HTTP Request and Response Analysis in Wireshark02

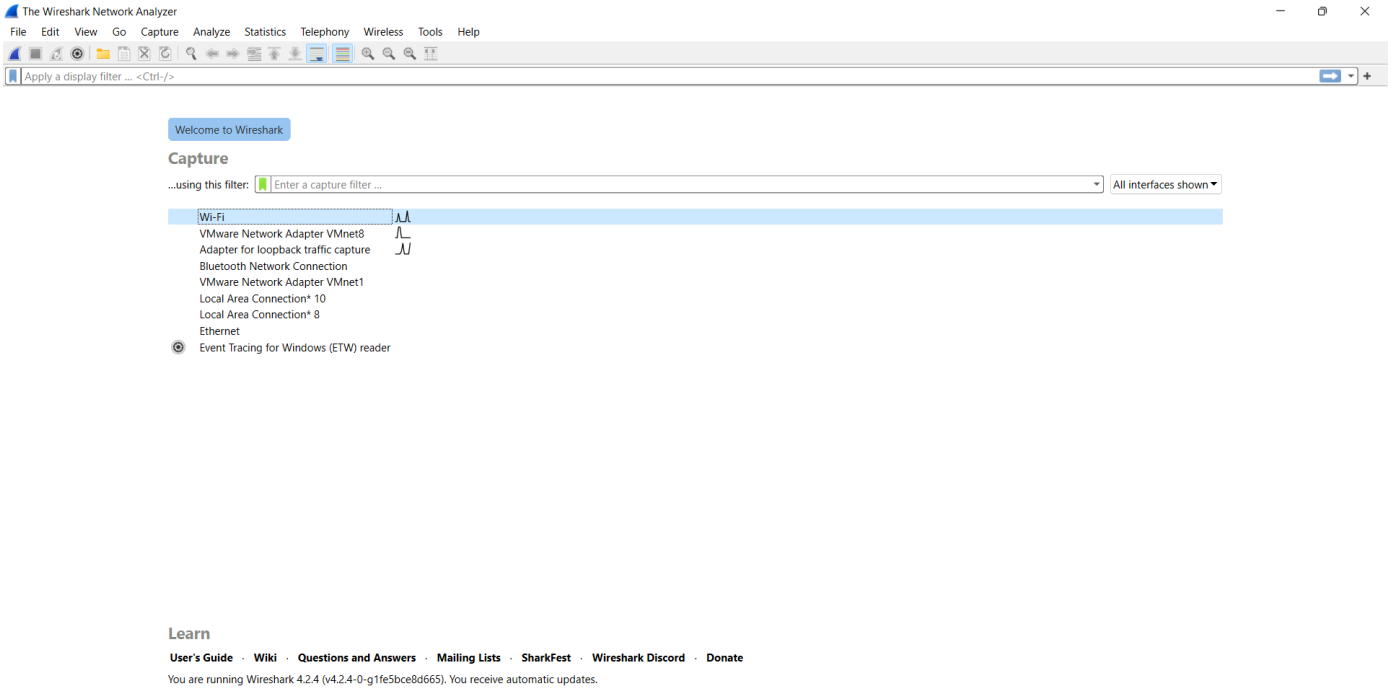
HTTP Request and Response Analysis

- **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**

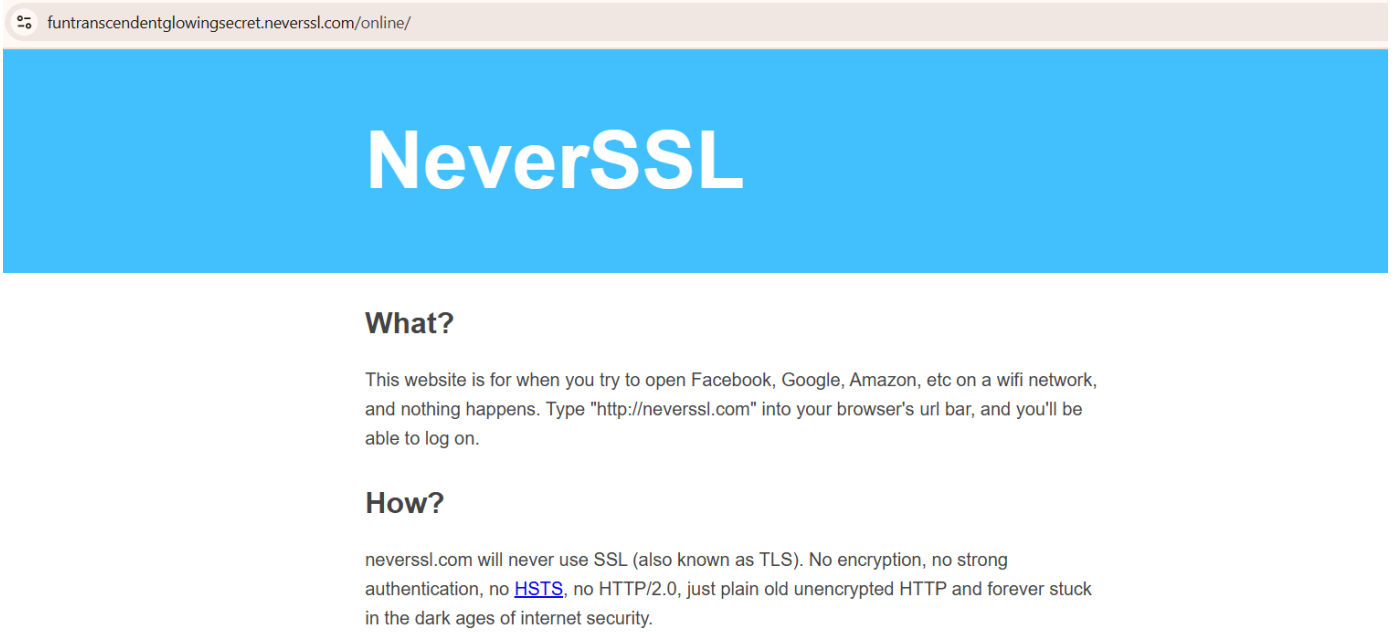


Step 2: Visit an HTTP Website

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

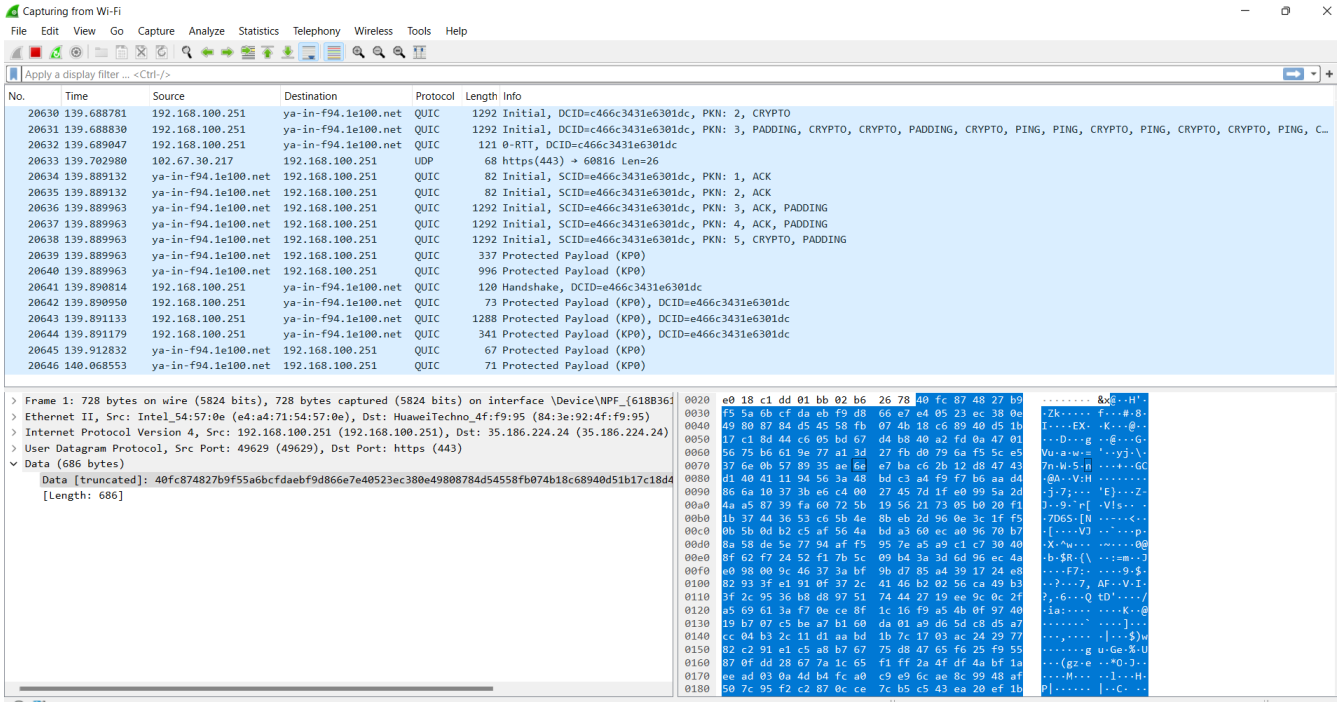
Example sites:

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



Step 3: Stop Capturing

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



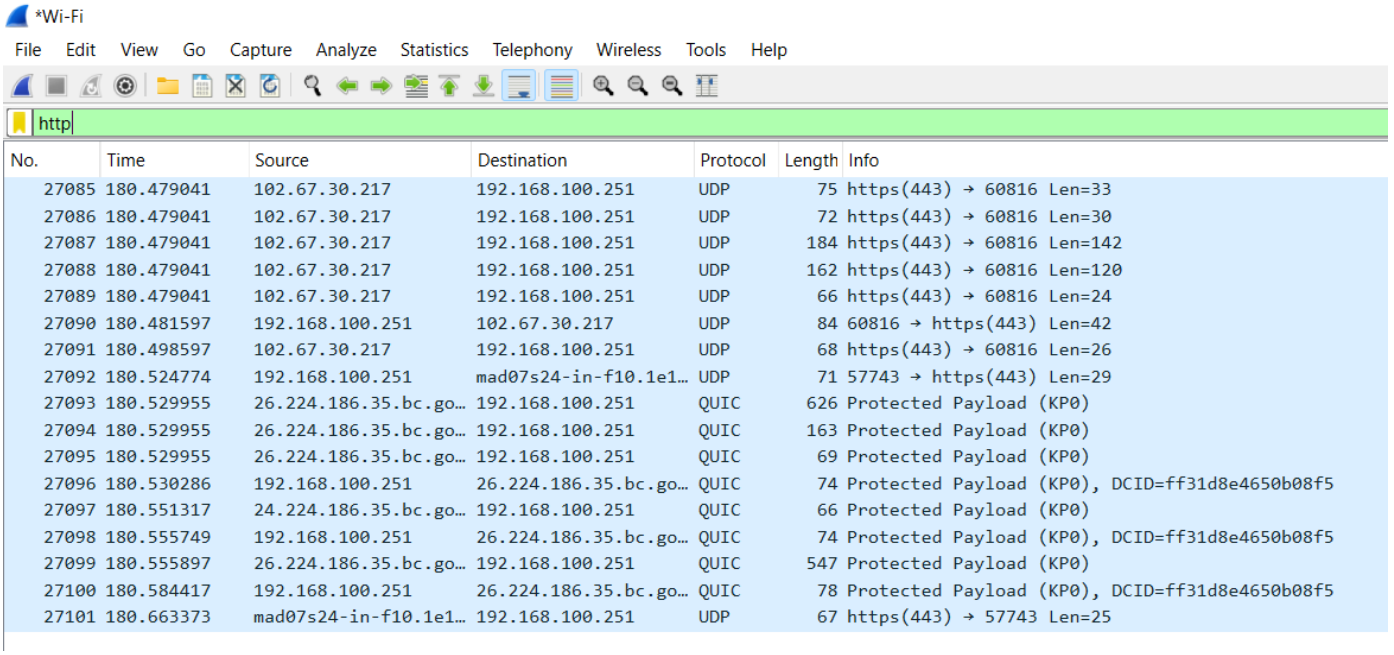
Step 4: Filter HTTP Traffic

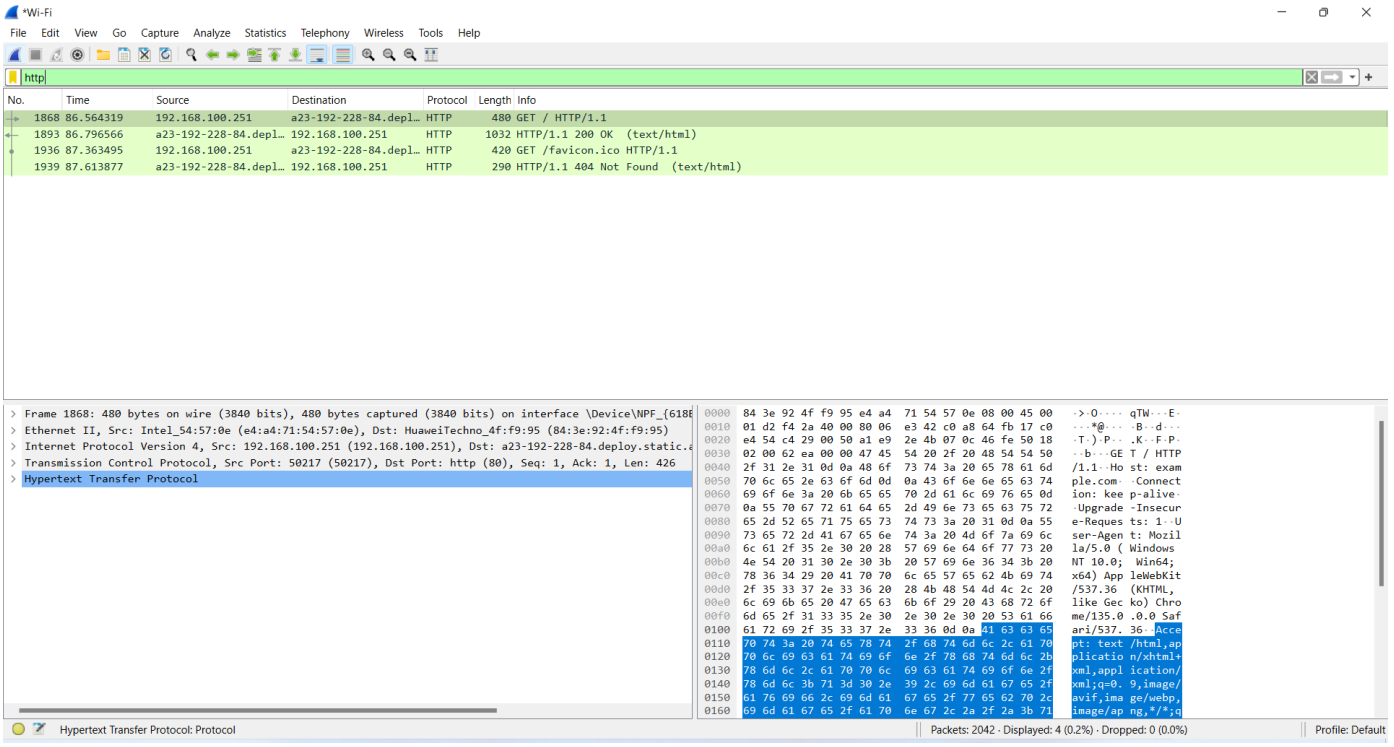
- In the filter bar at the top, type:

`http`

and press **Enter**.

Now you'll only see HTTP packets.

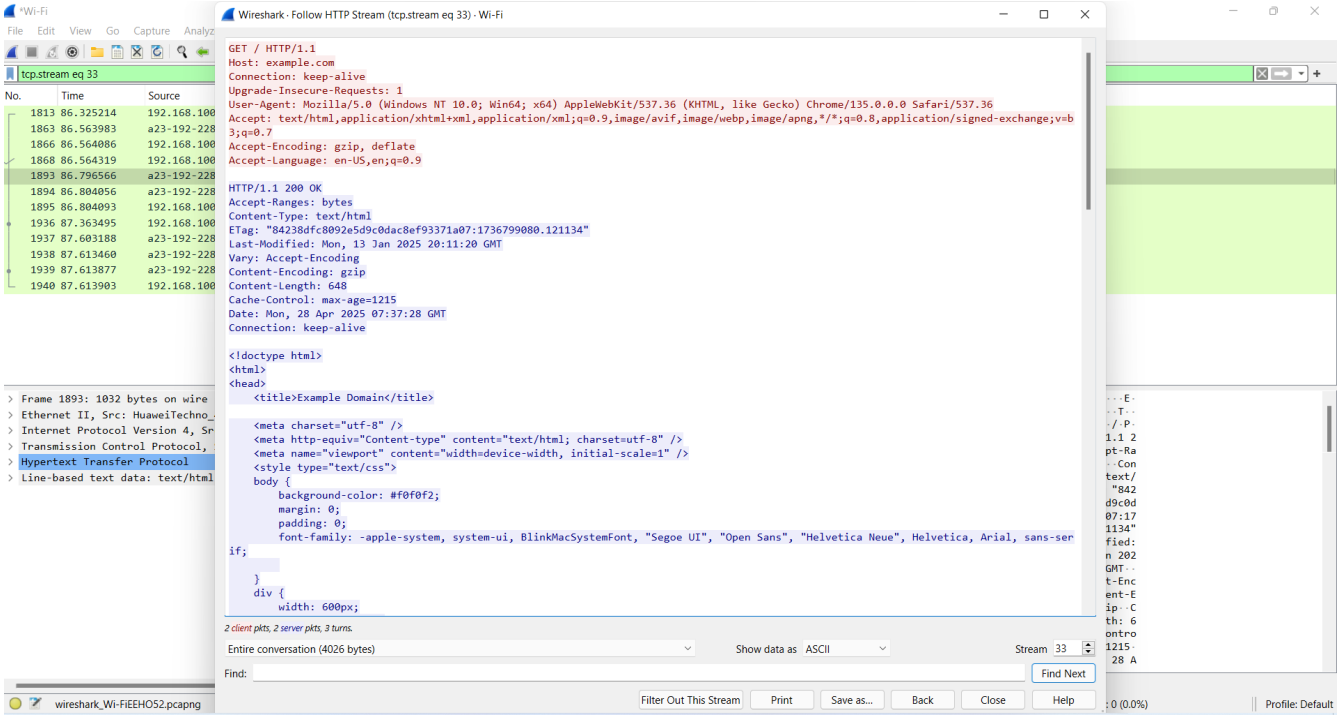




Step 5: Bonus - Follow the HTTP Stream

- 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!