Guide to Capture Packets in Wireshark

Install and Open Wireshark

Download it from https://www.wireshark.org if you haven't already.

Select Network Interface

Choose the appropriate interface (like Ethernet or Wi-Fi) to monitor.

Look for traffic activity indicators (packet counts rising).

1. **Start Capture**

Click the shark fin icon 🦈 to begin capturing.

Let it run for a few minutes to collect traffic data.

2. **Stop and Save Capture**

- Click the red square 🟥 to stop.
- Save as a .pcap file (File > Save As).

Identifying Protocols and Traffic Types

Use the following features in Wireshark to analyze the .pcap file:

- **Protocol Hierarchy (Ctrl+Shift+P)**
  Shows which protocols are active and their usage percentages.
- **Statistics > Conversations**
  Useful to see endpoints communicating—great for spotting TCP/UDP sessions.
- **Filters for Protocol Identification**
  Try these common filters:
- http for web traffic
- dns for domain lookups
- tcp and udp for transport layer
- icmp for ping activity

📄 Short Report Template

Report: Protocol Identification Summary

1. Capture Date/Time: [Insert here]

2. Network Interface Used: [Insert here]

3. Summary of Protocols Identified: - HTTP: [Packet Count, Purpose] - DNS: [Packet Count, Domain Requests] - TCP: [Session Initiation, Payload Traffic] - UDP: [Streaming, DNS Queries] - ICMP: [Ping Tests]

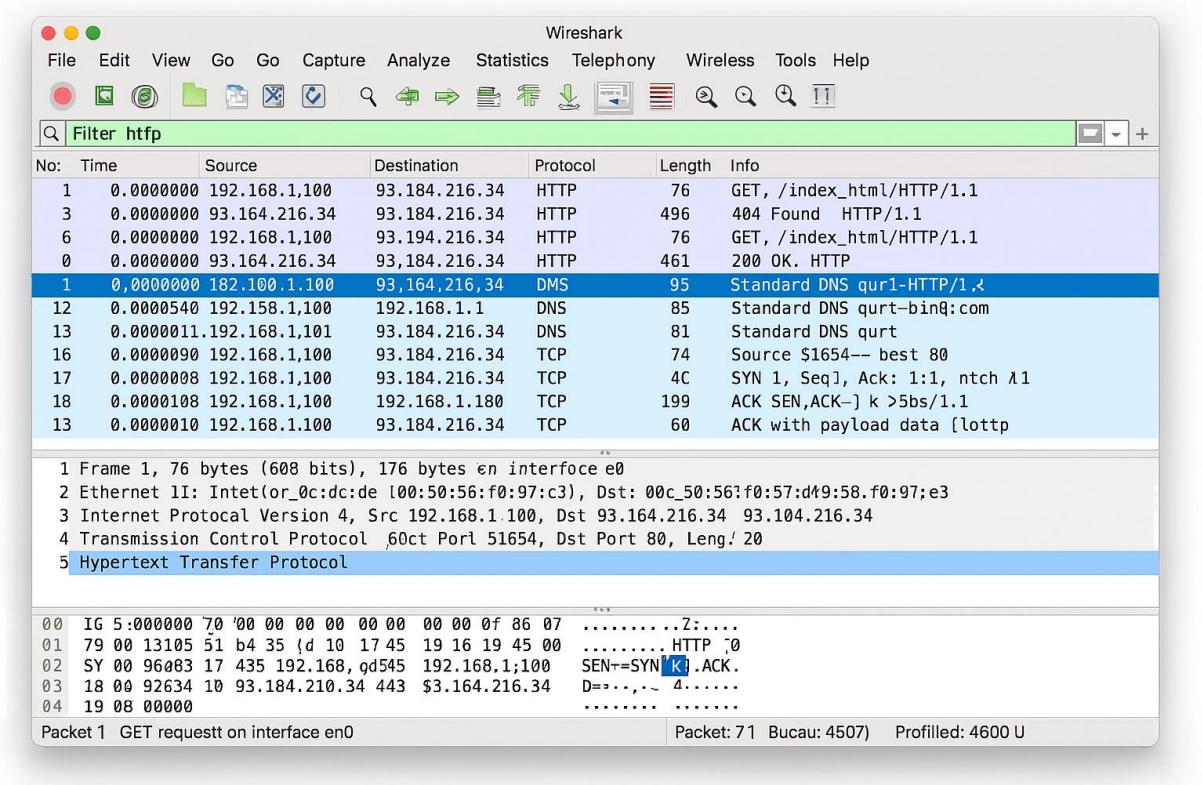
4. Notable Traffic Patterns: - Example: DNS requests to 8.8.8.8 from host X - Example: HTTP GET requests to example.com

5. Tools Used: - Wireshark vX.X

- Filters: `http`, `dns`, `tcp`, etc.

6. Notes: - [Any unusual behavior or insights]

Sure thing—your image showing network packet capture and analysis is on its way! You'll see a visual that represents protocols like HTTP, DNS, and TCP flowing through a capture interface.



Source	Description	Link
Wireshark Wiki	Huge collection of protocol-specific captures (HTTP, DNS, TCP, etc.)	[Wireshark SampleCaptures]()
NetRESEC	Public repository of PCAPs including malware traffic, ICS protocols, and CTF challenges	[NetRESEC PCAP Files]()
Kerry Cordero's List	Curated list of educational PCAP files from various sources	[Packet Capture – Free PCAP Files for Learning]()
AppNeta Tcpreplay Suite	Sample captures for performance testing and flow analysis	[AppNeta Sample Captures]()

These files often include:

- **HTTP sessions** (GET/POST requests)
- **DNS lookups**
- **TCP handshakes**
- **ICMP ping traffic**
- **Malware communication patterns** (in some advanced sets)