Wireshark Block 5 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. Is port scanning easy for the adversary?

A. Not Sure

B. Sometimes

C. Yes

D. No

2. Which operator is used to require both conditions in a display filter?

A. ||

B. +

C. --

D. &&

3. How do you add a protocol-specific color rule for a particular host?

A. Open Coloring Rules and set a color for ip.addr 10.0.0.5

B. Add a color rule to all traffic

C. Use a global default color

D. Open Coloring Rules, add a rule like ip.addr == 10.0.0.5, and assign a color

4. What is the start-of-image marker sequence commonly associated with JPEG files?

A. FF D8 FF E0

B. MZ

C. 89 50 4E 47

D. 25 50 44 46

5. In Wireshark, which action displays the HTTP conversation for a specific TCP stream and results in a display filter like tcp.stream eq <n>?

A. Right-click and choose Follow HTTP Stream

B. Apply display filter tcp.stream eq <n>

C. Decode As

D. Follow TCP Stream

6. Which path allows decrypting the SSL stream if a key is available?

A. Right click -> Follow SSL Stream

B. Analyze ->Follow -> TLS Stream

C. Right click -> Follow UDP Stream

D. Analyze ->Expert Info

7. How would you spot a large HTTP response with a small header?

A. Filter for http and check the host header value.

B. Inspect the Content-Length or Transfer-Encoding in the HTTP response and view the payload size via Follow HTTP Stream.

C. Use the Protocol Hierarchy to estimate data amount.

D. Look at the DNS response and compare to request ID.

8. What information does the Packet Bytes pane display?

A. It shows the raw hex and ASCII representation of the selected packet

B. It displays a graphical representation of the packet protocols

C. It lists all protocol fields parsed by the dissectors

D. It provides a packet summary for the capture

9. Which path in Wireshark would you use to export a summary of captures to CSV?

A. Statistics → Protocol Hierarchy

B. File → Open

C. Statistics → Summary and export

D. Edit → Preferences

10. During port scanning, what type of information is commonly identified?

A. Addressing, Routing, Version Numbers, Patch Levels, Protocols/Services Running

B. Usernames And Passwords

C. Physical Environment

D. Weather Data

Answers

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

Explanations

1. Is port scanning easy for the adversary?

A. Not Sure

B. Sometimes

C. Yes

D. No

Port scanning is a basic reconnaissance activity that maps which ports are open on a host and what services might be running. It's easy for an adversary because automated tools can scan large address spaces quickly, and many devices have services listening on well-known ports, so open ports are often apparent from simple probes. Even when some traffic is filtered, many scans still yield useful information, and banners or fingerprinting can reveal software versions and potential vulnerabilities for targeted follow-up. Defensive measures exist, but the general reality is that this step is relatively low effort, making port scanning easy for attackers.

2. Which operator is used to require both conditions in a display filter?

A. ||

B. +

C. --

D. &&

In display filters, to require both conditions you use the logical AND operator, written as &&. This makes a packet match only if every condition separated by && is true—for example, ip.addr == 192.168.1.1 && tcp.dstport == 80 will pass only when both the IP address and the destination port match. If you used the OR operator (||), a packet would pass as long as either condition is true, which isn't the same as requiring both. The other symbols listed aren't used to connect conditions for an AND relationship in display filters, so they don't express the required intersection.

3. How do you add a protocol-specific color rule for a particular host?

A. Open Coloring Rules and set a color for ip.addr 10.0.0.5

B. Add a color rule to all traffic

C. Use a global default color

D. Open Coloring Rules, add a rule like ip.addr == 10.0.0.5, and assign a color

Coloring rules in Wireshark work by attaching a color to packets that match a filter expression. To highlight a specific host, you create a rule whose condition identifies packets involving that host. Using ip.addr matches either source or destination IP, so ip.addr == 10.0.0.5 captures all traffic to or from that host. Then assign a color to that rule. This makes those packets stand out in the capture, regardless of protocol, which is useful for quickly spotting all activity from that host. If you wanted to focus on a particular protocol for that host, you could refine the rule to include a protocol condition, such as http and ip.addr == 10.0.0.5, but the method remains the same: create a coloring rule with a matching expression and assign a color. The other options would color broader traffic or not target the host specifically, so they don't provide the targeted highlighting.

4. What is the start-of-image marker sequence commonly associated with JPEG files?

A. FF D8 FF E0

B. MZ

C. 89 50 4E 47

D. 25 50 44 46

Recognizing file signatures and how a JPEG file begins is what this is about. A JPEG starts with a Start of Image marker, which is the two-byte sequence 0xFF 0xD8. Often the next marker is the APP0 segment, 0xFF 0xE0, which is commonly followed by the "JFIF" header. So the sequence FF D8 FF E0 identifies the start of a JPEG file. The other options are signatures for different file formats: MZ marks Windows executable files, 89 50 4E 47 is the PNG signature, and 25 50 44 46 is the PDF signature.

5. In Wireshark, which action displays the HTTP conversation for a specific TCP stream and results in a display filter like tcp.stream eq <n>?

A. Right-click and choose Follow HTTP Stream

B. Apply display filter tcp.stream eq <n>

C. Decode As

D. Follow TCP Stream

Following the HTTP conversation is the way to see the complete request and response exchange for a single TCP connection in a neatly formatted view. When you right-click an HTTP packet and choose Follow HTTP Stream, Wireshark reconstructs the application-layer dialogue for that TCP stream and, in the process, applies a display filter like tcp.stream eq <n> so only that stream remains visible in the main timeline. This makes it easy to examine the exact HTTP headers, payloads, and the sequence of requests and responses for that connection. Other options don't provide the same combination. Simply applying a display filter tcp.stream eq <n> isolates the stream but doesn't present the HTTP conversation in its structured, readable form. Decode As changes how a payload is interpreted but doesn't specifically reconstruct or isolate the HTTP dialogue. Following the TCP Stream shows the raw TCP payload reassembly for a stream, but it isn't tailored to HTTP and may not automatically present the HTTP conversation with the same focused filter.

6. Which path allows decrypting the SSL stream if a key is available?

A. Right click -> Follow SSL Stream

B. Analyze ->Follow -> TLS Stream

C. Right click -> Follow UDP Stream

D. Analyze ->Expert Info

The key idea is how to view decrypted TLS data by reconstructing the TLS conversation from the captured packets. If the necessary keys are available, Wireshark can decrypt the TLS stream and present the plaintext by following the TLS/SSL stream. The quickest way is to right-click on a packet that belongs to the TLS conversation and choose the stream-follow option, typically labeled Follow SSL Stream (or Follow TLS Stream in newer versions). This opens a window with the reassembled, decrypted data in the correct sequence, so you can read the application-layer messages. Other options won't reveal the decrypted TLS payload: following a UDP stream is for UDP traffic, and Expert Info or using the Analyze menu without the stream-follow action won't reconstruct the TLS conversation. Note that the exact label may vary by version, but the action of following the TLS stream from a TLS packet is the method that exposes the decrypted content when keys are available.

7. How would you spot a large HTTP response with a small header?

A. Filter for http and check the host header value.

B. Inspect the Content-Length or Transfer-Encoding in the HTTP response and view the payload size via Follow HTTP Stream.

C. Use the Protocol Hierarchy to estimate data amount.

D. Look at the DNS response and compare to request ID.

The main idea is that the size of an HTTP response's body is determined by the headers that accompany it, or by how the body is encoded. If the response has a small header, you can still determine or verify the actual payload size by checking the HTTP headers for size information and by reconstructing the body. Look at the Content-Length field in the HTTP response header to see the exact number of bytes in the body. If this header is present, it tells you precisely how large the payload is. If the response uses Transfer-Encoding, especially chunked encoding, there may not be a single Content-Length value. In that case, you need to reconstruct the full payload to know its size. Wireshark's Follow HTTP Stream tool is designed for this: it rebuilds the entire HTTP message, allowing you to see exactly how many bytes make up the payload and confirming whether the response is large despite a small header. So, by checking Content-Length or Transfer-Encoding and then using Follow HTTP Stream to view the reconstructed payload, you can accurately spot a large HTTP response even when the header portion is small. The other approaches don't directly reveal payload size: protocol hierarchy doesn't indicate body length, DNS responses aren't related to the HTTP message size, and filtering by host alone won't show how much data is carried in the body.

8. What information does the Packet Bytes pane display?

A. It shows the raw hex and ASCII representation of the selected packet

B. It displays a graphical representation of the packet protocols

C. It lists all protocol fields parsed by the dissectors

D. It provides a packet summary for the capture

The Packet Bytes pane shows the exact raw data of the selected packet as a hex dump, with an ASCII interpretation beside it. Each line starts with an offset, followed by the hexadecimal byte values, and then the corresponding printable ASCII characters. This reflects the actual bytes captured on the wire, including headers and payload, and it updates as you select different packets. It's especially helpful for inspecting byte-level details, spotting non-text bytes, or verifying specific byte patterns that might not be obvious from the parsed views. The other displays in Wireshark serve different purposes: a graphical or schematic view of protocols isn't what Packet Bytes provides, nor is a listing of all parsed protocol fields or a high-level packet summary. Those functions come from the Packet Details pane and the Packet List, respectively.

9. Which path in Wireshark would you use to export a summary of captures to CSV?

A. Statistics → Protocol Hierarchy

B. File → Open

C. Statistics → Summary and export

D. Edit → Preferences

Exporting a summary to CSV is done through the Statistics menu by using the Summary view and then exporting. The Summary window provides a quick, high-level snapshot of the capture—packet count, duration, and basic statistics—and offers an option to export that information as CSV for sharing or later analysis. The other options aren't for exporting: Protocol Hierarchy shows how packets are distributed among protocols, but it doesn't export a summary; Open loads a capture file; Preferences changes settings and doesn't produce an export.

10. During port scanning, what type of information is commonly identified?

A. Addressing, Routing, Version Numbers, Patch Levels, Protocols/Services Running

B. Usernames And Passwords

C. Physical Environment

D. Weather Data

Port scanning maps a target's reachable surface by probing ports to see what is open and what services respond. The information commonly identified includes how the host is addressed and reachable through the network (addressing and routing), the software running on the host (version numbers and patch levels), and the protocols or services listening on each open port. This combination helps gauge what could be exploitable and what defenses are needed. Other options don't fit because port scanning doesn't reveal usernames or passwords, which require authentication breaches or credential harvesting; it doesn't provide data about the physical environment; and it doesn't give weather information.

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://wiresharkblock5.examzify.com

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