

HTTP Request and Response Analysis in Wireshark02

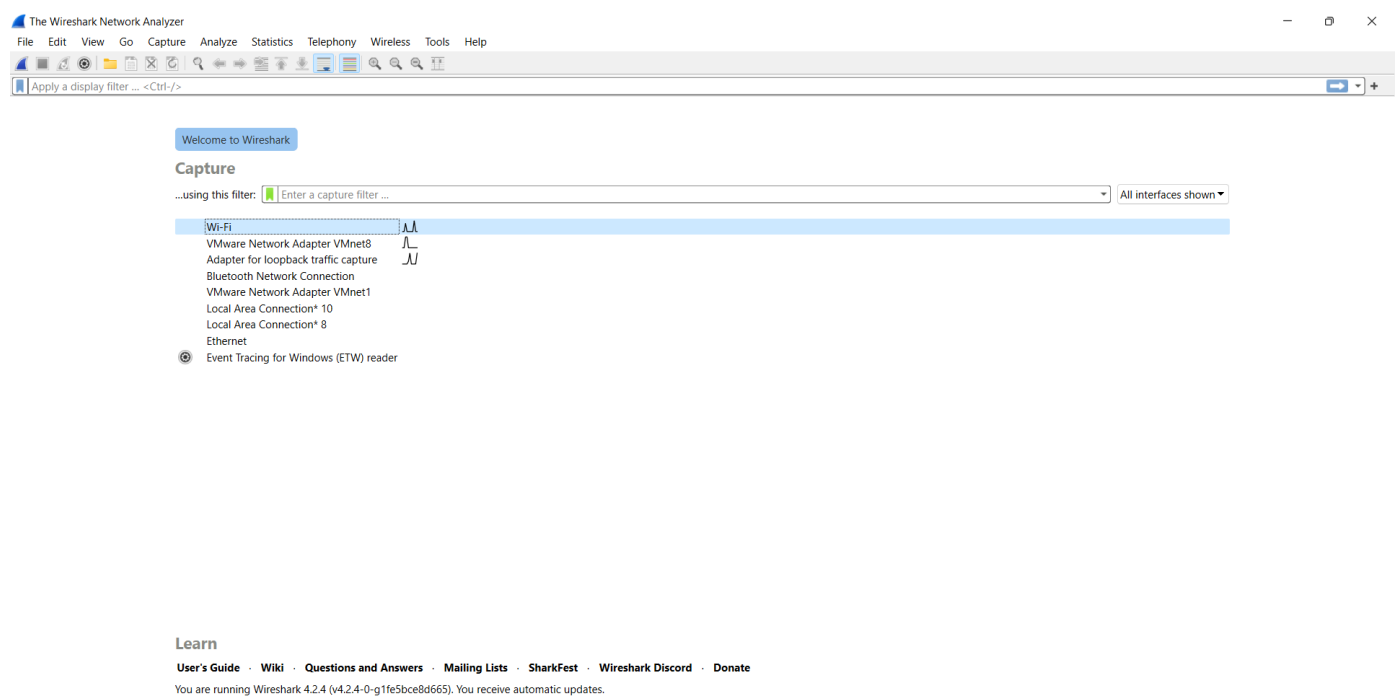
HTTP Request and Response Analysis

- **Goal:** Capture a webpage load and study the HTTP headers.
- **Tasks:**
 - Start capture.
 - Visit a basic HTTP website (non-HTTPS if possible, or use test environments).
 - Filter with `http`.
 - Analyze:
 - GET or POST requests.
 - Status codes (like `200 OK`, `404 Not Found`).
 - Headers (like `Host`, `User-Agent`).

Solution

Step 1: Open Wireshark

- Open Wireshark.
- Select your **Wi-Fi**



Step 2: Visit an HTTP Website

- In your web browser, visit a **non-HTTPS website**.
(Most websites today use HTTPS, but you can use a test site.)

Example sites:

- `http://neverssl.com` (made for HTTP testing)



What?

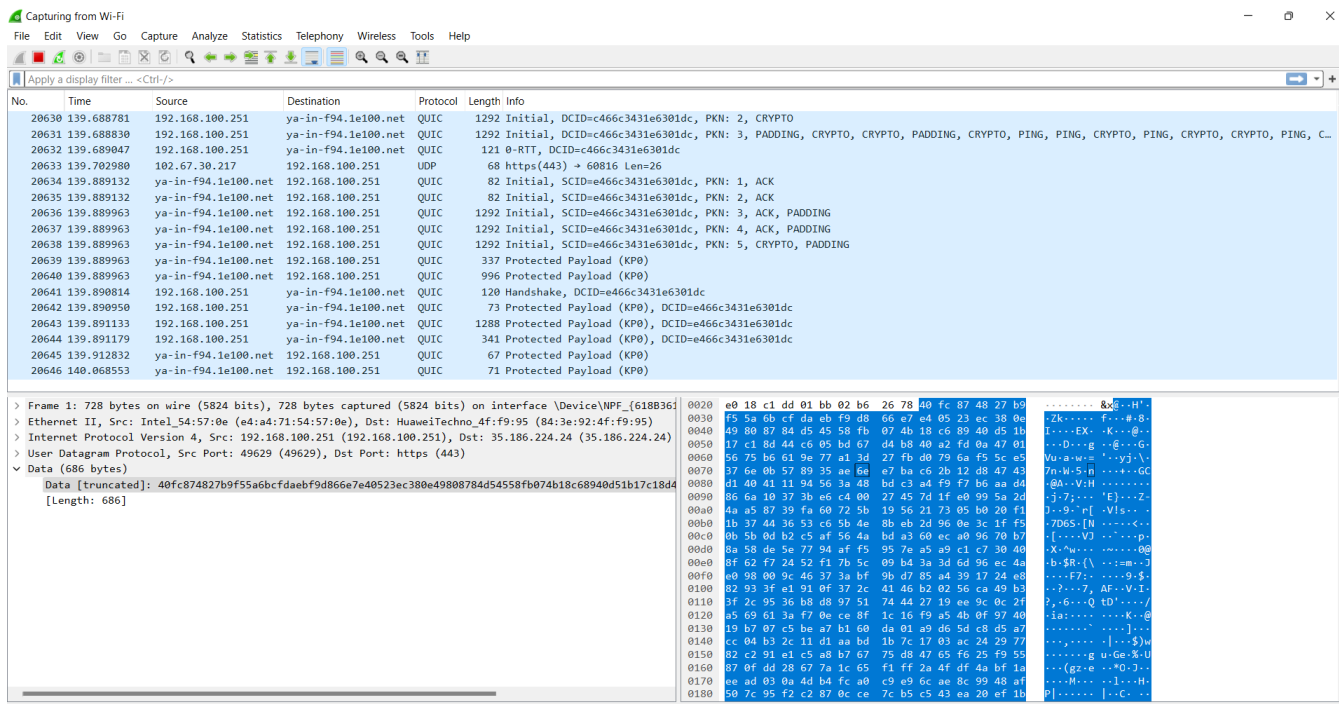
This website is for when you try to open Facebook, Google, Amazon, etc on a wifi network, and nothing happens. Type "http://neverssl.com" into your browser's url bar, and you'll be able to log on.

How?

neverssl.com will never use SSL (also known as TLS). No encryption, no strong authentication, no [HSTS](#), no HTTP/2.0, just plain old unencrypted HTTP and forever stuck in the dark ages of internet security.

Step 3: Stop Capturing

- After the site loads, go back to Wireshark and click the **red square "Stop"** button.



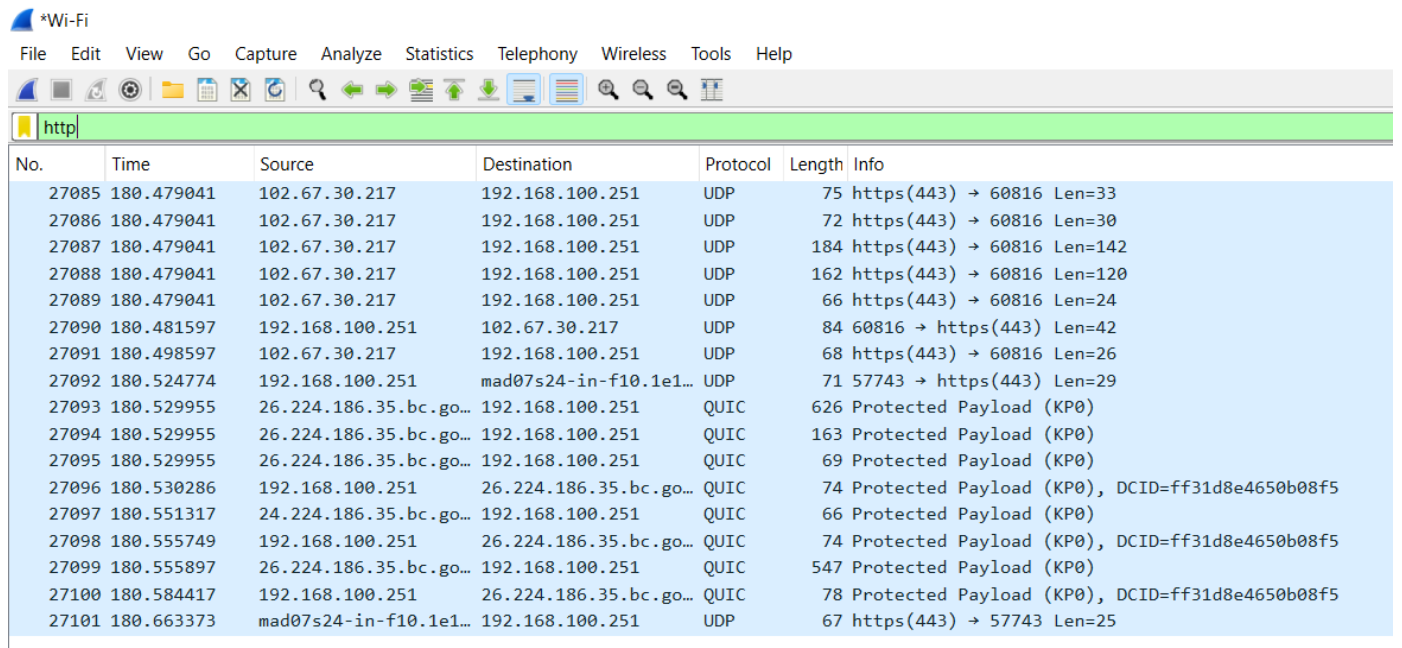
Step 4: Filter HTTP Traffic

- In the filter bar at the top, type:

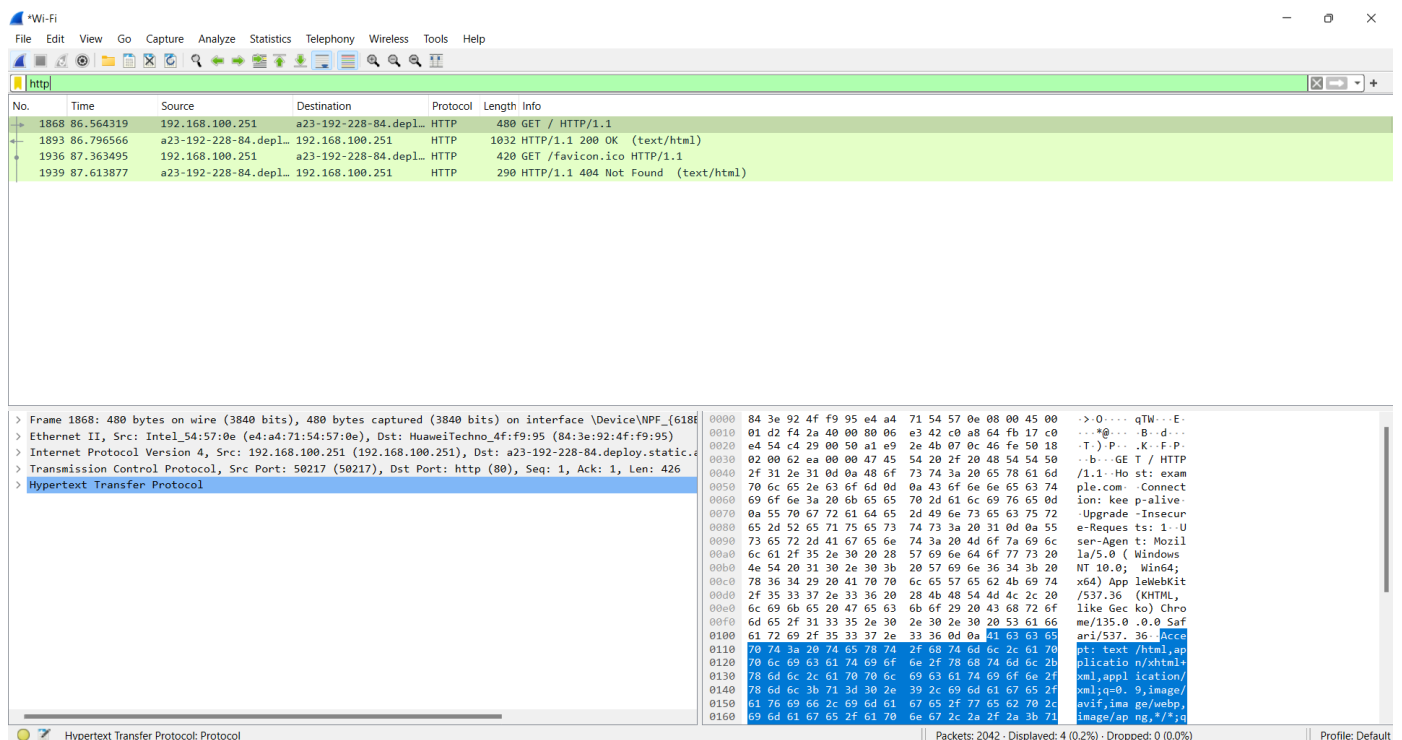
http

and press **Enter**.

Now you'll only see HTTP packets.



No.	Time	Source	Destination	Protocol	Length	Info
27085	180.479041	102.67.30.217	192.168.100.251	UDP	75	https(443) → 60816 Len=33
27086	180.479041	102.67.30.217	192.168.100.251	UDP	72	https(443) → 60816 Len=30
27087	180.479041	102.67.30.217	192.168.100.251	UDP	184	https(443) → 60816 Len=142
27088	180.479041	102.67.30.217	192.168.100.251	UDP	162	https(443) → 60816 Len=120
27089	180.479041	102.67.30.217	192.168.100.251	UDP	66	https(443) → 60816 Len=24
27090	180.481597	192.168.100.251	102.67.30.217	UDP	84	60816 → https(443) Len=42
27091	180.498597	102.67.30.217	192.168.100.251	UDP	68	https(443) → 60816 Len=26
27092	180.524774	192.168.100.251	mad07s24-in-f10.1e1...	UDP	71	57743 → https(443) Len=29
27093	180.529955	26.224.186.35.bc.go...	192.168.100.251	QUIC	626	Protected Payload (KP0)
27094	180.529955	26.224.186.35.bc.go...	192.168.100.251	QUIC	163	Protected Payload (KP0)
27095	180.529955	26.224.186.35.bc.go...	192.168.100.251	QUIC	69	Protected Payload (KP0)
27096	180.530286	192.168.100.251	26.224.186.35.bc.go...	QUIC	74	Protected Payload (KP0), DCID=ff31d8e4650b08f5
27097	180.551317	24.224.186.35.bc.go...	192.168.100.251	QUIC	66	Protected Payload (KP0)
27098	180.555749	192.168.100.251	26.224.186.35.bc.go...	QUIC	74	Protected Payload (KP0), DCID=ff31d8e4650b08f5
27099	180.555897	26.224.186.35.bc.go...	192.168.100.251	QUIC	547	Protected Payload (KP0)
27100	180.584417	192.168.100.251	26.224.186.35.bc.go...	QUIC	78	Protected Payload (KP0), DCID=ff31d8e4650b08f5
27101	180.663373	mad07s24-in-f10.1e1...	192.168.100.251	UDP	67	https(443) → 57743 Len=25



No.	Time	Source	Destination	Protocol	Length	Info
1868	86.564319	192.168.100.251	a23-192-228-84.depl...	HTTP	480	GET / HTTP/1.1
1893	86.796566	a23-192-228-84.depl...	192.168.100.251	HTTP	1032	HTTP/1.1 200 OK (text/html)
1936	87.363495	192.168.100.251	a23-192-228-84.depl...	HTTP	420	GET /favicon.ico HTTP/1.1
1939	87.613877	a23-192-228-84.depl...	192.168.100.251	HTTP	290	HTTP/1.1 404 Not Found (text/html)

> Frame 1868: 480 bytes on wire (3840 bits), 480 bytes captured (3840 bits) on interface \Device\NPF_{618F...}

> Ethernet II, Src: Intel_54:57:0e (e4:a4:71:54:57:0e), Dst: HuaweiTechno_4f:f9:95 (84:3e:92:4f:f9:95)

> Internet Protocol Version 4, Src: 192.168.100.251 (192.168.100.251), Dst: a23-192-228-84.deploy.static...

> Transmission Control Protocol, Src Port: 50217 (50217), Dst Port: http (80), Seq: 1, Ack: 1, Len: 426

> Hypertext Transfer Protocol

Hypertext Transfer Protocol: Protocol

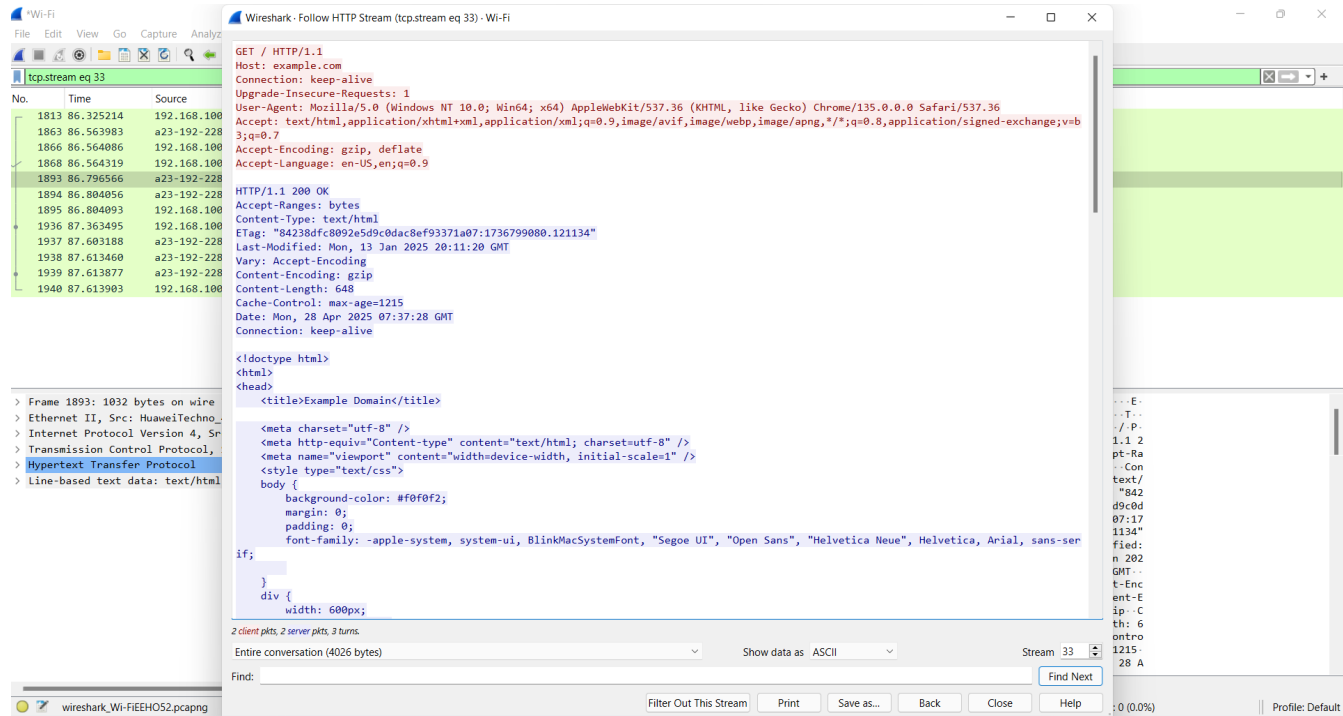
Packets: 2042 - Displayed: 4 (0.2%) - Dropped: 0 (0.0%)

Profile: Default

Step 5: Bonus - Follow the HTTP Stream

- Right-click on any HTTP request packet.
- Click **"Follow" > "HTTP Stream"**.

- There is a full conversation between your browser and the server (clear text!).



Analyze HTTP Requests and Responses

Now look at the details:

What to Look For	How to Find It
HTTP Request	Look for "GET /something" or "POST /something".
HTTP Response	Look for "HTTP/1.1 200 OK" or "404 Not Found".
Headers	Expand the packet details and find "Host", "User-Agent", "Accept", etc.

Quick guide:

- **GET** = Your browser asking for a webpage.
- **POST** = Sending data (like login info).
- **200 OK** = Success.
- **404 Not Found** = Page missing.

Lesson: I have captured HTTP traffic and learned how the web browser and servers talk!