WIRESHARK BLOCK 5 PRACTICE EXAM (SAMPLE)

STUDY GUIDE

SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://wiresharkblock5.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. What steps are required to decrypt TLS 1.2 traffic using private keys (RSA) in Wireshark?

A. Import the server's private key for the certificate in Wireshark, enable TLS decryption, and ensure the traffic uses RSA key exchange (not ECDHE)

B. Import a client private key to decrypt TLS

C. Enable TLS decryption without providing keys

D. Use a pre-shared key (PSK) for decryption

2. How can you compare throughput or data volume across two captures in Wireshark?

A. Compare Statistics Summary data, use Protocol Hierarchy or Endpoints, or export to CSV and compare

B. Visually compare color intensities

C. Only compare the timestamp fields

D. Use a single capture and infer differences manually

3. 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

4. Which frames indicate a WPA2 4-way handshake for decryption?

A. EAPOL key frames (the four-message handshake)

B. WPA-PSK frames

C. TLS handshake frames

D. HTTP request frames

5. Which expression allows filtering by protocol name rather than a port or IP?

A. http (or any other protocol)

B. ip.addr

C. tcp.port

D. frame contains data

6. Which display filter filters traffic to or from 10.0.0.5?

A. ip.dst == 10.0.0.5

B. ip.src == 10.0.0.5

C. ip.addr == 10.0.0.5

D. tcp.dst == 10.0.0.5

7. Which path opens a window showing all the TLS segments on the same TLS connection as a selected packet?

A. Analyze ->Follow -> TLS Stream

B. Analyze ->Follow -> SSL Stream

C. Right click -> Follow UDP Stream

D. Analyze -> Expert Info

8. For RSA-based TLS decryption in Wireshark, what must be true about the key exchange mechanism?

A. It must use ECDHE

B. It must use PSK

C. It must use RSA key exchange

D. It must be TLS 1.3

9. Windows NT 6.2 corresponds to which Windows version?

A. Windows 8.1

B. Windows 8

C. Windows 7

D. Windows Vista

10. If you write ip.addr==A and ip.addr==B, what is required for a match?

A. The packet must have both IP addresses in a single frame

B. The packet must have either A or B

C. The packet must have neither A nor B

D. The packet must be TCP

Answers

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

Explanations

1. What steps are required to decrypt TLS 1.2 traffic using private keys (RSA) in Wireshark?

A. Import the server's private key for the certificate in Wireshark, enable TLS decryption, and ensure the traffic uses RSA key exchange (not ECDHE)

B. Import a client private key to decrypt TLS

C. Enable TLS decryption without providing keys

D. Use a pre-shared key (PSK) for decryption

When TLS uses RSA key exchange, the server's private key is the piece that unlocks the session keys needed to decrypt the traffic. The client sends a pre-master secret encrypted with the server's public key; the server uses its private key to decrypt that secret, and from there both sides derive the master secret and the symmetric keys used to encrypt and decrypt the subsequent records. That's why providing the server's private key in Wireshark allows it to reconstruct the session. So the right approach is to import the server's private key corresponding to the certificate shown in the handshake, in a format Wireshark can read (typically PEM), enable TLS decryption in Wireshark's settings, and ensure the capture uses RSA key exchange (not ephemeral methods like ECDHE). If the handshake uses an ephemeral key exchange such as ECDHE, the private key alone won't enable decryption because the session keys aren't derived from the server's private key; in that case you'd need a client-side key log or another method to obtain the master secrets. This is why the server private key approach works only for RSA key exchange and not for other key exchange methods.

2. How can you compare throughput or data volume across two captures in Wireshark?

A. Compare Statistics Summary data, use Protocol Hierarchy or Endpoints, or export to CSV and compare

B. Visually compare color intensities

C. Only compare the timestamp fields

D. Use a single capture and infer differences manually

When you want to compare throughput or data volume between two captures, use Wireshark's built-in statistics to obtain quantitative metrics and then export those results for side-by-side analysis. The Statistics views provide concrete numbers: Summary gives total bytes and packets (and can show throughput over the capture window), Protocol Hierarchy shows how data is distributed among protocols, and Endpoints reveals how much data each host sent or received. Exporting these statistics to CSV lets you line up the numbers from both captures in a spreadsheet or similar tool, making it easy to see exact differences in totals, distribution, or per-endpoint data. Visually relying on color coding is not precise for comparing volumes, and focusing only on timestamps misses data volume entirely. Inferring differences from a single capture manually is error-prone and wastes effort needed for accurate comparison.

3. 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.

4. Which frames indicate a WPA2 4-way handshake for decryption?

A. EAPOL key frames (the four-message handshake)

B. WPA-PSK frames

C. TLS handshake frames

D. HTTP request frames

The WPA2 4-way handshake is carried inside EAPOL Key frames. These four EAPOL Key frames exchanged between the access point and the client establish the Pairwise Transient Key (PTK) and confirm the encryption keys needed to decrypt the data frames. When you see the sequence of four EAPOL Key frames following authentication, that indicates the handshake is in progress and the keys will be derived for decryption. Other frame types don't indicate this key negotiation: TLS handshake frames belong to TLS sessions, not Wi Fi encryption; HTTP requests are application-layer traffic that occurs after decryption; WPA-PSK refers to the authentication method and its frames aren't the formal four-message handshake that derives the encryption keys.

5. Which expression allows filtering by protocol name rather than a port or IP?

A. http (or any other protocol)

B. ip.addr

C. tcp.port

D. frame contains data

Filtering by protocol name uses the protocol's identifier (the dissector name) to select packets that Wireshark can recognize as carrying that protocol, regardless of which port or IP they use. So you can filter with http to see all HTTP traffic no matter the source or destination port, or similarly with any other protocol you're interested in. This is exactly what you want when you're focusing on the protocol itself rather than the transport details. The other options filter by port numbers, IP addresses, or general frame content. ip.addr narrows traffic by who's communicating, not by the protocol in use. tcp.port restricts by a specific TCP port, which misses traffic of the same protocol on different ports or traffic from other protocols using that port. frame contains data is a broad check on the frame payload and doesn't target a specific protocol. Note that if the data is encrypted (like HTTPS), the http dissector may not apply, so the protocol-name filter won't match those packets until decryption is available.

6. Which display filter filters traffic to or from 10.0.0.5?

A. ip.dst == 10.0.0.5

B. ip.src == 10.0.0.5

C. ip.addr == 10.0.0.5

D. tcp.dst == 10.0.0.5

Filtering traffic by IP on either end of a conversation. To see all packets that involve 10.0.0.5, use a filter that matches the IP address regardless of whether it's the source or the destination. ip.addr does that: it matches packets where either the source or destination IP address is 10.0.0.5, catching both inbound and outbound traffic for that host. The other options look at only one side or a different protocol field: ip.dst finds packets where 10.0.0.5 is the destination, ip.src finds packets where it is the source, and tcp.dst tests the TCP destination port (a number), not an IP address, so it won't match 10.0.0.5.

7. Which path opens a window showing all the TLS segments on the same TLS connection as a selected packet?

A. Analyze ->Follow -> TLS Stream

B. Analyze ->Follow -> SSL Stream

C. Right click -> Follow UDP Stream

D. Analyze -> Expert Info

To see all TLS segments that belong to a single connection, use the Follow feature to reconstruct the TLS stream. Accessing Analyze Follow TLS Stream opens a window that shows the entire TLS conversation for the selected packet's connection, in order, including the handshake and subsequent TLS records. This makes it easy to follow how the session was negotiated and how data flows across packets. In some older Wireshark versions you might see SSL Stream there, but TLS Stream is the current naming for this function. The other options don't apply: Follow UDP Stream follows UDP datagrams, not TLS over TCP, and Expert Info is just a diagnostic summary, not a tool to reconstruct the TLS conversation.

8. For RSA-based TLS decryption in Wireshark, what must be true about the key exchange mechanism?

A. It must use ECDHE

B. It must use PSK

C. It must use RSA key exchange

D. It must be TLS 1.3

RSA-based TLS decryption in Wireshark works when the handshake uses RSA key exchange, where the client sends the pre-master secret encrypted with the server's public RSA key. The server can decrypt that secret with its private key, derive the master secret, and then Wireshark can compute the session keys to decrypt the traffic. If the handshake uses ephemeral key exchange like ECDHE, the pre-master secret isn't encrypted with the server's private key; it's derived from the Diffie-Hellman exchange and the server's private key is only used to sign parameters. In that case, possessing the server's private key doesn't let Wireshark decrypt the session keys. TLS 1.3 uses a different mechanism altogether and does not rely on RSA key transport for decryption in the same way, so RSA-based decryption isn't applicable there. Therefore, the decryption method requires RSA key exchange.

9. Windows NT 6.2 corresponds to which Windows version?

A. Windows 8.1

B. Windows 8

C. Windows 7

D. Windows Vista

Windows uses internal NT kernel version numbers that map to the public Windows release names. The sequence goes like this: 6.0 is Vista, 6.1 is Windows 7, 6.2 is Windows 8, and 6.3 is Windows 8.1 (with 10.0 coming for Windows 10). So a kernel version of 6.2 identifies Windows 8 (and its server counterpart Windows Server 2012). That's why the correct match is Windows 8.

10. If you write ip.addr==A and ip.addr==B, what is required for a match?

A. The packet must have both IP addresses in a single frame

B. The packet must have either A or B

C. The packet must have neither A nor B

D. The packet must be TCP

ip.addr matches an IP address in the packet's IP header, either the source or the destination. When you combine two such tests with AND, both conditions must be true for the same packet. So ip.addr==A and ip.addr==B will only match if the IP packet has A as one endpoint and B as the other—that is, the packet carries both addresses in its header (the two endpoints of that IP flow). A packet from A to someone else or from someone else to B would fail because one of the conditions wouldn't be met. The protocol doesn't matter here; any IP packet can match as long as its source/destination pair satisfies the two-address requirement.

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!