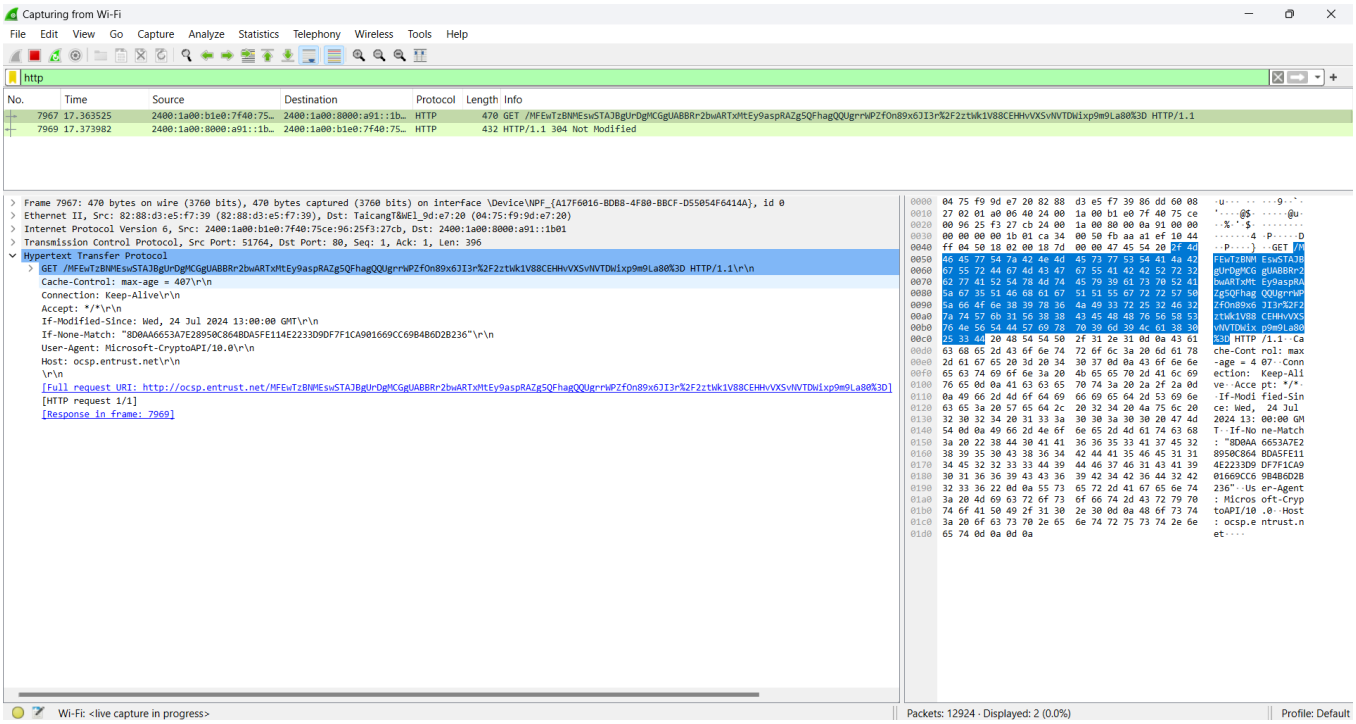
1. Capture the packet while an http request also capture the request. Dissect the request and response.



➢ **Let's dissect the HTTP request and response captured in the Wireshark screenshot shown above.**

❖ HTTP Request Details

1. Frame Information:

- **Frame Number**: 7967
- **Time**: 17.363525 seconds
- **Source**: 2400:1a00:b000:9127:20:: (IPv6 address)

- **Destination**: 2400:1a00:b00e:f740:75:: (IPv6 address)
- **Protocol**: HTTP
- **Length**: 470 bytes

2. Ethernet II Details:

- **Source MAC Address**: 82:88:d3:e5:f7:39
- **Destination MAC Address**: 04:75:f9:90:e7:20

3. Internet Protocol Version 6 (IPv6) Details:

- **Source IP Address**: 2400:1a00:b000:9127:20::
- **Destination IP Address**: 2400:1a00:b00e:f740:75::
- **Next Header**: TCP (6)
- **Hop Limit**: 128

4. Transmission Control Protocol (TCP) Details:

- **Source Port**: 51764
- **Destination Port**: 80 (HTTP)
- **Sequence Number**: 1
- **Acknowledgment Number**: 1
- **Header Length**: 32 bytes
- **Flags**: 0x018 (PSH, ACK)
- **Window Size**: 8192

- **Checksum**: Correct
- **Urgent Pointer**: 0

5. Hypertext Transfer Protocol (HTTP) Details:

- **Request Method**: GET
- **Request URI**: http://ocsp.entrust.net/MEwFZzBNMEswSTAJBgUrDgMCGgUABBrr2bWARtXMtEy9sasPRAZg5OFhaqQOQUgrNwPZfon89xGj73k%2F2zt1tk1V88CEHHvVXSvNTDWiJxp9mL8a0%3D
- **Request Version**: HTTP/1.1

Headers:

- **Cache-Control**: max-age = 407
- **Connection**: Keep-Alive
- **Accept**: */*
- **If-Modified-Since**: Wed, 24 Jul 2024 13:00:00 GMT
- **If-None-Match**: "8D0AA6535A72B59C68DAB5E114E2233D9DF7F1CA0916690C69B48D6DB2236"
- **User-Agent**: Microsoft-CryptoAPI/10.0
- **Host**: ocsp.entrust.net

❖ HTTP Response Details

1. Frame Information:

- **Frame Number**: 7969
- **Time**: 17.379382 seconds
- **Source**: 2400:1a00:b00e:f740:75:: (IPv6 address)
- **Destination**: 2400:1a00:b000:9127:20:: (IPv6 address)
- **Protocol**: HTTP
- **Length**: 432 bytes

2. Hypertext Transfer Protocol (HTTP) Details:

- **Response Version**: HTTP/1.1
- **Status Code**: 304 (Not Modified)
- **Response Phrase**: Not Modified

Headers:

- **Cache-Control**: max-age = 407
- **Date**: Wed, 24 Jul 2024 13:00:00 GMT
- **Server**: Microsoft-IIS/10.0
- **X-Powered-By**: ASP.NET
- **Content-Length**: 0

Analysis

❖ Request Analysis:

- The client (source) is sending an HTTP GET request to the server (destination) at ocsp.entrust.net.
- The request includes several headers:
  - **Cache-Control**: The client requests that the response be cached for 407 seconds.
  - **Connection**: Keep-Alive to keep the connection open for further requests.
  - **Accept**: */* meaning the client accepts any type of response content.
  - **If-Modified-Since** and **If-None-Match**: These headers are used for cache validation. The client is asking the server to return the resource only if it has been modified since the specified date or if the entity tag (ETag) has changed.

❖ Response Analysis:

- The server responds with a status code 304 Not Modified, indicating that the requested resource has not been modified since the date provided in the If-Modified-Since header and the ETag provided in the If-None-Match header matches.

- The response includes caching directives and server information, but no content (Content-Length: 0).

This exchange is typical for validating cached resources to avoid re-downloading unchanged content, which conserves bandwidth and reduces server load.