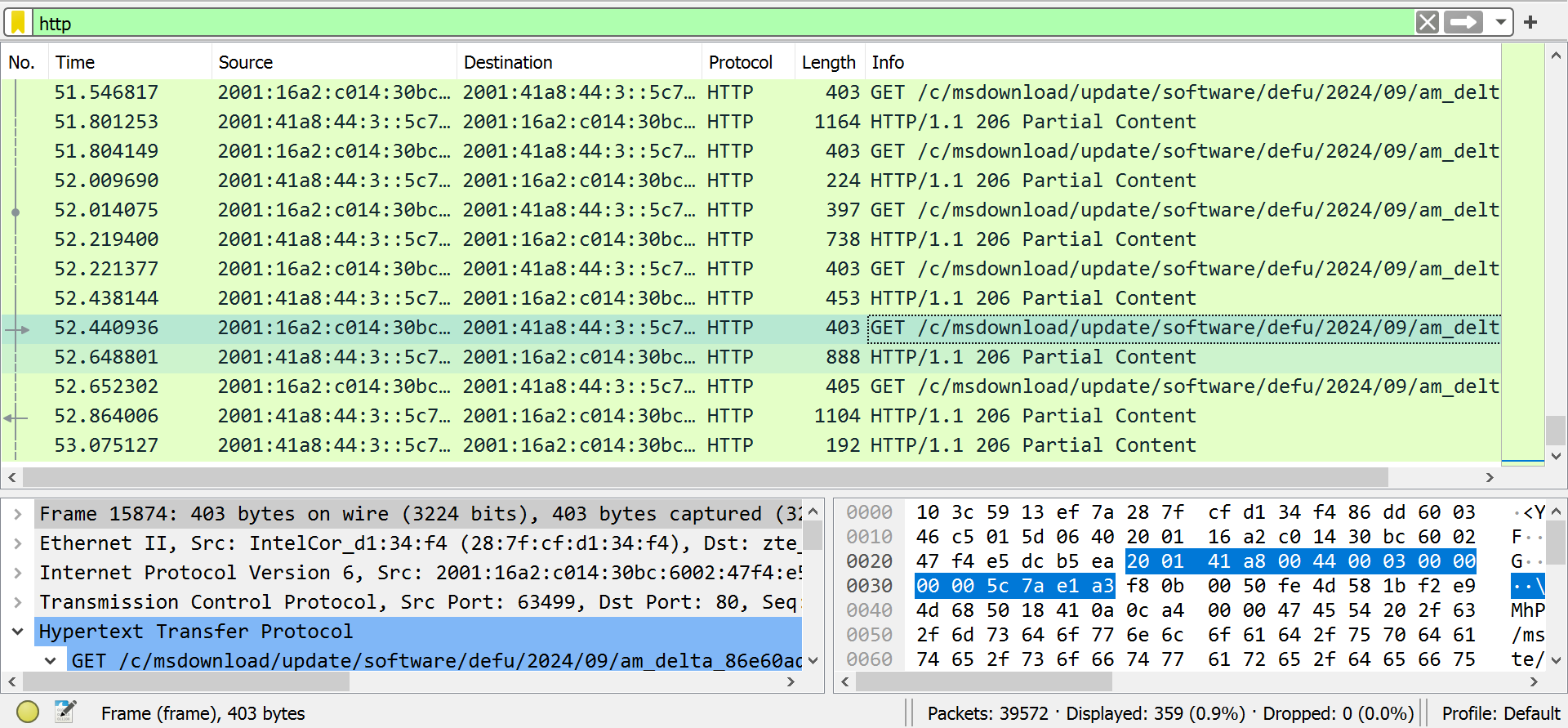
Wireshark Protocols Analysis Report

Name: Tala Fahad 411201913

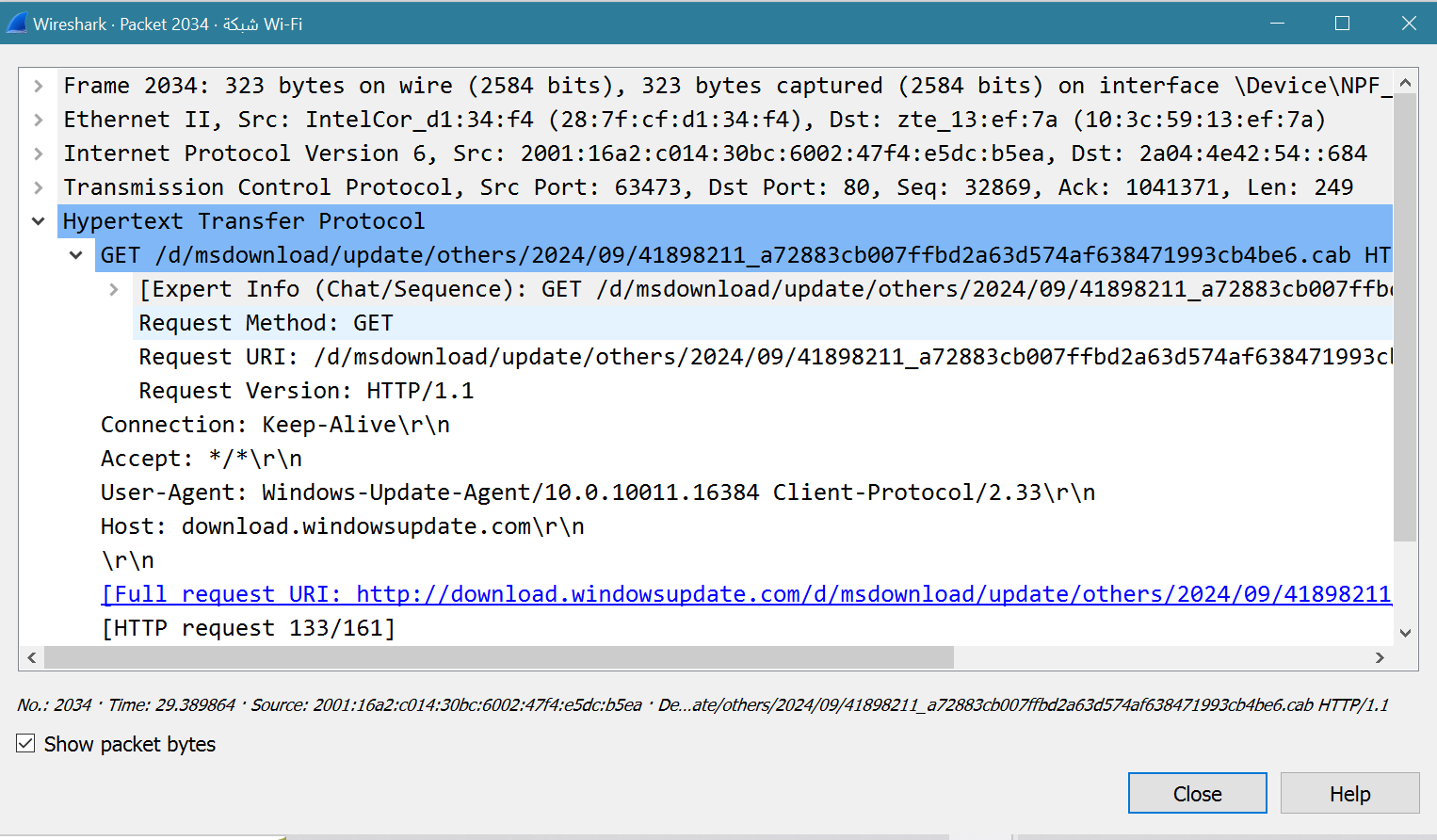
Introduction

This report provides an analysis of captured HTTP traffic using Wireshark.



HTTP Request Method

The HTTP GET method was observed in all captured requests. GET is used to request resources from the server, and in this case, it was employed to fetch update files, as seen in the following request:



HTTP Response Method

The server returned a 200 ok status code in response to the GET requests. This status code indicates that the request was successful, and the server has returned the requested resource.

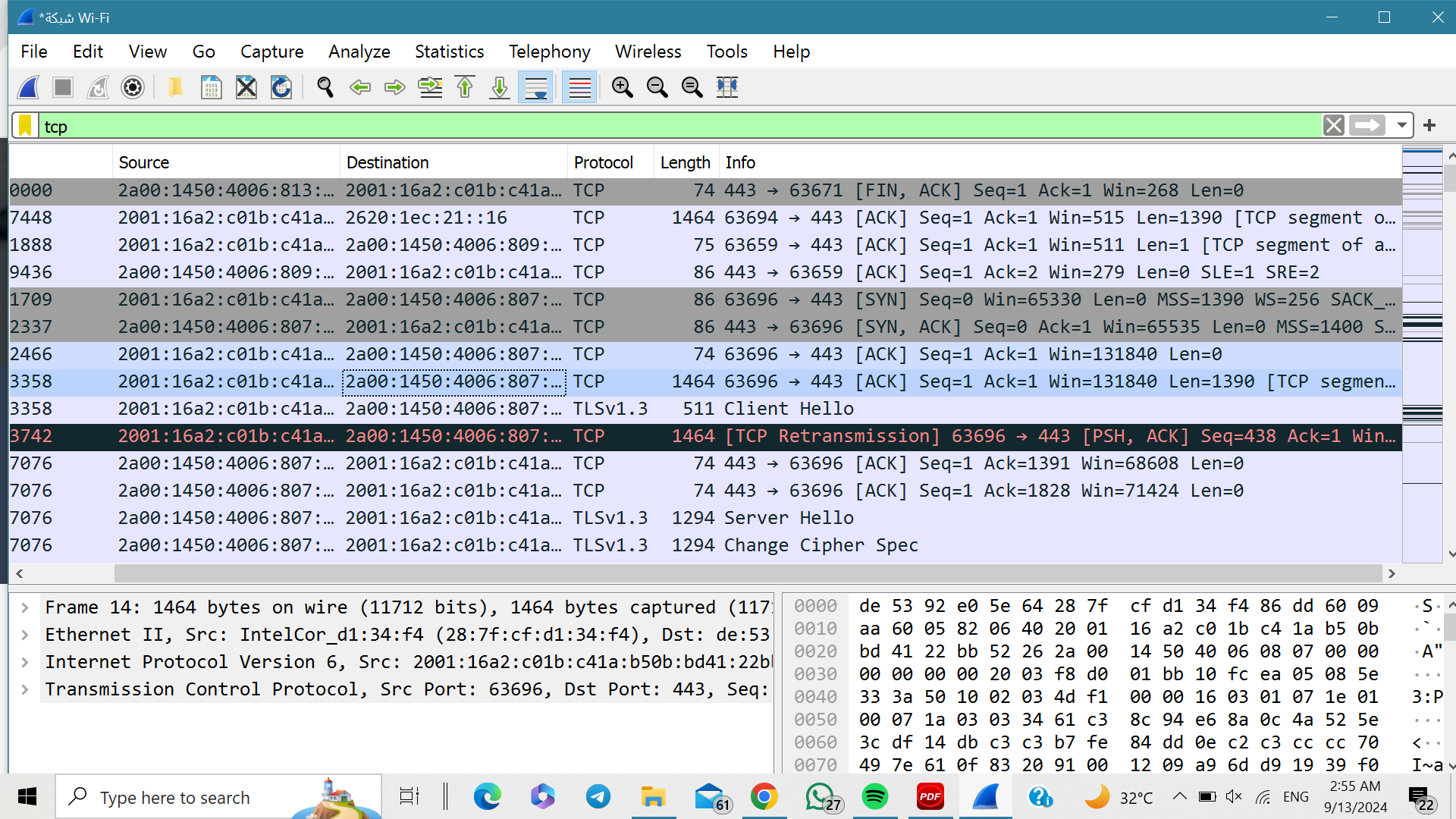
صورة تحتوي على نص, الإلكترونيات, لقطة شاشة, برمجيات

تم إنشاء الوصف تلقائياً

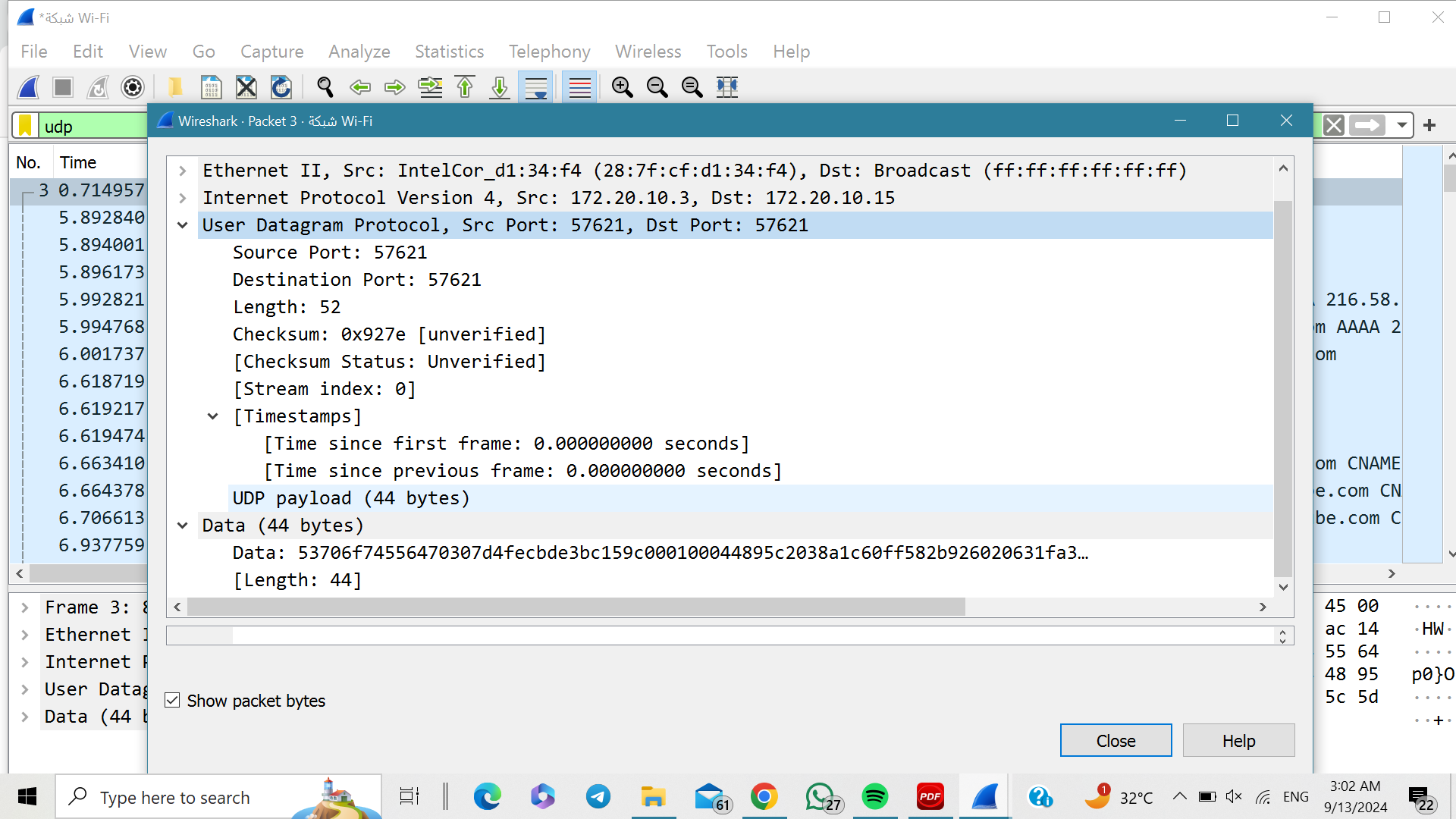
The Wireshark capture demonstrated the typical behavior of an HTTP GET request and 200 ok responses, which indicates that the request was successfully processed, and the requested data was fully returned.

TCP Protocol

The TCP three-way handshake:



UDP Protocol



صورة تحتوي على نص, الإلكترونيات, لقطة شاشة, برمجيات

تم إنشاء الوصف تلقائياً

Part 4: Comparing TCP and UDP

|  |  |  |
| --- | --- | --- |
|  | TCP or UDP | Reasons |
| Reliability & Connection Establishment | TCP **(**Reliable**)** | TCP ensures data is delivered in the correct order by establishing a connection by handshaking |
| Data Integrity and Ordering | TCP | TCP ensures that all data arrives using sequence number and acknowledgement systems, as well as checksum to ensure the data is not corrupted |

|  |  |  |
| --- | --- | --- |
|  | TCP | UDP |
| Use cases | Web browsing, email, http https | Streaming media (audio/video), online gaming |
| Performance | Slower due to connection overhead and error correction | Faster since UDP doesn't have error checking or retransmission, |