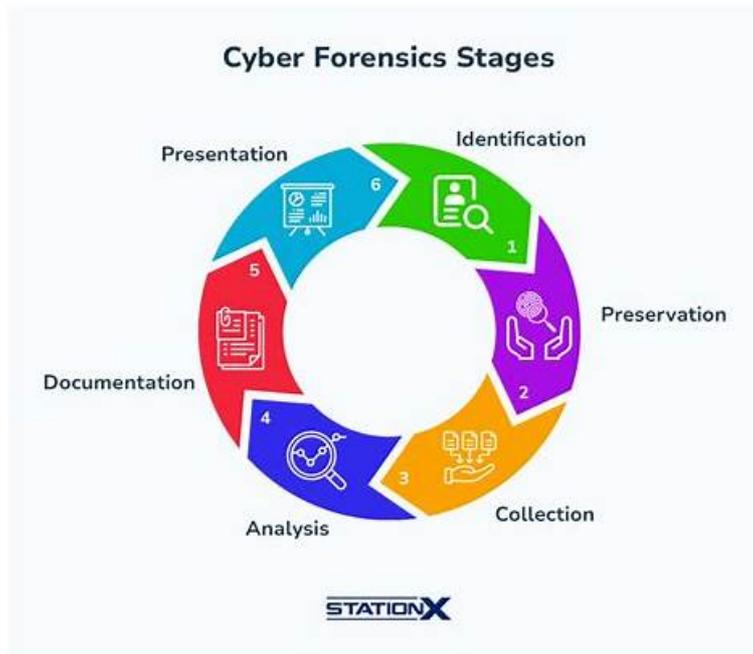


# Digital-Forensics-in-Cybersecurity 模擬対策 & Digital-Forensics-in-Cybersecurity 問題数



Fast2testはあなたに素晴らしい資料を提供するだけでなく、良いサービスも提供してあげます。Fast2testの試験 Digital-Forensics-in-Cybersecurity問題集を購入したら、Fast2testは無料で一年間のアップデートを提供します。すると、あなたがいつでも最新のDigital-Forensics-in-Cybersecurity試験情報を持つことができます。それに、万一の場合、問題集を利用してからやはり試験に失敗すれば、Fast2testは全額返金のことを約束します。こうすれば、まだ何を心配しているのですか。心配する必要がないでしょう。Fast2testは自分の資料に十分な自信を持っているから、あなたもFast2testを信じたほうがいいです。あなたのDigital-Forensics-in-Cybersecurity試験の成功のために、Fast2testをミスしないでください。Fast2testをミスすれば、あなたが成功するチャンスを見逃したということになります。

## WGU Digital-Forensics-in-Cybersecurity 認定試験の出題範囲:

トピック	出題範囲
トピック 1	<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>
トピック 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>
トピック 3	<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>
トピック 4	<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>

- **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.

## &gt;&gt; Digital-Forensics-in-Cybersecurity模擬対策 &lt;&lt;

## 無料PDF Digital-Forensics-in-Cybersecurity模擬対策 & 資格試験におけるリーダーオファー & 公認されたDigital-Forensics-in-Cybersecurity問題数

あなたの社会生活で成功し、高い社会的地位を所有するためには、あなたはいくつかの分野で十分な能力と十分な知識を所有しなければなりません。テストDigital-Forensics-in-Cybersecurity試験に合格すると、これらの目標を達成し、有能であることを証明できます。Digital-Forensics-in-Cybersecurity模擬テストを購入すると、Digital-Forensics-in-Cybersecurity試験に流passに合格し、学習にかかる時間と労力が少なくて済みます。Digital-Forensics-in-Cybersecurityテスト問題の質問と回答は入念に選択されており、重要な情報を簡素化して学習をリラックスして効率的にしています。

### WGU Digital Forensics in Cybersecurity (D431/C840) Course Exam 認定 Digital-Forensics-in-Cybersecurity 試験問題 (Q70-Q75):

#### 質問 # 70

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

正解: A

解説:

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.

#### 質問 # 71

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

正解: B

解説:

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.

### 質問 # 72

Susan was looking at her credit report and noticed that several new credit cards had been opened lately in her name. Susan has not opened any of the credit card accounts herself.

Which type of cybercrime has been perpetrated against Susan?

- A. Cyberstalking
- B. SQL injection
- C. Identity theft
- D. Malware

正解: C

解説:

Comprehensive and Detailed Explanation From Exact Extract:

Identity theft occurs when an attacker unlawfully obtains and uses another person's personal information to open accounts, access credit, or commit fraud. The opening of credit cards without the victim's consent is a classic example.

\* SQL injection is a web application attack method that does not directly relate to this case.

\* Cyberstalking involves harassment via digital means and is unrelated.

\* Malware is malicious software and may be used to facilitate identity theft but is not the crime itself.

Reference:According to the U.S. Federal Trade Commission (FTC) definitions and NIST Cybersecurity Framework, identity theft is defined as the unauthorized use of someone's personal information for fraudulent purposes, perfectly matching Susan's situation.

### 質問 # 73

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

正解: C

解説:

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.

### 質問 # 74

Which Windows component is responsible for reading the boot.ini file and displaying the boot loader menu on Windows XP during the boot process?

- A. Winload.exe
- B. BCD

- C. BOOTMGR
- **D. NTLDR**

正解: D

解説:

Comprehensive and Detailed Explanation From Exact Extract:

NTLDR (NT Loader) is the boot loader for Windows NT-based systems including Windows XP. It reads the boot.ini configuration file and displays the boot menu, initiating the boot process.

\* Later Windows versions (Vista and above) replaced NTLDR with BOOTMGR.

\* Understanding boot components assists forensic investigators in boot process analysis.

Reference: Microsoft technical documentation and forensic training materials outline NTLDR's role in legacy Windows systems.

## 質問 # 75

.....

WGUのDigital-Forensics-in-Cybersecurity試験の認定はIT業種で不可欠な認定で、あなたはWGUのDigital-Forensics-in-Cybersecurity認定試験に合格するのに悩んでいますか。Fast2testは君の悩みを解決できます。Fast2testのサイトは長い歴史を持っていて、WGUのDigital-Forensics-in-Cybersecurity試験トレーニング資料を提供するサイトです。長年の努力を通じて、Fast2testのWGUのDigital-Forensics-in-Cybersecurity認定試験の合格率が100パーセントになっていました。

**Digital-Forensics-in-Cybersecurity問題数:** <https://jp.fast2test.com/Digital-Forensics-in-Cybersecurity-premium-file.html>

- Digital-Forensics-in-Cybersecurity合格問題 □ Digital-Forensics-in-Cybersecurity試験番号 □ Digital-Forensics-in-Cybersecurity試験解説問題 □ { [www.goshiken.com](http://www.goshiken.com) }にて限定無料の▶ Digital-Forensics-in-Cybersecurity □問題集をダウンロードせよ Digital-Forensics-in-Cybersecurity資料勉強
- Digital-Forensics-in-Cybersecurity試験の準備方法 | 検証するDigital-Forensics-in-Cybersecurity模擬対策試験 | 最高のDigital Forensics in Cybersecurity (D431/C840) Course Exam問題数 □ 【 [www.goshiken.com](http://www.goshiken.com) 】にて限定無料の▷ Digital-Forensics-in-Cybersecurity ◁問題集をダウンロードせよ Digital-Forensics-in-Cybersecurityクラムメディア
- Digital-Forensics-in-Cybersecurity試験の準備方法 | 100%合格率Digital-Forensics-in-Cybersecurity模擬対策試験 | 最高のDigital Forensics in Cybersecurity (D431/C840) Course Exam問題数 □ □ Digital-Forensics-in-Cybersecurity □の試験問題は ✓ [www.mogixam.com](http://www.mogixam.com) □ ✓ □で無料配信中Digital-Forensics-in-Cybersecurityオンライン試験
- 有難いDigital-Forensics-in-Cybersecurity | 最新のDigital-Forensics-in-Cybersecurity模擬対策試験 | 試験の準備方法 Digital Forensics in Cybersecurity (D431/C840) Course Exam問題数 □ ▷ [www.goshiken.com](http://www.goshiken.com) ◁サイトで★ Digital-Forensics-in-Cybersecurity □ ★ □の最新問題が使えるDigital-Forensics-in-Cybersecurity模擬トレーニング
- Digital-Forensics-in-Cybersecurity試験の準備方法 | 100%合格率Digital-Forensics-in-Cybersecurity模擬対策試験 | 最高のDigital Forensics in Cybersecurity (D431/C840) Course Exam問題数 □ ➡ [www.jpctestking.com](http://www.jpctestking.com) □から「Digital-Forensics-in-Cybersecurity」を検索して、試験資料を無料でダウンロードしてくださいDigital-Forensics-in-Cybersecurityオンライン試験
- WGU Digital-Forensics-in-Cybersecurity模擬対策: Digital Forensics in Cybersecurity (D431/C840) Course Exam-GoShiken 価値高い 問題数 合格のために □ 【 [www.goshiken.com](http://www.goshiken.com) 】に移動し、“Digital-Forensics-in-Cybersecurity”を検索して無料でダウンロードしてくださいDigital-Forensics-in-Cybersecurity日本語pdf問題
- Digital-Forensics-in-Cybersecurity試験資料 □ Digital-Forensics-in-Cybersecurity模擬トレーニング □ Digital-Forensics-in-Cybersecurity資格問題対応 □ ➡ [www.jpexam.com](http://www.jpexam.com) □から ➡ Digital-Forensics-in-Cybersecurity □を検索して、試験資料を無料でダウンロードしてくださいDigital-Forensics-in-Cybersecurity日本語pdf問題
- Digital-Forensics-in-Cybersecurity試験の準備方法 | 100%合格率Digital-Forensics-in-Cybersecurity模擬対策試験 | 最高のDigital Forensics in Cybersecurity (D431/C840) Course Exam問題数 □ □ [www.goshiken.com](http://www.goshiken.com) □を開いて《Digital-Forensics-in-Cybersecurity》を検索し、試験資料を無料でダウンロードしてくださいDigital-Forensics-in-Cybersecurity過去問
- 信頼的なDigital-Forensics-in-Cybersecurity | 有効的なDigital-Forensics-in-Cybersecurity模擬対策試験 | 試験の準備方法 Digital Forensics in Cybersecurity (D431/C840) Course Exam問題数 □ □ [www.jpshiken.com](http://www.jpshiken.com) □で { Digital-Forensics-in-Cybersecurity }を検索して、無料でダウンロードしてくださいDigital-Forensics-in-Cybersecurity資格問題対応
- Digital-Forensics-in-Cybersecurity試験の準備方法 | 100%合格率Digital-Forensics-in-Cybersecurity模擬対策試験 | 最高のDigital Forensics in Cybersecurity (D431/C840) Course Exam問題数 □ ✓ [www.goshiken.com](http://www.goshiken.com) □ ✓ □の無料ダウンロード ▶ Digital-Forensics-in-Cybersecurity □ページが開きます Digital-Forensics-in-Cybersecurity試験番号
- Digital-Forensics-in-Cybersecurity模擬トレーニング □ Digital-Forensics-in-Cybersecurity試験解説問題 □ Digital-Forensics-in-Cybersecurity模擬トレーニング □ ウェブサイト【 [www.mogixam.com](http://www.mogixam.com) 】から { Digital-Forensics-in-Cybersecurity }を開いて検索し、無料でダウンロードしてくださいDigital-Forensics-in-Cybersecurity真実試験

