WIRESHARK TRAFFIC ANALYSIS PRACTICE EXAM (SAMPLE)

STUDY GUIDE

SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://wiresharttrafficanalysis.examzify.com

Table of Contents

Copyright 1

Table of Contents 2

Introduction 3

How to Use This Guide 4

Questions 5

Answers 8

Explanations 10

Next Steps 15

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 is the standard method used to hide traffic from eavesdroppers on the internet?

A. IPsec VPN

B. SSH

C. Tor

D. HTTPS/TLS encryption

2. What does JNDI do in this context?

A. Loads remote resources

B. Encrypts traffic

C. Parses HTML

D. Serves DNS

3. Which attack uses ARP spoofing to intercept traffic?

A. Denial of Service (DoS) attack

B. DNS cache poisoning

C. Man-in-the-Middle (MITM)

D. Brute-force password attack

4. How can you identify TLS handshake messages in a capture?

A. Filter on http.response.code >= 400.

B. Filter on dns.query.type == A.

C. Filter on tls or ssl; expand ClientHello, ServerHello, Certificate, ServerKeyExchange, Finished messages.

D. Expand ARP protocol.

5. Which of the following statements about UDP is true?

A. It uses a three-way handshake before data transfer.

B. It does not guarantee delivery, order, or error checking.

C. It always requires a response from the destination.

D. It always encrypts payload data.

6. Which message begins the TLS handshake from the client?

A. Finished

B. Server Hello

C. Certificate

D. Client Hello

7. Which of the following can you see in TLS encrypted traffic?

A. IP addresses, domains (SNI), and packet sizes

B. Payload data

C. Certificates

D. User credentials

8. What protocol was found inside ICMP tunneling in the exercise?

A. SSH

B. DNS

C. ARP

D. HTTP

9. Which DHCP message is transmitted by a client to indicate it needs network configuration?

A. DHCP Discover

B. DHCP Offer

C. DHCP Request

D. DHCP Acknowledge

10. What is used for stealth communication?

A. TLS tunneling

B. SSH tunneling

C. FTP tunneling

D. DNS/ICMP tunneling

Answers

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

Explanations

1. What is the standard method used to hide traffic from eavesdroppers on the internet?

A. IPsec VPN

B. SSH

C. Tor

D. HTTPS/TLS encryption

HTTPS/TLS encryption is the standard way to hide traffic from eavesdroppers because it protects the data as it travels between your device and the web server. When you use HTTPS, the HTTP messages — the requests you send and the responses you receive — are encrypted with TLS. This means a passive listener on the network can't read the content of what you're sending or receiving, and any tampering with the data would be detected. This approach is universally deployed: every modern browser and most websites use HTTPS by default, so you don't need to install special software or set up a VPN. Other options operate in different ways or contexts—IPsec VPN secures traffic by tunneling it through a VPN endpoint, SSH is designed for secure remote access or port forwarding, and Tor focuses on anonymity by routing traffic through multiple relays and can be slower and less practical for everyday browsing. For regular internet use, HTTPS/TLS is the standard method to keep your web traffic confidential.

2. What does JNDI do in this context?

A. Loads remote resources

B. Encrypts traffic

C. Parses HTML

D. Serves DNS

JNDI is a Java API for locating resources by name in a directory or naming service. The core idea is that an application asks a naming service to resolve a logical name to an actual resource, which can be a local object or a reference to something remote. In this context, that means JNDI can fetch a reference to a resource that may be hosted remotely (for example, a directory entry that points to a remote object or code). So JNDI's role here is about locating and loading resources, potentially from remote servers, rather than encrypting traffic, parsing HTML, or serving DNS.

3. Which attack uses ARP spoofing to intercept traffic?

A. Denial of Service (DoS) attack

B. DNS cache poisoning

C. Man-in-the-Middle (MITM)

D. Brute-force password attack

Intercepting traffic between two devices on a local network is accomplished by placing the attacker in the middle of the communication path. ARP spoofing does this by tricking devices on the LAN into associating the attacker's MAC address with the IP address of another host (often the gateway). As a result, traffic that should go to that host is sent to the attacker, who can simply forward it on or modify it, effectively eavesdropping and potentially altering the communication. This positioning—being able to watch and control the data as it passes between two endpoints—is the essence of a Man-in-the-Middle attack. The other options don't describe this scenario: DoS would disrupt or prevent traffic rather than intercept it, DNS cache poisoning targets name resolution rather than traffic routing at the LAN layer, and brute-force attacks aim to guess credentials rather than intercept communications.

4. How can you identify TLS handshake messages in a capture?

A. Filter on http.response.code >= 400.

B. Filter on dns.query.type == A.

C. Filter on tls or ssl; expand ClientHello, ServerHello, Certificate, ServerKeyExchange, Finished messages.

D. Expand ARP protocol.

To identify TLS handshake messages, look at the TLS protocol layer in your capture. The handshake is the sequence that sets up a secure session, so filtering for TLS (or SSL on older captures) focuses your view on the relevant traffic. Once you filter for TLS and expand the TLS protocol in a packet, you'll see the handshake message types: ClientHello, ServerHello, Certificate, ServerKeyExchange, and Finished. These messages trace the negotiation of cryptographic parameters and the establishment of the secure channel, with the Finished message indicating the handshake has completed and normal encrypted data can follow. Other filters don't fit this task because they target different protocols or layers: an HTTP filter would show web responses, not the handshake; a DNS filter would show name lookups; and ARP is a link-layer protocol unrelated to TLS. The TLS approach directly highlights the handshake steps, usually occurring after the TCP connection is established (often on port 443), and it's the clearest way to identify the TLS handshake in a capture.

5. Which of the following statements about UDP is true?

A. It uses a three-way handshake before data transfer.

B. It does not guarantee delivery, order, or error checking.

C. It always requires a response from the destination.

D. It always encrypts payload data.

UDP is a connectionless, best-effort transport protocol. It does not establish a connection or perform a handshake before sending data, so there is no guarantee that a packet will arrive, nor that it will arrive in order. Packets can be lost, arrive out of order, or be duplicated, and the protocol provides no built-in mechanism for reliable delivery or retransmission. A checksum exists to detect corruption, but it does not provide error correction or delivery guarantees. Encryption is not provided by UDP itself; securing UDP requires additional layers (like DTLS or application-layer encryption). Because of its lack of delivery guarantees, lack of ordering, and absence of built-in error handling, the statement that best describes UDP is that it does not guarantee delivery, order, or error checking.

6. Which message begins the TLS handshake from the client?

A. Finished

B. Server Hello

C. Certificate

D. Client Hello

TLS handshakes begin with the client sending a ClientHello to start the negotiation. This message asks for things like the protocol version the client supports, a list of cipher suites it can use, compression methods, and some random data to help generate keys. It may also include extensions such as SNI to identify the hostname the client is connecting to. After that, the server replies with ServerHello, deciding on the version and cipher suite to use and providing its own random data. The server then sends its certificate in a Certificate message to prove its identity. The handshake continues with additional messages to finish key exchange and verification, culminating in a Finished message once the secure keys are in place. Because the client's ClientHello starts the process, it is the message that begins the TLS handshake.

7. Which of the following can you see in TLS encrypted traffic?

A. IP addresses, domains (SNI), and packet sizes

B. Payload data

C. Certificates

D. User credentials

In TLS, the payload you send and receive is encrypted, but some surrounding information stays visible. You can observe the IP addresses involved in the connection (source and destination) and the sizes of the TLS records that are sent, even though you can't read the actual application data inside those records. The server name requested by the client is typically carried in the SNI field of the ClientHello and is sent in the clear, so observers can often see which domain is being contacted. Packet or record sizes give you an idea of how much data is being exchanged without revealing the content. The actual application data isn't readable, and user credentials in the application layer aren't exposed in the encrypted stream. Certificates are exchanged as part of the handshake, but that exchange isn't the encrypted application data, so it's not what's meant by "TLS encrypted traffic" in this context. Therefore, the elements that are visible are the IPs, the domain via SNI, and the TLS record sizes, matching the best answer.

8. What protocol was found inside ICMP tunneling in the exercise?

A. SSH

B. DNS

C. ARP

D. HTTP

ICMP tunneling hides another protocol's traffic inside the payload of ICMP packets, so you identify what protocol is being transported by looking for its characteristic patterns inside that payload. In this exercise, the ICMP payload contained data that matches SSH: the SSH identification string (for example, "SSH-2.0-…") and the subsequent key-exchange material. That clear SSH handshake pattern inside the ICMP tunnel tells you the inside protocol is SSH. DNS would show DNS query/response structure and domain-name data, ARP isn't transported over IP in this way, and HTTP would present HTTP request/response headers and methods inside the payload rather than an SSH handshake.

9. Which DHCP message is transmitted by a client to indicate it needs network configuration?

A. DHCP Discover

B. DHCP Offer

C. DHCP Request

D. DHCP Acknowledge

DHCP uses a four-step exchange to obtain IP configuration, and the client starts by broadcasting a DHCP Discover message to locate any DHCP servers on the network. This is the indication that the client needs network settings and hasn't yet chosen a server or an address. Servers that hear the Discover respond with DHCP Offer messages proposing configuration parameters. The client then selects an offer and sends DHCP Request to ask for that specific configuration, and the server finalizes with DHCP Acknowledge to confirm the lease. So, the message the client sends to initiate configuration is DHCP Discover, since it signals the need and starts the negotiation.

10. What is used for stealth communication?

A. TLS tunneling

B. SSH tunneling

C. FTP tunneling

D. DNS/ICMP tunneling

Stealth communication relies on covert channels that blend with normal network activity so data can move without easily attracting attention. DNS tunneling is especially effective because DNS traffic is almost always allowed through networks, and data can be hidden in domain names or DNS records sent to an attacker-controlled server, making it look like ordinary lookups. ICMP tunneling also exists, taking advantage of the permissibility of ICMP traffic to carry payloads inside echo requests and replies. While TLS, SSH, or FTP tunnels can conceal traffic, they tend to be more detectable due to their recognizable protocol behavior and security controls, making DNS/ICMP tunneling the more commonly used stealth channel.

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://wiresharttrafficanalysis.examzify.com

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