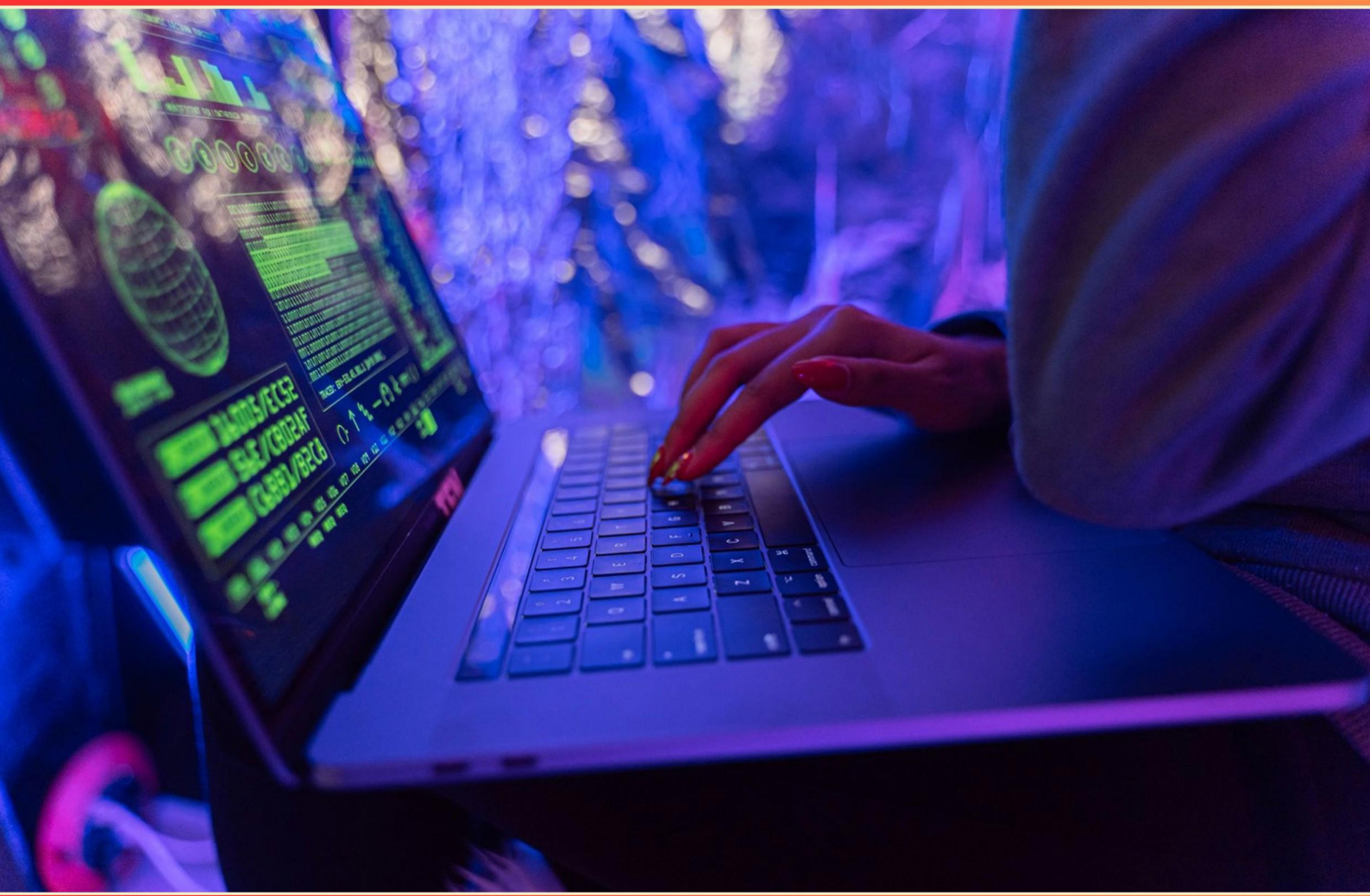
COMPUTER HACKING FORENSIC INVESTIGATOR (CHFI) V11 PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://chfiv11.examzify.com

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. **Which file should be used to restore archived email messages for someone using Microsoft Outlook?**

   A. Outlook bak

   B. Outlook ost

   C. Outlook NK2

   D. Outlook pst

2. **To determine source, nature, and time of an attack from Application and Web server logs, you should:**

   A. Analyzing log files

   B. Analyzing SAM file

   C. Analyzing rainbow tables

   D. Analyzing hard disk boot records

3. **The newer Macintosh Operating System (MacOS X) is based on which of the following?**

   A. OS/2

   B. BSD Unix

   C. Windows

   D. Linux

4. **If you discover a criminal act while investigating a corporate policy abuse, it becomes a public-sector investigation and should be referred to law enforcement?**

   A. True

   B. False

   C. Not applicable

   D. Cannot say

5. **During the cataloging of digital evidence, what is the primary objective?**

   A. Make bit-stream images of all hard drives

   B. Preserve evidence integrity

   C. Not remove the evidence from the scene

   D. Not allow the computer to be turned off

6. During a security audit, a tester disguised as a technician follows employees into restricted areas, enabling access to the server room. What attack type is this?

A. Fuzzing

B. Tailgating

C. Backtrapping

D. Man trap attack

7. In Linux forensic imaging, what would the command dcfldd if=/dev/zero of=/dev/hda bs=4096 conv=noerror, sync accomplishes?

A. Low-level format

B. Fill the disk with 4096 zeros

C. Copy files from the master disk to the slave disk on the secondary IDE controller

D. Fill the disk with zeros

8. DNS poisoning primarily results in wrong responses from which component?

A. The local DNS resolver cache

B. Root DNS servers

C. Authoritative DNS servers

D. DNS forwarders

9. In social engineering training, which principle was demonstrated when an attacker leverages a superior's name to obtain credentials?

A. Social Validation

B. Friendship/Liking

C. Scarcity

D. Reciprocation

10. Which statement is NOT part of disk imaging tool requirements?

A. Not change the original content

B. Log I/O errors in an accessible form

C. Withstand peer review

D. Should not compute a hash value for the complete bit stream copy

Answers

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

Explanations

1. Which file should be used to restore archived email messages for someone using Microsoft Outlook?

A. Outlook bak

B. Outlook ost

C. Outlook NK2

D. Outlook pst

Outlook stores local mail data in PST files, which are used for personal storage and archiving. When messages are archived, they are typically saved in a PST file (often named Archive.pst). To restore those archived messages, you open or import that PST file in Outlook, which adds the archived emails back to the mailbox view. An OST file is a cached offline copy of a mailbox from an Exchange/IMAP account, and it isn't meant for restoring archived messages. NK2 is just the nickname cache for autocomplete, not mail data. A .bak is simply a backup copy and would only be used if you have a backup of a PST and need to recover from it, but it's not the standard archive file Outlook uses for restoring archived messages.

2. To determine source, nature, and time of an attack from Application and Web server logs, you should:

A. Analyzing log files

B. Analyzing SAM file

C. Analyzing rainbow tables

D. Analyzing hard disk boot records

Analyzing log files from applications and web servers is the most effective way to determine where an attack came from, what the attacker did, and when it happened. Logs capture timestamps, source IPs, requested resources, response codes, user agents, and error messages. By examining these records, you can identify the origin (the source IP or proxy), the nature of the attack (for example, repeated login failures, unusual URLs, SQL injection patterns, or scripted probes), and the sequence of events (using timestamps to build a timeline). Correlating entries across web and application logs, and across different systems like firewalls, strengthens attribution and timing. Ensuring synchronized clocks and preserving log integrity are important for credible reconstruction. Other data types don't provide the same forensic value for this task: the SAM file contains user account information and security metadata, not attack activity; rainbow tables are used for password cracking rather than documenting events; boot records relate to the system's startup sequence and don't reflect ongoing network activity.

3. The newer Macintosh Operating System (MacOS X) is based on which of the following?

A. OS/2

B. BSD Unix

C. Windows

D. Linux

MacOS X is built on a Unix-based foundation, specifically BSD Unix. The kernel (XNU) is a hybrid that combines Mach with BSD components, and the Darwin layer provides the open-source core that includes BSD-style userland utilities and interfaces. This Unix lineage gives MacOS X its POSIX compatibility and many familiar Unix tools, even though its GUI was shaped by NeXTSTEP. Because of this, MacOS X is not based on OS/2, Windows, or Linux—the direct lineage is BSD Unix.

4. If you discover a criminal act while investigating a corporate policy abuse, it becomes a public-sector investigation and should be referred to law enforcement?

A. True

B. False

C. Not applicable

D. Cannot say

When you uncover a criminal act during an internal investigation, the matter shifts from policy review to law enforcement territory. Criminal offenses are handled by authorities empowered to investigate, arrest, and prosecute; internal teams don't have the authority to pursue criminal charges or conduct formal criminal proceedings. Because evidence in criminal cases must be collected and preserved under proper legal procedures, you should promptly escalate the issue to law enforcement and coordinate with corporate counsel to report it. Preserve and document all evidence with a clear chain of custody, provide investigators with access to relevant materials, and follow legal and regulatory requirements for reporting. This approach protects the integrity of the investigation, helps ensure admissibility of evidence, and aligns with legal and regulatory expectations.

5. During the cataloging of digital evidence, what is the primary objective?

A. Make bit-stream images of all hard drives

B. Preserve evidence integrity

C. Not remove the evidence from the scene

D. Not allow the computer to be turned off

The main concept being tested is preserving evidence integrity. When cataloging digital evidence, the goal is to create a precise, verifiable record of what was found, where it came from, its condition, and how it has been handled, so the evidence remains unchanged and trustworthy from collection to presentation. This includes documenting metadata (such as device type and identifiers), recording the chain of custody, and using hash values to prove the data hasn't been altered. While other actions like imaging drives or keeping a system powered on are part of the broader process, the cataloging step specifically focuses on ensuring the evidence remains authentic and traceable.

6. During a security audit, a tester disguised as a technician follows employees into restricted areas, enabling access to the server room. What attack type is this?

A. Fuzzing

B. Tailgating

C. Backtrapping

D. Man trap attack

Tailgating is the act of gaining unauthorized entry by closely following an authorized person into a restricted area. In this scenario, the tester uses a disguise as a technician and relies on the legitimate employee's presence to slip past access controls into the server room. It's a social engineering breach that targets human behavior and the tendency to not challenge someone who appears to belong, rather than bypassing a technical system directly. Fuzzing, by contrast, is a software testing technique that bombards inputs to find bugs, not a physical intrusion. Backtrapping isn't a standard term for this context, and a man trap describes a controlled entry designed to prevent tailgating through mechanical means; the situation here centers on the social lapse of following someone through the door, which is tailgating.

7. In Linux forensic imaging, what would the command dcfldd if=/dev/zero of=/dev/hda bs=4096 conv=noerror, sync accomplishes?

A. Low-level format

B. Fill the disk with 4096 zeros

C. Copy files from the master disk to the slave disk on the secondary IDE controller

D. Fill the disk with zeros

The command is overwriting the entire disk with zeros by using a stream of zero bytes as input. /dev/zero provides an endless supply of zeros, and writing to the destination device writes those zeros across the whole drive. The block size of 4096 bytes just determines how many bytes are processed per I/O operation. The options conv=noerror,sync ensure the operation keeps going if any read errors occur and pads any partial block with zeros so every write is a full 4KB block. The net effect is wiping the disk by filling it with zeros, which is different from a true low-level format and not about copying data from another disk. This is a zero-fill wipe.

8. DNS poisoning primarily results in wrong responses from which component?

A. The local DNS resolver cache

B. Root DNS servers

C. Authoritative DNS servers

D. DNS forwarders

DNS poisoning works by tricking the local DNS resolver into storing a false mapping of a domain name to an IP address. When a user asks for a domain, the recursive resolver evaluates the request and caches the answer it receives. If an attacker can inject a spoofed, seemingly legitimate response during the query window, the resolver may store that malicious IP in its cache. Later requests for the same domain are answered from the resolver's cache with the incorrect IP, sending the user to the attacker's site instead of the legitimate one. The TTL controls how long that poisoned entry stays in the cache, so the incorrect result can persist until it expires. Root DNS servers and authoritative servers hold source-of-truth data for domains, and poisoning them would require compromising those upstream systems themselves, which is far more difficult and would affect services globally. DNS forwarders simply relay queries to upstream resolvers; poisoning them is not the typical mechanism by which end users receive wrong answers—the user-facing impact most often comes from the poisoned cache in the local resolver.

9. In social engineering training, which principle was demonstrated when an attacker leverages a superior's name to obtain credentials?

A. Social Validation

B. Friendship/Liking

C. Scarcity

D. Reciprocation

Leveraging a superior's name taps into the reciprocation instinct. When someone signals backing by citing a higher-up, others feel obligated to help and to return the perceived favor or support. The request seems endorsed by authority, which lowers resistance and makes it more likely the target will comply to maintain goodwill or avoid disappointing the supervisor. It's not primarily about liking someone or about following what many people are doing, nor about scarcity; it's about the urge to reciprocate and assist someone who appears to have authority behind them. In practice, verify such requests through independent channels rather than acting on the stated authority alone.

10. Which statement is NOT part of disk imaging tool requirements?

A. Not change the original content

B. Log I/O errors in an accessible form

C. Withstand peer review

D. Should not compute a hash value for the complete bit stream copy

In forensic disk imaging, the tool must keep the original data intact, provide a clear audit trail, and be capable of withstanding scrutiny by others. Not changing the original content means the imaging process should be read-only or use a write blocker to prevent any alteration of evidence. Logging I/O errors in an accessible form creates an auditable record of what happened during the imaging, which is essential for later validation and chain-of-custody reviews. Withstanding peer review ensures that the method and results are reproducible and trusted by the forensic community. Computing a hash value for the complete bit stream copy is a standard part of this process because it allows you to verify that the image exactly matches the source and remains unchanged over time. Saying you should not compute a hash conflicts with that critical integrity check. Therefore the statement about not computing a hash is not part of the proper disk-imaging requirements.

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://chfiv11.examzify.com

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