Western Governors University (WGU) ITAS2140 D431 Digital Forensics in Cybersecurity Practice Exam (Sample)

Study Guide

BY EXAMZIFY

Everything you need from our exam experts!

Notice: Examzify makes every reasonable effort to obtain from reliable sources accurate, complete, and timely information about this product.

Table of Contents

Introduction

Preparing for a certification exam can feel overwhelming, but with the right tools, it becomes an opportunity to build confidence, sharpen your skills, and move one step closer to your goals. At Examzify, we believe that effective exam preparation isn’t just about memorization, it’s about understanding the material, identifying knowledge gaps, and building the test-taking strategies that lead to success.

This guide was designed to help you do exactly that.

Whether you’re preparing for a licensing exam, professional certification, or entry-level qualification, this book offers structured practice to reinforce key concepts. You’ll find a wide range of multiple-choice questions, each followed by clear explanations to help you understand not just the right answer, but why it’s correct.

The content in this guide is based on real-world exam objectives and aligned with the types of questions and topics commonly found on official tests. It’s ideal for learners who want to:

- **Practice answering questions under realistic conditions,**
- **Improve accuracy and speed,**
- **Review explanations to strengthen weak areas, and**
- **Approach the exam with greater confidence.**

We recommend using this book not as a stand-alone study tool, but alongside other resources like flashcards, textbooks, or hands-on training. For best results, we recommend working through each question, reflecting on the explanation provided, and revisiting the topics that challenge you most.

Remember: successful test preparation isn’t about getting every question right the first time, it’s about learning from your mistakes and improving over time. Stay focused, trust the process, and know that every page you turn brings you closer to success.

Let’s begin.

How to Use This Guide

This guide is designed to help you study more effectively and approach your exam with confidence. Whether you're reviewing for the first time or doing a final refresh, here's how to get the most out of your Examzify study guide:

1. Start with a Diagnostic Review

Skim through the questions to get a sense of what you know and what you need to focus on. Don't worry about getting everything right, your goal is to identify knowledge gaps early.

2. Study in Short, Focused Sessions

Break your study time into manageable blocks (e.g. 30 – 45 minutes). Review a handful of questions, reflect on the explanations, and take breaks to retain information better.

3. Learn from the Explanations

After answering a question, always read the explanation, even if you got it right. It reinforces key points, corrects misunderstandings, and teaches subtle distinctions between similar answers.

4. Track Your Progress

Use bookmarks or notes (if reading digitally) to mark difficult questions. Revisit these regularly and track improvements over time.

5. Simulate the Real Exam

Once you're comfortable, try taking a full set of questions without pausing. Set a timer and simulate test-day conditions to build confidence and time management skills.

6. Repeat and Review

Don't just study once, repetition builds retention. Re-attempt questions after a few days and revisit explanations to reinforce learning.

7. Use Other Tools

Pair this guide with other Examzify tools like flashcards, and digital practice tests to strengthen your preparation across formats.

There’s no single right way to study, but consistent, thoughtful effort always wins. Use this guide flexibly — adapt the tips above to fit your pace and learning style. You've got this!

Questions

1. **Documentary evidence is defined as what type of evidence?**

   A. Physical objects that can be touched and observed

   B. Testimony taken from a witness before trial

   C. Scientific evidence presented in a trial

   D. Data stored in written or electronic form

2. **What certification is specific to the use and mastery of FTK?**

   A. Certified Forensic Computer Examiner (CFCE)

   B. AccessData Certified Examiner

   C. EnCase Certified Examiner

   D. Certified Hacking Forensic Investigator

3. **Which file system is used by Windows 2000 and newer operating systems?**

   A. FAT32

   B. NTFS

   C. FTP32

   D. FAT16

4. **What tool is used to send a test packet to check if a machine is reachable?**

   A. Traceroute

   B. Tracert

   C. Ipconfig

   D. Ping

5. **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. Forensic lab logbooks

   B. Forensic software logs

   C. Chain of custody

   D. Chain of email messages

6. Which file system is supported by Mac?

A. Hierarchical File System Plus (HFS+)

B. Extended File System (Ext)

C. Berkeley Fast File System (FFS)

D. Reiser File System (ReiserFS)

7. Which of the following correctly shows how the instructions in a computer's BIOS are stored?

A. EEPROM

B. RAM

C. ROM

D. PROM

8. Which command would be used in Linux to change file ownership?

A. chmod

B. chown

C. chgrp

D. ls

9. Which of the following statements about 'init' is correct in the context of Unix?

A. It is a search tool in Linux

B. It is responsible for managing system daemons

C. It handles multimedia functions

D. It provides file access controls

10. What term describes any use of another person's identity?

A. Fraud

B. Logic bomb

C. Identity theft

D. Cyberstalking

Answers

1. **D**
2. **B**
3. **B**
4. **D**
5. **C**
6. **A**
7. **A**
8. **B**
9. **B**
10. **C**

Explanations

1. Documentary evidence is defined as what type of evidence?

A. Physical objects that can be touched and observed

B. Testimony taken from a witness before trial

C. Scientific evidence presented in a trial

D. Data stored in written or electronic form

Documentary evidence refers specifically to data that exists in written or electronic form. This includes a wide range of materials such as contracts, emails, reports, photographs, and any records that can provide information relevant to the case at hand. It serves as a crucial piece of evidence in legal contexts since it can be presented to substantiate claims or provide clarity on events. In legal settings, documentary evidence is often valued for its reliability and the ability to verify facts or timelines. Unlike physical objects or scientific evidence, which may require specialized analysis or interpretation, documentary evidence can often be evaluated directly by a judge or jury. This form of evidence is foundational in establishing a record of events, agreements, or conversations that have significant bearing on a case.

2. What certification is specific to the use and mastery of FTK?

A. Certified Forensic Computer Examiner (CFCE)

B. AccessData Certified Examiner

C. EnCase Certified Examiner

D. Certified Hacking Forensic Investigator

The AccessData Certified Examiner certification is specifically designed for individuals who have demonstrated proficiency in using FTK (Forensic Toolkit), which is a software suite developed by AccessData for digital investigations. Obtaining this certification entails mastering the functionalities of FTK, including its capabilities for data acquisition, analysis, and reporting during forensic investigations. The emphasis on the use of FTK in this certification distinguishes it from others that focus on different tools and methodologies in digital forensics. In contrast, the other certifications mentioned are tied to different tools or broader aspects of digital forensics. For instance, the Certified Forensic Computer Examiner focuses on a wide range of forensic principles and practices, while the EnCase Certified Examiner is centered around EnCase software. The Certified Hacking Forensic Investigator also encompasses broader skills in hacking and investigative techniques rather than mastery of FTK specifically. This specificity to FTK usage makes the AccessData Certified Examiner the correct answer for this question.

3. Which file system is used by Windows 2000 and newer operating systems?

A. FAT32

B. NTFS

C. FTP32

D. FAT16

The file system used by Windows 2000 and newer operating systems is NTFS, or New Technology File System. NTFS was introduced to provide advanced features such as improved data storage, security permissions, and support for larger files and volumes compared to its predecessors. It allows for file system journaling, which enhances the integrity and recovery of data in the event of a system failure. NTFS supports additional attributes, such as encryption and disk quotas, which make it more suited for modern computing needs. With the evolution of Windows operating systems, NTFS became the standard file system, reflecting the need for better performance, security, and efficiency in managing files on hard drives. In contrast, FAT32 and FAT16 are older file systems with limitations in terms of file size and overall performance, making them less suitable for contemporary operating systems. FTP32 is not a file system but rather a reference to a protocol related to file transfers, which is unrelated to the question of operating system file system standards. Thus, NTFS stands out as the correct choice for Windows 2000 and newer versions.

4. What tool is used to send a test packet to check if a machine is reachable?

A. Traceroute

B. Tracert

C. Ipconfig

D. Ping

The tool used to send a test packet to check if a machine is reachable is Ping. Designed to send Internet Control Message Protocol (ICMP) Echo Request packets to the target host, Ping measures the time it takes for these packets to reach the destination and return. This helps in determining network connectivity and diagnosing network issues. If the target machine responds, it confirms that the device is reachable over the network. In contrast, Traceroute and Tracert are utilities that trace the path packets take from one device to another, providing insight into the route and the time taken for each hop along the way. These tools are useful for network troubleshooting but do not specifically test reachability in the same direct manner as Ping. Ipconfig is primarily used for network configuration management on Windows operating systems. It displays current TCP/IP network configuration values, including the IP address, subnet mask, and default gateway, but it does not send test packets to check reachability. Thus, Ping's functionality specifically focuses on testing reachability through packet transmission, making it the correct answer to the question.

5. 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. Forensic lab logbooks

B. Forensic software logs

C. Chain of custody

D. Chain of email messages

Forensic specialists demonstrate that digital evidence has been handled in a protected and secure manner through the establishment and maintenance of a chain of custody. The chain of custody is a documented process that outlines who collected the evidence, how it was handled after collection, and the individuals that had access to it throughout the investigation. This ensures that the integrity of the evidence is preserved and that the evidence remains uncontaminated from the point of collection to analysis and presentation in court. Maintaining a detailed chain of custody is crucial for providing transparency and accountability in forensic investigations. It reduces the risk of evidence tampering or contamination and helps establish the reliability and authenticity of the evidence when being examined or presented during legal proceedings. While forensic lab logbooks and forensic software logs can serve important roles in documenting procedures and operations within the forensic environment, they do not provide a comprehensive overview of the handling of specific pieces of evidence as the chain of custody does. The chain of email messages option does not pertain to the physical or logical management of evidence in a forensic context.

6. Which file system is supported by Mac?

A. Hierarchical File System Plus (HFS+)

B. Extended File System (Ext)

C. Berkeley Fast File System (FFS)

D. Reiser File System (ReiserFS)

The Hierarchical File System Plus (HFS+) is the correct answer because it is specifically designed for use with macOS, previously known as Mac OS X. HFS+ is an advanced version of the original HFS, providing enhancements such as support for larger files and more efficient file storage. This file system has been the standard for Apple devices, supporting features like journaling to protect against data corruption and allowing for more complex directory structures. The other file systems listed are not specifically designed for Mac. The Extended File System (Ext) is primarily used by Linux operating systems, Berkeley Fast File System (FFS) is associated with BSD Unix systems, and Reiser File System (ReiserFS) is another file system mainly utilized in Linux environments. Therefore, HFS+ is the only option compatible with macOS, making it the definitive choice in this context.

7. Which of the following correctly shows how the instructions in a computer's BIOS are stored?

A. EEPROM

B. RAM

C. ROM

D. PROM

The correct choice demonstrates that BIOS instructions are indeed stored in EEPROM, which stands for Electrically Erasable Programmable Read-Only Memory. This type of memory allows for the BIOS to be updated or re-flashed when necessary, which is important for maintaining system compatibility and security. EEPROM is non-volatile, meaning it retains data even when the power is turned off, making it suitable for storing firmware like the BIOS that must remain accessible for the computer's startup processes. In comparison, RAM (Random Access Memory) is volatile and loses its contents when the power is turned off, making it unsuitable for storing BIOS instructions. ROM (Read-Only Memory) is more traditional for storing firmware, but it is not as flexible as EEPROM since it typically requires specific methods to update. PROM (Programmable Read-Only Memory) can only be written to once and is not as adaptable for changes as EEPROM. Each of these alternatives does not provide the same level of flexibility or functionality as EEPROM for the purpose of updating BIOS firmware.

8. Which command would be used in Linux to change file ownership?

A. chmod

B. chown

C. chgrp

D. ls

The command used to change file ownership in Linux is the 'chown' command. This command allows a user to specify a new owner for a file or directory, effectively altering its ownership. The syntax typically involves the new owner's username followed by the file or directory name, enabling a smooth transition of ownership rights which can be important for file access and management in a multi-user system. For instance, when a file is created by a user, that user becomes the owner of the file. If there's a need for another user to take over ownership for collaboration or administrative purposes, 'chown' facilitates this process. Understanding file ownership is crucial, as it directly relates to security and access permissions within a Linux environment. While other options serve important functions—like 'chmod' for changing file permissions, 'chgrp' for changing the group associated with a file, and 'ls' for listing files—only 'chown' specifically targets the alteration of file ownership.

9. Which of the following statements about 'init' is correct in the context of Unix?

A. It is a search tool in Linux

B. It is responsible for managing system daemons

C. It handles multimedia functions

D. It provides file access controls

In the context of Unix and its derivatives like Linux, 'init' is a crucial system process that has the primary role of managing system daemons. When the operating system boots, 'init' is one of the first processes that is started by the kernel and it sets up the user space by launching services and managing processes. It acts as the parent process for all other processes on the system. Its responsibilities include starting system services (daemons), managing the boot process, and handling run levels, which determine the state of the machine such as whether it is in single-user mode, multi-user mode, or graphical mode. Understanding the significance of 'init' in managing daemons is essential because these daemons are background processes that perform various tasks necessary for system operation, such as handling network requests, performing scheduled tasks, or managing hardware resources. This foundational role of 'init' is vital for the stability and functionality of the Unix system environment.

10. What term describes any use of another person's identity?

A. Fraud

B. Logic bomb

C. Identity theft

D. Cyberstalking

The term that describes any use of another person's identity is identity theft. This concept encompasses various activities where someone assumes the identity of another individual without their consent, typically for fraudulent purposes. Identity theft can lead to financial loss for the victim, damage to their credit, and significant emotional distress. This definition captures the broader scope of identity-related crimes where someone's personal information—such as social security numbers, credit card information, or bank details—is exploited. The implications of identity theft are severe in the realm of cybersecurity, especially as it involves the unauthorized use of personal data. Fraud generally pertains to deceptive practices that lead to financial or personal gain but does not exclusively refer to identity-related crimes. A logic bomb is a type of malware that activates under specific conditions to disrupt system operations, while cyberstalking involves harassment and threats that can use technology but do not specifically entail the use of another person’s identity.

Next Steps

Congratulations on reaching the final section of this guide. You've taken a meaningful step toward passing your certification exam and advancing your career.

As you continue preparing, remember that consistent practice, review, and self-reflection are key to success. Make time to revisit difficult topics, simulate exam conditions, and track your progress along the way.

If you need help, have suggestions, or want to share feedback, we’d love to hear from you. Reach out to our team at hello@examzify.com.

Or visit your dedicated course page for more study tools and resources:

https://wgu-itas2140-d431.examzify.com

We wish you the very best on your exam journey. You've got this!