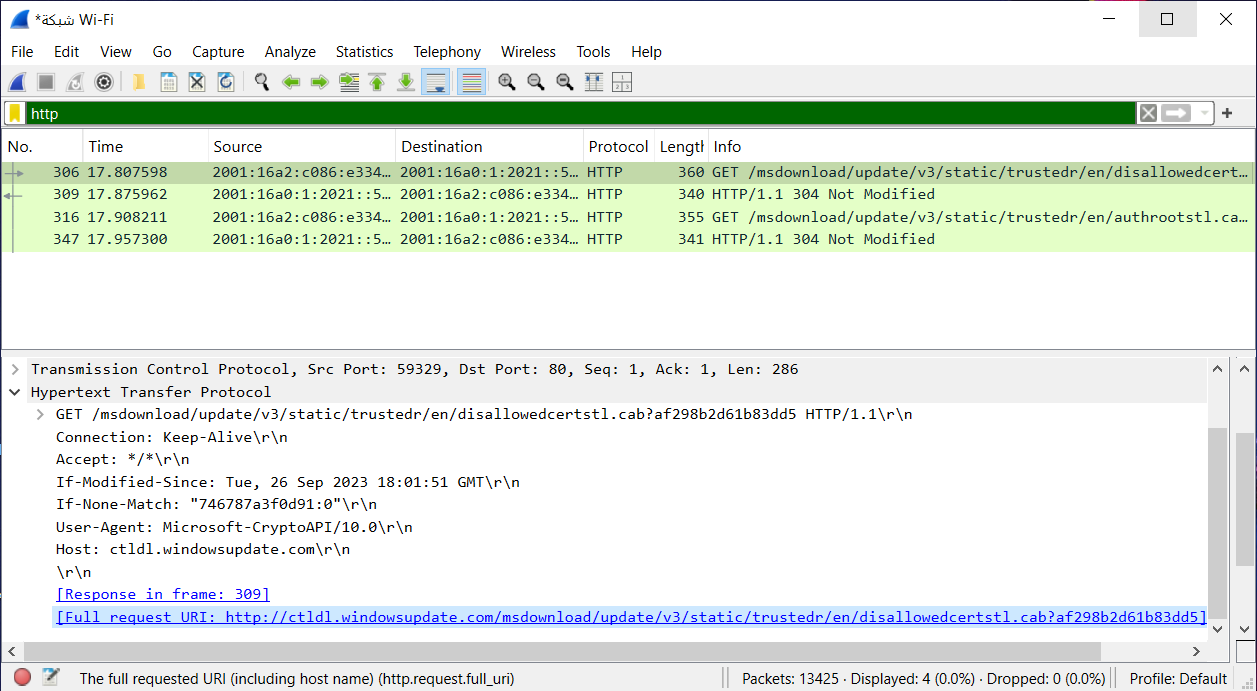
**LAB 2:**

**Reham Obaidallah Alharbi 411201881**

**Part 1: Capturing HTTP Traffic.**

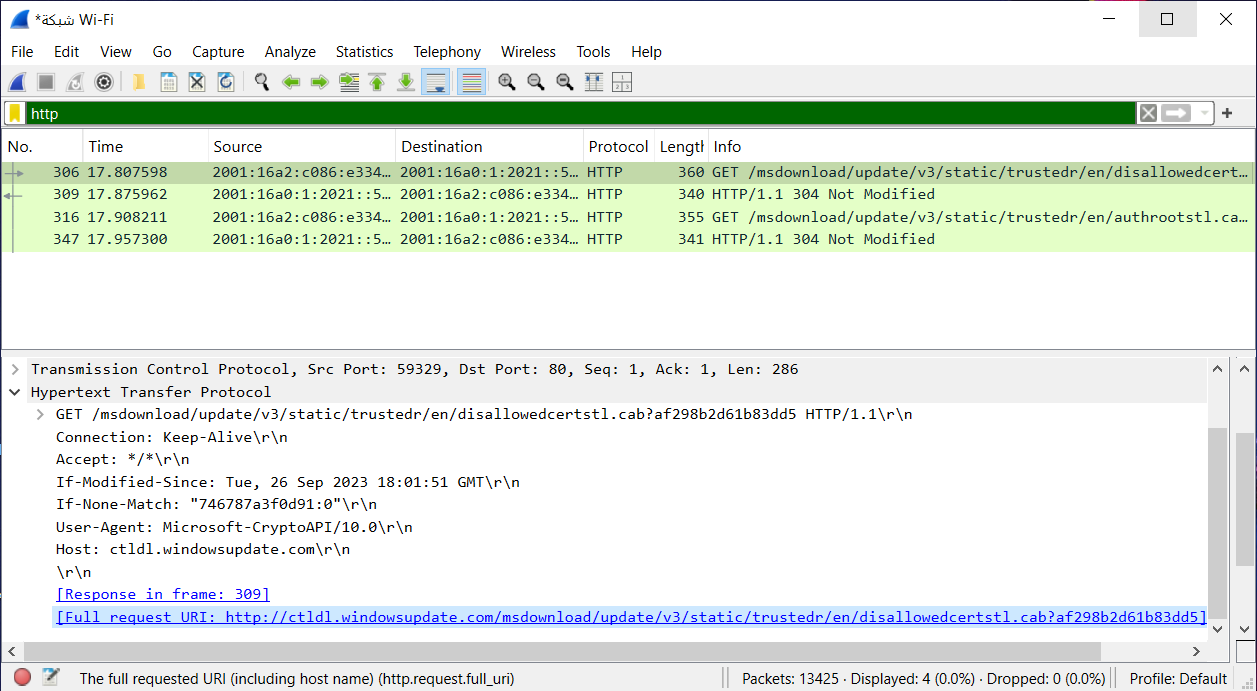
Select the network interface connected to the internet Wi-Fi

This provides an analysis of captured HTTP traffic using Wireshark



**HTTP Request Method:**

used to request resources from the server, was observed in all captured requests. It was employed to fetch update files, as demonstrated in the following request**:**





**HTTP Response Method:**

The server responded with a 200 OK status code, indicating the request was successful and the requested resource was returned.

صورة تحتوي على نص, الإلكترونيات, لقطة شاشة, برمجيات

تم إنشاء الوصف تلقائياً

**Note**:

**Method** : GET

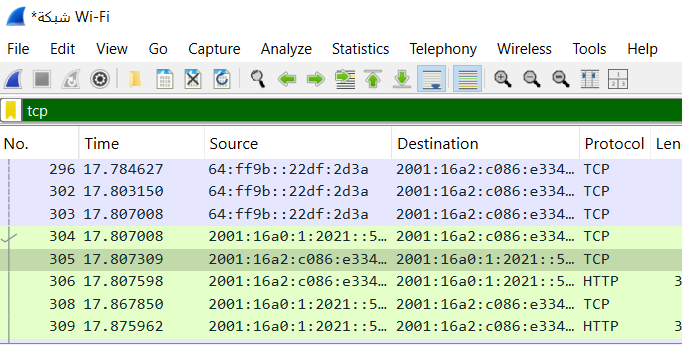
**URL**: [Full request URI: <http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?af298b2d61b83dd5>]

**Response codes**: 200 OK

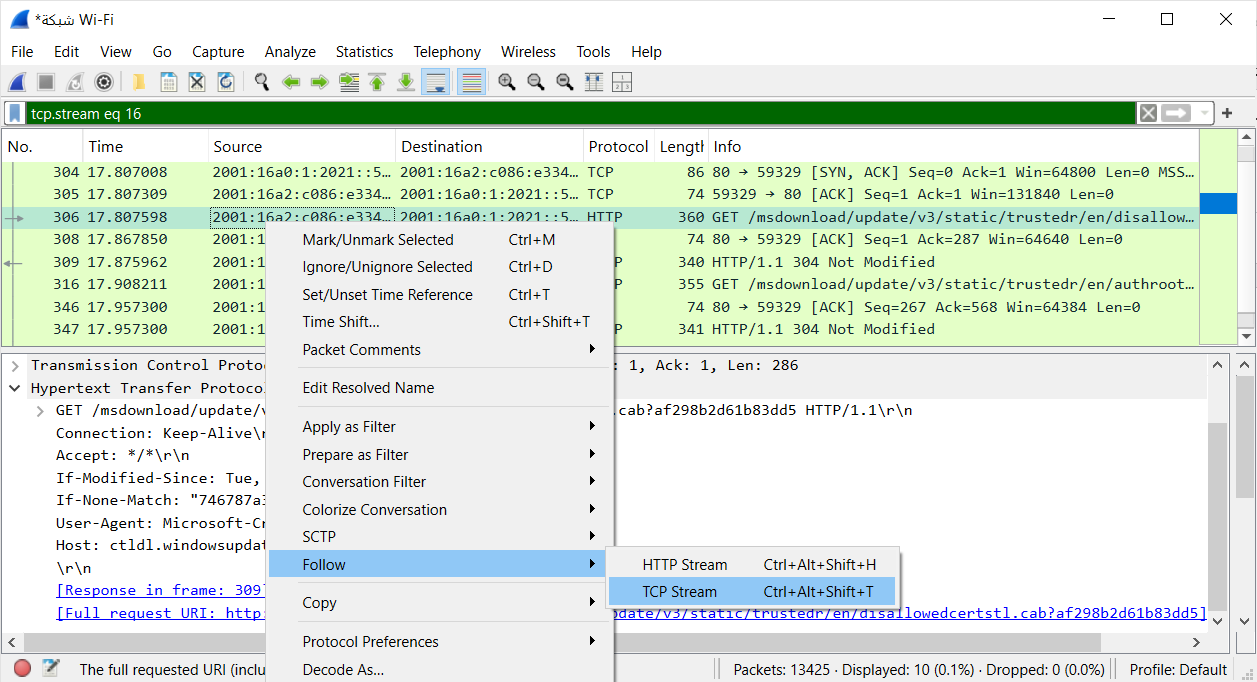
**Part 2: Analyzing TCP/IP Traffic.**

**Filter TCP packets**

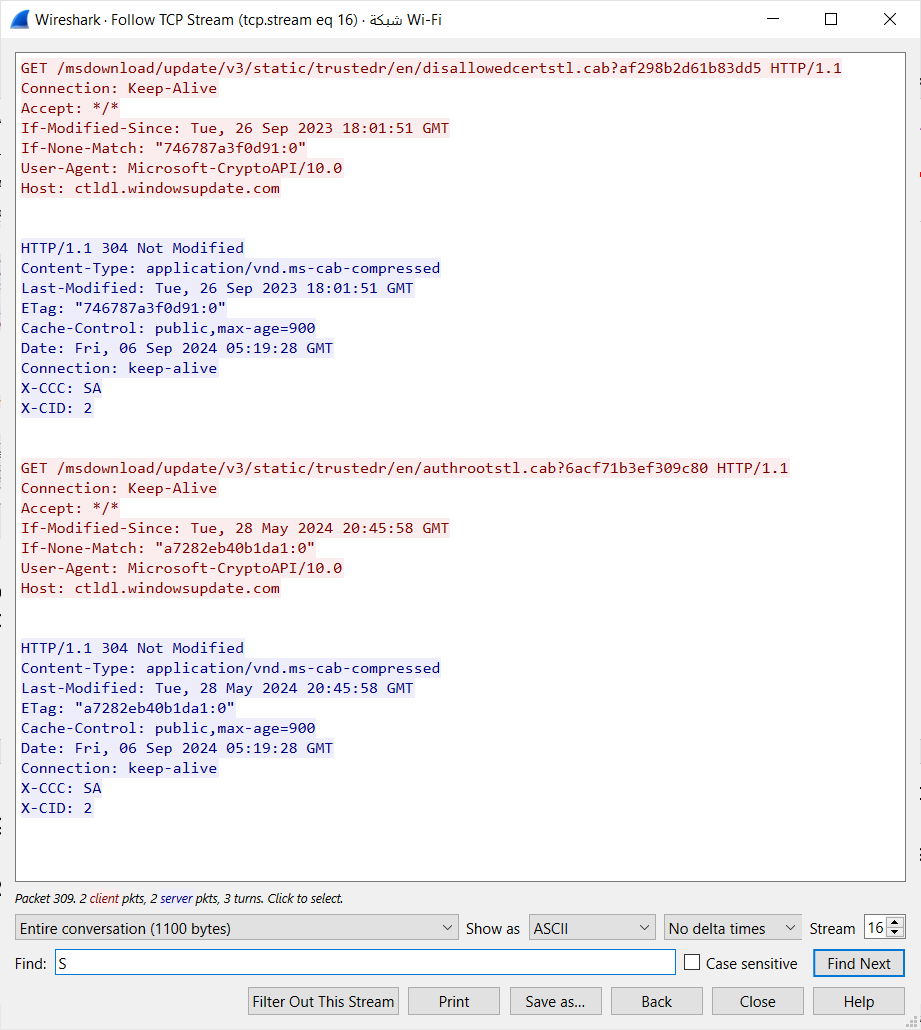
In the filter bar, type tcp and press Enter



Right-click on the packet and select "Follow" -> "TCP Stream".



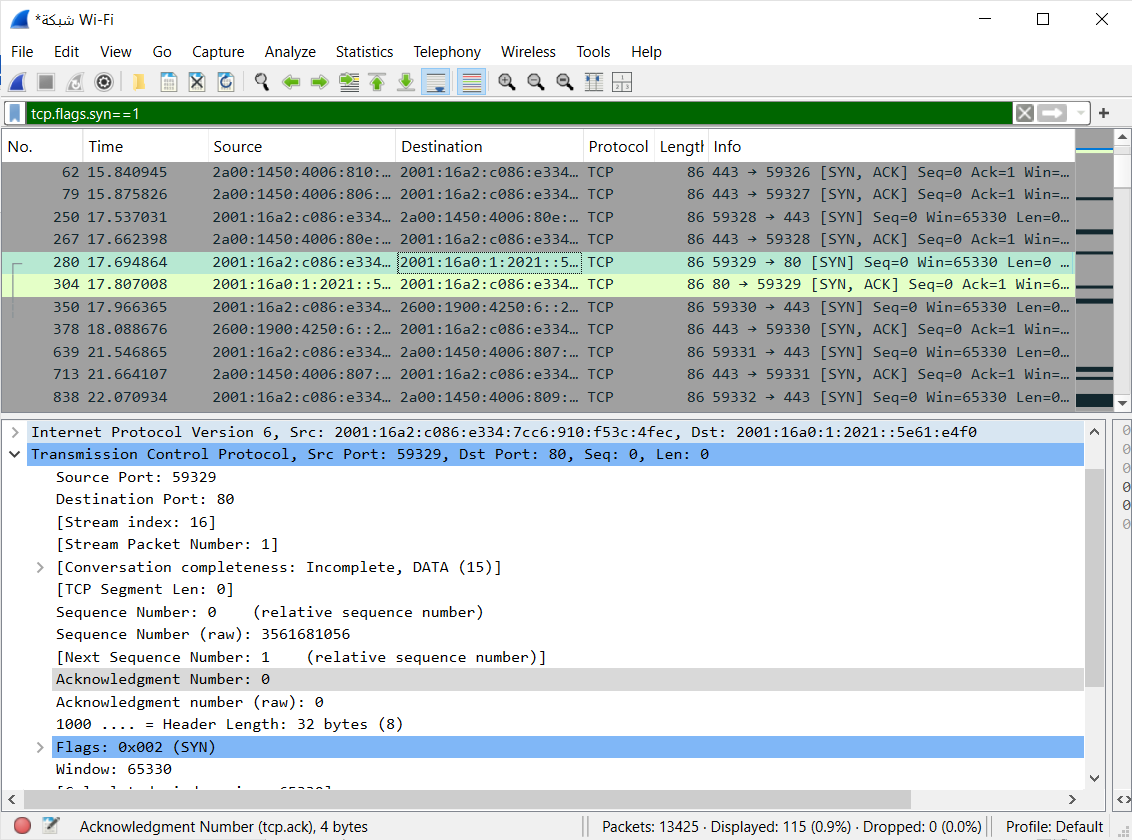
This shows the entire conversation between the client and server:



**Analyze TCP handshake and investigate Data Transfer and Termination:**

**Task2 :**

SYN : the sequence and acknowledgment numbers



SYN with sequence number 0 and ack number 0

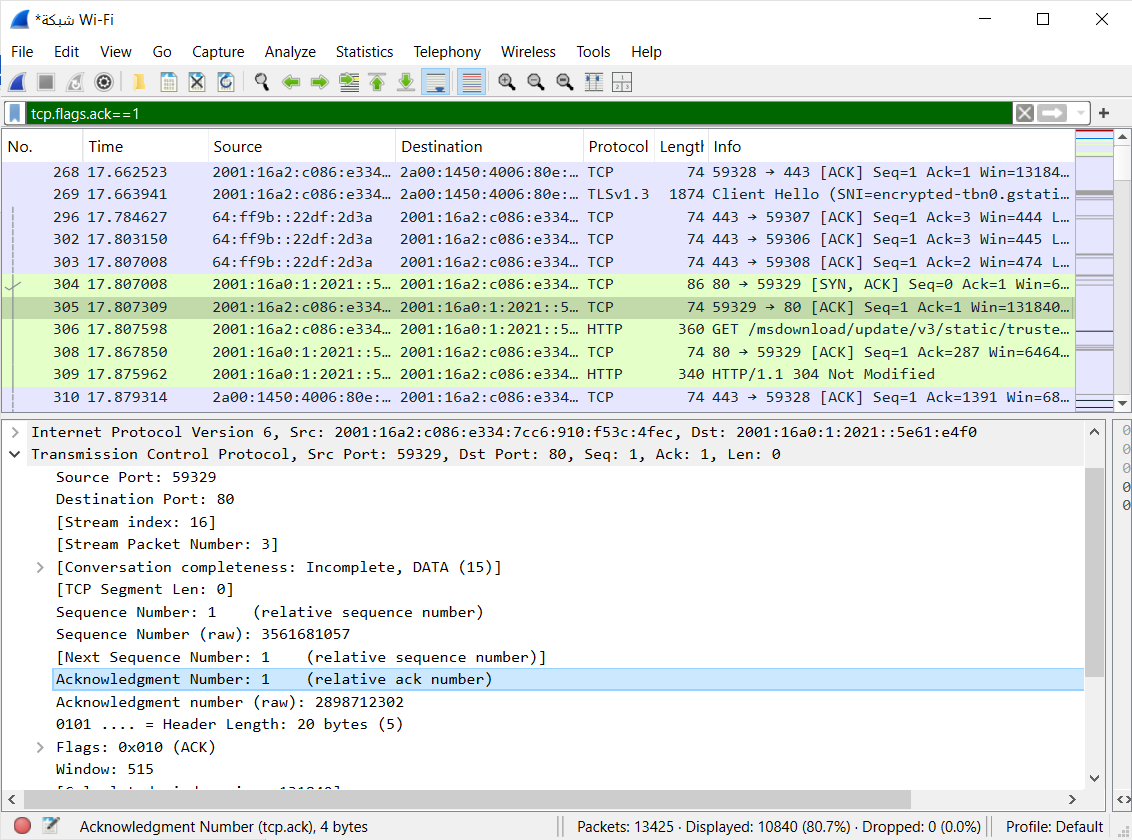
SYN-ACK: the sequence and acknowledgment numbers

صورة تحتوي على نص, الإلكترونيات, لقطة شاشة, برمجيات

تم إنشاء الوصف تلقائياً

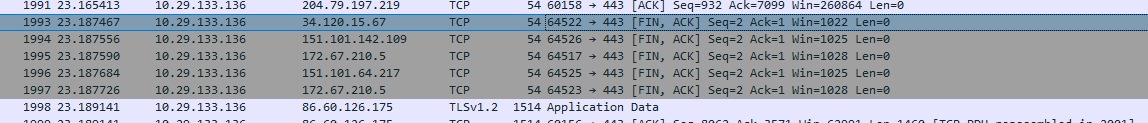
SYN-ACK with sequence number 0 and ack number 1

ACK: the sequence and acknowledgment numbers



ACK with sequence number 1 and ack number 1

Step 4:



**Part 3: Capturing and Analyzing UDP Traffic**

In the filter bar, type udp and press Enter

صورة تحتوي على نص, لقطة شاشة, برمجيات, صفحة ويب

تم إنشاء الوصف تلقائياً

source :49573

Det: 443

Length:42

**Compare the simplicity of UDP headers with TCP headers:**

**Explanation: UDP headers are simple because they don't require a persistent connection, unlike TCP which is more complex due to acknowledgment and data confirmation mechanisms.**

**Part 4: Comparing TCP and UDP by filling in the following tables. Save your work (e.g., in an MS Word document), and upload it to your online git repo.**

**Task 1: Fill in the following table and provide reasons.**

|  |  |  |
| --- | --- | --- |
|  | **TCP or UDP** | **Reasons** |
| Reliability and Connection Establishment | TCP | TCP ensures reliable connections with acknowledgment of data receipt. |
| Data Integrity and Ordering | TCP | TCP guarantees that data is received in the correct order and checks for integrity, whereas UDP sends data without order confirmation or integrity checks. |

**Task 2: Identify the use Cases and Performance of TCP and UDP.**

|  |  |  |
| --- | --- | --- |
|  | **TCP** | **UDP** |
| Use cases | File transfer, email, HTTP protocol | Video streaming, online gaming, VoIP |
| Performance | Slower due to confirmation of reliability and ordering | Faster as it doesn’t require connection confirmation or packet ordering |