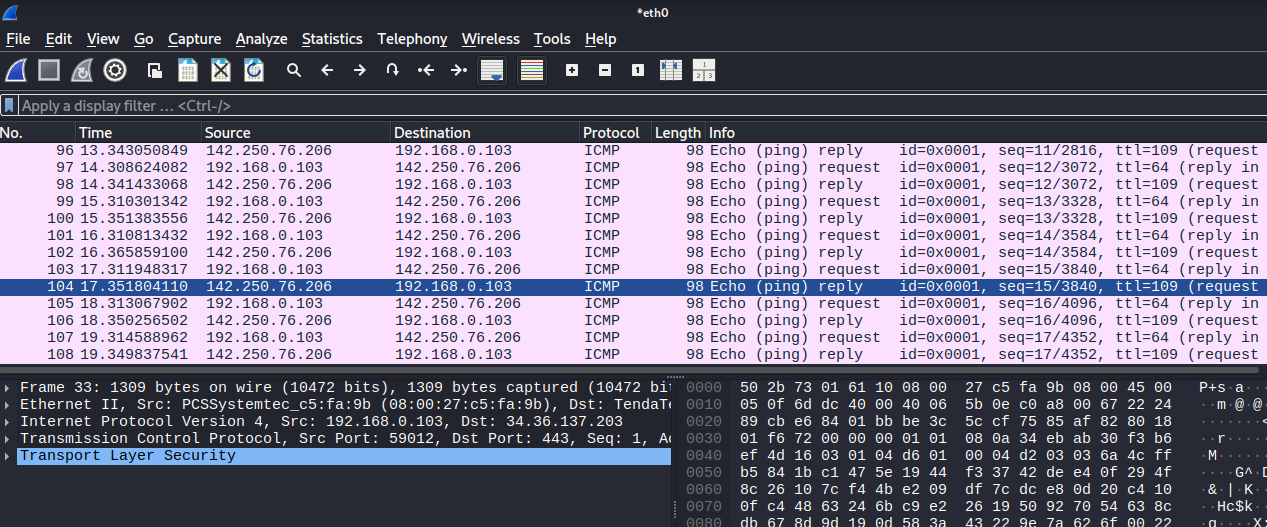
Wireshark Capture and Analysis Guide

Install Wireshark



Start Capturing Packets

Open Wireshark.

Select your active network interface (e.g., eth0, wlan0, or Wi-Fi).

Click "Start capturing packets" (blue shark fin icon).

Generate Network Traffic

Open a terminal or browser:

ping google.com

Let it run for about 60 seconds.

Stop the Capture

Click the red square stop button.

Filter Packets by Protocol

In the filter bar, apply filters like:

http (for web traffic)

dns (for domain name queries)

tcp (for general connections)

icmp (for ping/echo)

ssl or tls (for HTTPS)

📡 6. Identify 3+ Protocols

You should now see various protocols. Common ones include:

| Protocol | Function |
| --- | --- |
| DNS | Resolves domain names to IPs |
| TCP | Manages reliable connections |
| HTTP | Web browsing (unsecure) |
| HTTPS / TLS | Encrypted web browsing |
| ICMP | Used by ping |
| ARP | Resolves IPs to MAC addresses |

Export as .pcap File

Go to File → Export Specified Packets.

Choose format: Wireshark/tcpdump/... - \*.pcap

Name it and save.

Summarize Findings

Here’s a template you can use to summarize your .pcap analysis:

Wireshark Capture Summary

Capture Duration: 60 seconds  
Interface: wlan0 (example)  
Traffic Generated: ping google.com, browsing example.com

Detected Protocols

| Protocol | Role | Notes |
| --- | --- | --- |
| DNS | Resolves domain names | You’ll see queries like A google.com, response with IP |
| ICMP | Ping (echo request/reply) | Shows if ping to server worked |
| TCP | Connection protocol | Handshake seen (SYN, SYN-ACK, ACK) |
| HTTP | Web browsing | Shows GET/POST requests and headers if unencrypted |
| TLS/SSL | Encrypted web | Secure site traffic, includes Client Hello |

Interesting Packet Details

1. DNS Query Example:

Source: 192.168.1.5 (your machine)

Destination: 8.8.8.8 (Google DNS)

Query: A record for example.com

Response: IP address 93.184.216.34

2. ICMP Ping Example:

Type: Echo Request/Reply

Round-trip time: ~24ms

Success: Yes, no packet loss

3. HTP Request Example:

Method: GET

Host: example.com

User-Agent: Mozilla/5.0

Response Code: 200 OK

Important Observations

Unencrypted HTTP traffic shows full data, including headers.

TLS traffic shows only handshake metadata — actual content is encrypted.

Ping uses ICMP which is not reliable for data transfer, only for reachability checks.

DNS leaks domain names even when using HTTPS, unless DNS over HTTPS is used.

Plaintext Passwords

What to look for: Login info over HTTP, FTP, or Telnet.

Risk: Easy to steal passwords.

How to see: Filter by protocol (e.g., http, ftp) and follow TCP stream.

Unencrypted Traffic

What to look for: Sites using HTTP instead of HTTPS.

Risk: Sensitive info can be stolen.

How to see: Filter http, check for login forms or credentials.

DNS Leaks

What to look for: DNS requests to public or unknown servers.

Risk: Shows all sites visited, good for recon.

How to see: Filter by dns, check query names.

Open Ports / Services

What to look for: Services like Telnet, SMB, or unknown ports.

Risk: Exploitable services may be exposed.

How to check: Use nmap scan or watch in Wireshark for protocol types.

Old or Weak SSL/TLS

What to look for: SSL handshake with weak ciphers.

Risk: Easy to decrypt or MITM.

How to see: Filter by ssl or tls, inspect handshake.

Suspicious IPs or Connections

What to look for: Connections to unknown IPs or countries.

Risk: Could be malware or data leak.

How to see: Check ip.dst or ip.src and GeoIP lookup.

ICMP (Ping Floods)

What to look for: Too many ICMP packets.

Risk: DoS attack or probing.

How to see: Filter by icmp, check traffic volume.

Sample Wireshark Filters:

http → See unencrypted web traffic.

ftp → See file transfer with credentials.

dns → See DNS queries.

icmp → See ping attacks.

tcp.port == 23 → See Telnet traffic.