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

Study Guide

Everything you need from our exam experts!

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. 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.

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. 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. Where are kernel images commonly kept?

A. The /boot Directory

B. The /var/spool Directory

C. The /proc Directory

D. The /usr Directory

2. What is the main purpose of a firewall in a network?

A. To block all incoming traffic

B. To monitor and control network traffic

C. To encrypt communication

D. To provide user authentication

3. What is meant by symmetric cryptography?

A. The art and science of writing hidden messages

B. Using one key to encrypt and another to decrypt

C. Using the same key for both encryption and decryption

D. Substituting letters in an alphabet for encryption

4. In FAT and NTFS file systems, a _____ is used to map files to specific clusters where they are stored on the disk.

A. table

B. partition

C. node

D. cluster

5. Which starting-point forensic certification covers the general principles and techniques of forensics, but not specific tools such as EnCase or FTK?

A. High Tech Crime Network Certifications

B. EC Council Certified Hacking Forensic Investigator

C. Global Information Assurance Certification Certifications

D. (ISC)2 CISSP certification

6. Which concept requires that scientific evidence presented in a trial must be peer-reviewed?

A. Documentary evidence

B. The Daubert Standard

C. Demonstrative evidence

D. Consistent scientific manner

7. How is transposition defined in the context of cryptography?

A. Swapping of blocks of ciphertext

B. Determination of whether a file hides other information

C. Art and science of writing hidden messages

D. Method of deriving a cryptographic key

8. Which search tool is commonly used in Linux/UNIX environments for searching text within files?

A. inode

B. init

C. scalpel

D. grep

9. The _____ is a unique identification number developed by the U.S. Federal Communications Commission (FCC) to identify cell phones.

A. integrated circuit card identifier (ICCID)

B. international mobile equipment identity (IMEI) number

C. home location register (HLR)

D. electronic serial number (ESN)

10. What act contains many provisions about recordkeeping and destruction of electronic records relating to publicly held companies?

A. Sarbanes-Oxley Act of 2002

B. Computer Security Act of 1987

C. Federal Privacy Act of 1974

D. Privacy Protection Act of 1980

Answers

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

Explanations

1. Where are kernel images commonly kept?

A. The /boot Directory

B. The /var/spool Directory

C. The /proc Directory

D. The /usr Directory

Kernel images are commonly kept in the /boot directory of a Unix-like operating system. This directory is specifically designated for files that are essential for the boot process, including the kernel itself, which is necessary for the system to start up and run. The kernel image contains the core components of the operating system and is crucial for managing system resources and hardware. Other directories mentioned, such as /var/spool, /proc, and /usr, serve different purposes. The /var/spool directory is used for storing files that are queued for processing, such as print jobs. The /proc directory contains virtual files that provide information about system processes and hardware in real-time, but it does not store the kernel image. The /usr directory is typically used for user applications and files, separate from the core operating system files found in /boot.

2. What is the main purpose of a firewall in a network?

A. To block all incoming traffic

B. To monitor and control network traffic

C. To encrypt communication

D. To provide user authentication

The main purpose of a firewall in a network is to monitor and control network traffic. Firewalls serve as a security barrier between a trusted internal network and untrusted external networks, typically the internet. They evaluate the incoming and outgoing traffic based on predefined security rules and policies, allowing or blocking data packets based on that assessment. This capability helps to prevent unauthorized access and attacks while permitting legitimate communication. By inspecting traffic patterns, firewalls can also detect potential threats, such as intrusions or malicious activities, and take action to mitigate them. In addition, while other functions such as user authentication and encryption play significant roles in overall network security, they do not define the primary role of a firewall. Firewalls are specifically designed to handle traffic control rather than to provide encryption or perform user authentication.

3. What is meant by symmetric cryptography?

A. The art and science of writing hidden messages

B. Using one key to encrypt and another to decrypt

C. Using the same key for both encryption and decryption

D. Substituting letters in an alphabet for encryption

Symmetric cryptography refers to a method of encryption where the same key is utilized for both the processes of encryption and decryption. This means that the sender and the recipient share a single key that is used to lock and unlock the information exchanged. The primary advantage of this approach is its efficiency; symmetric algorithms are generally faster than asymmetric ones, making them suitable for encrypting large amounts of data. In symmetric cryptography, both parties must keep the key confidential to ensure the security of the communication, as anyone possessing the key can decrypt the messages. This aspect highlights its reliance on secure key management practices—if the key is compromised, so too is the confidentiality of the encrypted data. The other options describe different concepts. Writing hidden messages is more related to steganography rather than cryptography, while using two keys (one for encryption and another for decryption) refers to asymmetric cryptography. Substituting letters for encryption pertains to classical ciphers, which can be a form of symmetric cryptography but does not encompass the broader principle of using the same key for both processes. Therefore, the definition of symmetric cryptography is best captured by the choice indicating the use of the same key for both encryption and decryption.

4. In FAT and NTFS file systems, a _____ is used to map files to specific clusters where they are stored on the disk.

A. table

B. partition

C. node

D. cluster

In FAT (File Allocation Table) and NTFS (New Technology File System) file systems, a table is utilized to maintain a mapping of files to the specific clusters on the disk where those files are stored. For FAT file systems, the File Allocation Table itself serves this purpose by indicating which clusters are in use, which are free, and how files are segmented across the disk. This table effectively tracks the allocation status of each cluster, allowing the operating system to access files efficiently by following the chain of allocated clusters. In the case of NTFS, a similar principle applies, although it employs a more complex structure. NTFS uses a Master File Table (MFT), which contains detailed information about every file and directory on the volume, including their locations. The MFT entries specify where the actual data of the file resides on the disk, allowing for quick retrieval and management of files. Therefore, the use of a table in both of these file systems is crucial for the organization, storage, and retrieval of data, making this the correct answer to the question posed.

5. Which starting-point forensic certification covers the general principles and techniques of forensics, but not specific tools such as EnCase or FTK?

A. High Tech Crime Network Certifications

B. EC Council Certified Hacking Forensic Investigator

C. Global Information Assurance Certification Certifications

D. (ISC)2 CISSP certification

The EC Council Certified Hacking Forensic Investigator is designed to provide a foundation in the general principles and techniques involved in digital forensics without delving into the specifics of particular forensic tools, such as EnCase or FTK. This certification encompasses the essential concepts of evidence collection, preservation, analysis, and presentation within a forensic context, making it an appropriate starting point for those looking to enter the field of digital forensics. On the other hand, the other certifications mentioned either focus on specific tools or have broader scopes that include more advanced topics or specific skill sets. Therefore, the Certified Hacking Forensic Investigator is particularly aligned with the objective of introducing foundational forensic principles without the complication of tool-specific training.

6. Which concept requires that scientific evidence presented in a trial must be peer-reviewed?

A. Documentary evidence

B. The Daubert Standard

C. Demonstrative evidence

D. Consistent scientific manner

The Daubert Standard is a legal criterion used to determine the admissibility of expert witness testimony and scientific evidence in court. It was established in the case of Daubert v. Merrell Dow Pharmaceuticals, Inc. and articulates that for scientific evidence to be considered valid and credible, it must be subjected to peer review and publication in reputable scientific journals. This peer review process ensures that the methodology is sound, the findings can be replicated, and that the evidence is generally accepted within the relevant scientific community. In the context of digital forensics and cybersecurity, adhering to the Daubert Standard is crucial for ensuring that any scientific analysis—including forensic reports and expert testimony—can withstand scrutiny in a legal setting. This standard helps maintain integrity in the judicial process by ensuring that the scientific evidence presented is both reliable and relevant.

7. How is transposition defined in the context of cryptography?

A. Swapping of blocks of ciphertext

B. Determination of whether a file hides other information

C. Art and science of writing hidden messages

D. Method of deriving a cryptographic key

Transposition in cryptography refers specifically to the method of rearranging the positions of characters or groups of characters in the plaintext to create the ciphertext. This restructuring is achieved through specific algorithms that maintain the original letters and their frequency but alter their order. By swapping blocks of ciphertext, the intended message remains obscured to unauthorized parties while still being recoverable through the appropriate decryption process. This technique is fundamental to various classical cipher methods, such as the columnar transposition cipher. By rearranging the order of the characters, transposition adds a level of complexity that can effectively protect the data against straightforward analysis. The key used in transposition ciphers often dictates the pattern or method in which the rearrangement occurs, making understanding this concept essential for analyzing cryptographic techniques effectively.

8. Which search tool is commonly used in Linux/UNIX environments for searching text within files?

A. inode

B. init

C. scalpel

D. grep

The choice of grep as the correct tool for searching text within files in Linux/UNIX environments is well-founded due to its specific design and functionality. Grep stands for "Global Regular Expression Print," and it is engineered to search through text using regular expressions, making it powerful and versatile for finding specific patterns within files. Grep operates efficiently by scanning files line by line and matching patterns, allowing users to quickly retrieve lines of text that contain specified strings or regex patterns. This capability is fundamental for system administrators, developers, and anyone working in a UNIX-like environment who needs to search through large amounts of data efficiently. In contrast, other options listed do not serve this purpose. For example, inode refers to a data structure on a filesystem that stores information about a file but does not perform text searches. Init is a system and service manager for UNIX-like systems, responsible for starting processes during boot time, and is unrelated to text searching tasks. Scalpel, though a data recovery tool, is more focused on file carving and recovery processes rather than searching for text within existing files. Thus, grep is specifically tailored for the task detailed in the question, making it the most suitable and commonly used tool for searching text within files in a Linux/UNIX environment

9. The _____ is a unique identification number developed by the U.S. Federal Communications Commission (FCC) to identify cell phones.

A. integrated circuit card identifier (ICCID)

B. international mobile equipment identity (IMEI) number

C. home location register (HLR)

D. electronic serial number (ESN)

The correct response is that the unique identification number developed by the U.S. Federal Communications Commission (FCC) to identify cell phones is the electronic serial number (ESN). The ESN is a specific number assigned to a CDMA (Code Division Multiple Access) phone, which serves as a unique identifier for that device on a mobile network. It is used primarily for billing and network management purposes, ensuring that the network can track device usage and authenticate connections. The ESN is critical in identifying devices on a telecom network, enabling service providers to manage and secure communication services effectively. Unlike the other identifiers mentioned, the ESN is primarily associated with CDMA technology. In contrast, other options like the integrated circuit card identifier (ICCID) are used for identifying SIM cards, not devices directly; the international mobile equipment identity (IMEI) number serves as a unique identifier for GSM (Global System for Mobile Communications) devices but is not specifically issued by the FCC; and the home location register (HLR) is a database used in mobile networks to store information about subscribers, such as their location and subscription details, rather than serving as a unique identifier for smartphones.

10. What act contains many provisions about recordkeeping and destruction of electronic records relating to publicly held companies?

A. Sarbanes-Oxley Act of 2002

B. Computer Security Act of 1987

C. Federal Privacy Act of 1974

D. Privacy Protection Act of 1980

The Sarbanes-Oxley Act of 2002 is significant in establishing strict requirements for recordkeeping and the destruction of electronic records for publicly held companies. This legislation was enacted in response to corporate scandals and aimed to protect shareholders by improving the accuracy and reliability of corporate disclosures. One of the key provisions of the Sarbanes-Oxley Act is the requirement that companies maintain certain records for a minimum period and ensure their integrity. This includes emails, financial data, and other critical records. The act enforces strict penalties for the destruction of records that are required to be maintained, reinforcing the importance of proper data management in corporate governance. The other acts mentioned focus on different aspects of regulation. The Computer Security Act of 1987 is primarily concerned with the security of federal computer systems but does not specifically address recordkeeping for publicly held companies. The Federal Privacy Act of 1974 emphasizes the privacy of personal information held by government agencies rather than corporate practices. Lastly, the Privacy Protection Act of 1980 deals with the limitations on police searches of newsrooms and the protection of journalistic materials, rather than corporate recordkeeping. Thus, the Sarbanes-Oxley Act is the correct answer as it specifically targets the governance and management of

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!