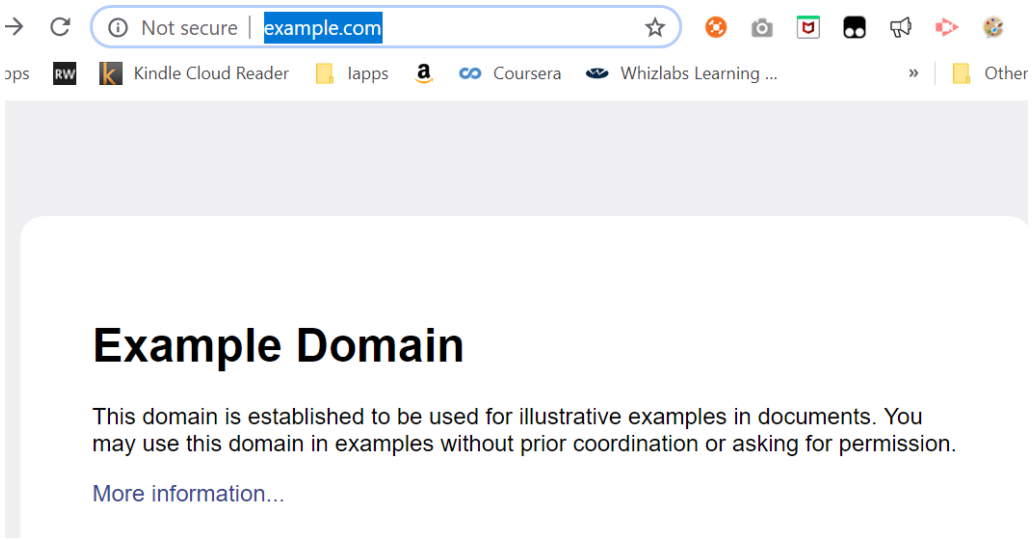
# Practical 06
# Capture HTTP Traffic and IP Traffic

A. Capture HTTP Traffic
B. Analyze HTTP Request Traffic
C. Analyze HTTP Response Traffic
D. Analyze HTTPS Traffic

## A. Capture HTTP Traffic

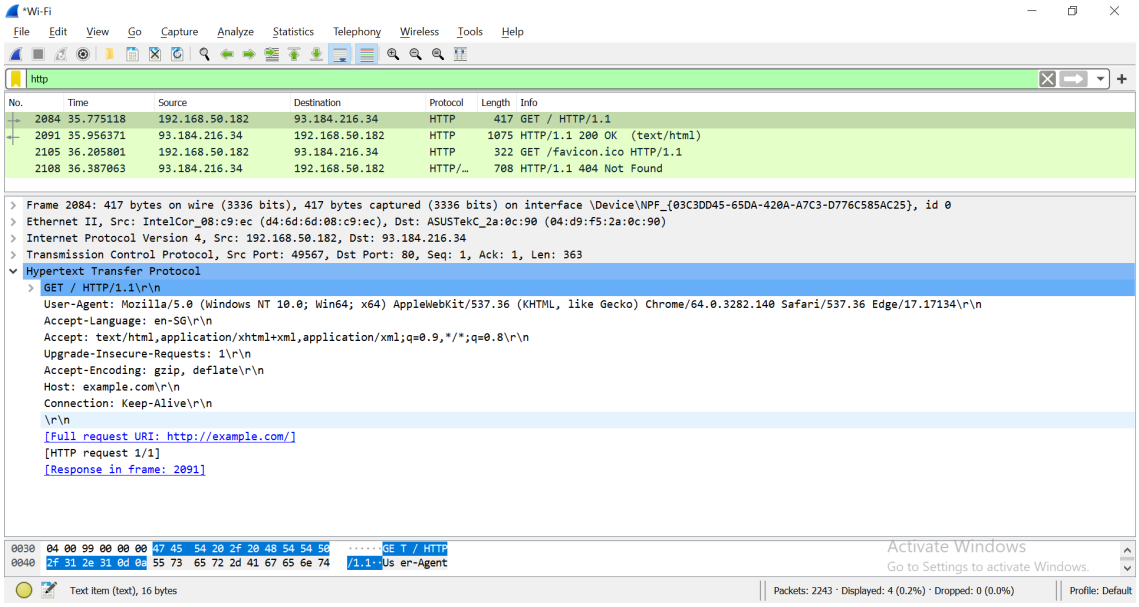
1. Open a new browser tab.
2. Start a Wireshark capture.
3. Browse the web page http://example.com.




4. Stop Wireshark capture.

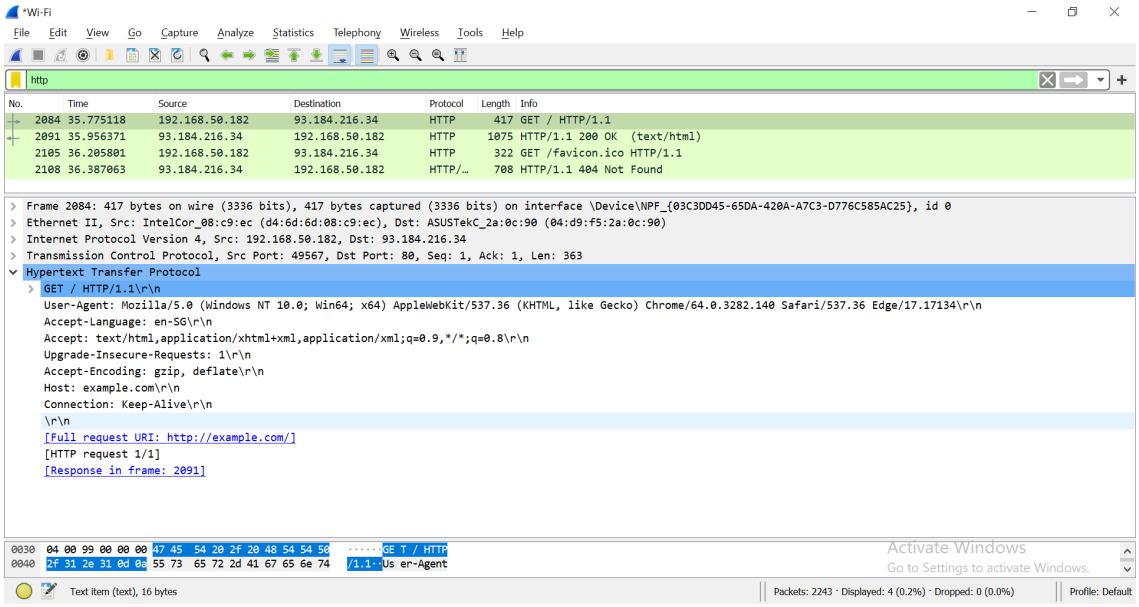
## B. Analyze HTTP Traffic

1. Observe the traffic captured in the top Wireshark packet list pane. To view only HTTP traffic, type tcp.port == 80 (lower case) or **http** in the Filter box and press Enter.
2. Select the HTTP packet labelled "*GET / HTTP/1.1*"

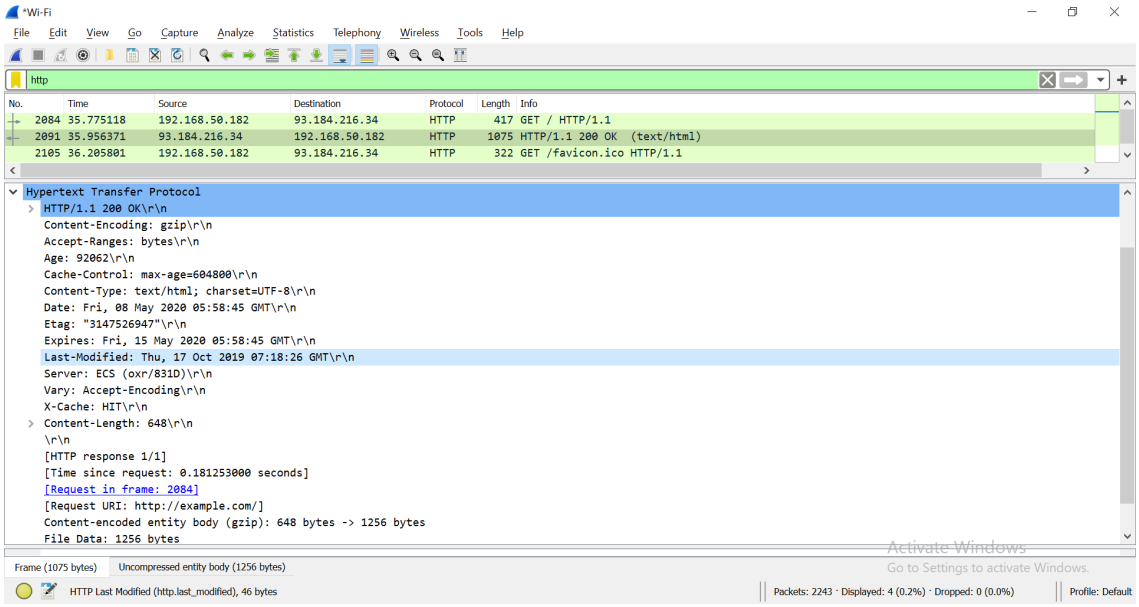



3. Observe the packet details in the middle Wireshark packet details pane. Notice that it is an Ethernet II / Internet Protocol Version 4 / Transmission Control Protocol / Hypertext Transfer Protocol.

4. Observe the HTTP request.



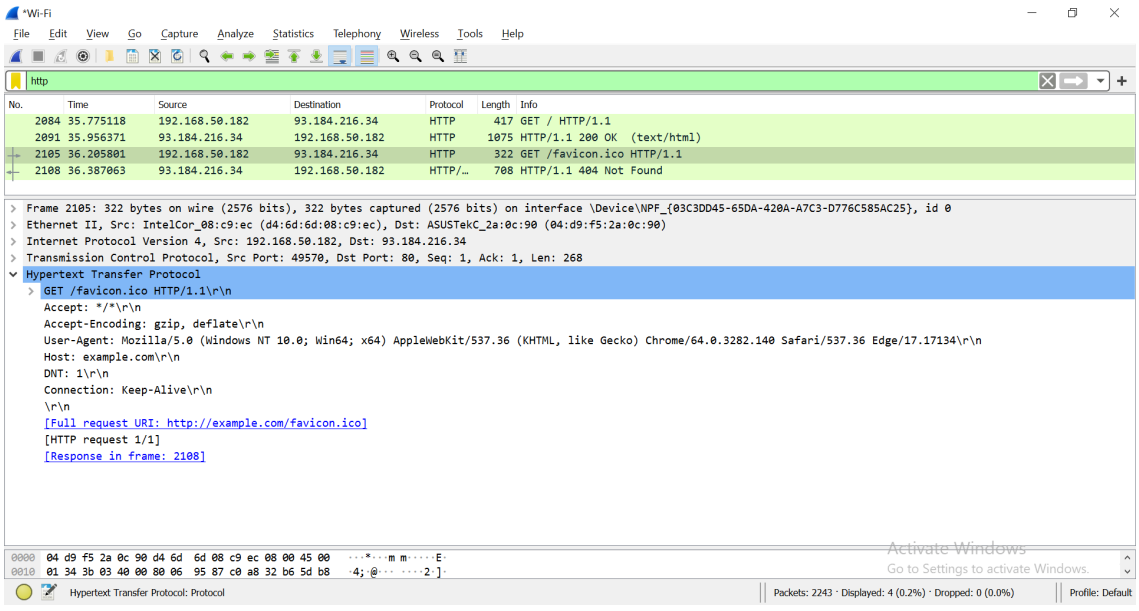
5. Observe the HTTP response.




What is the HTTP response code for the request?

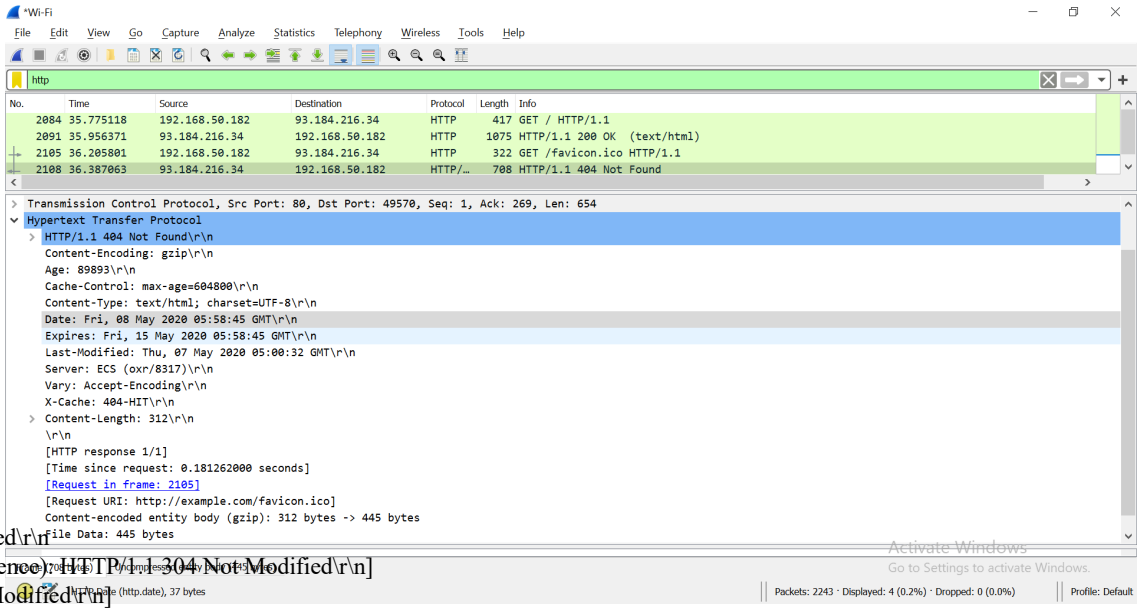
GET /SGX/LCWL/Windows/sgx_white_list_cert.bin HTTP/1.0\r\n
[Expert Info (Chat/Sequence): GET /SGX/LCWL/Windows/sgx_white_list_cert.bin HTTP/1.0\r\n]
Request Method: GET
Request URI: /SGX/LCWL/Windows/sgx_white_list_cert.bin
Request Version: HTTP/1.0

6. Examine the HTTP packet labelled as "*GET /favicon.ico HTTP/1.1*".




**Note:** If you don't have the above HTTP request in Wireshark, you can use another browser to send request to example.com again.

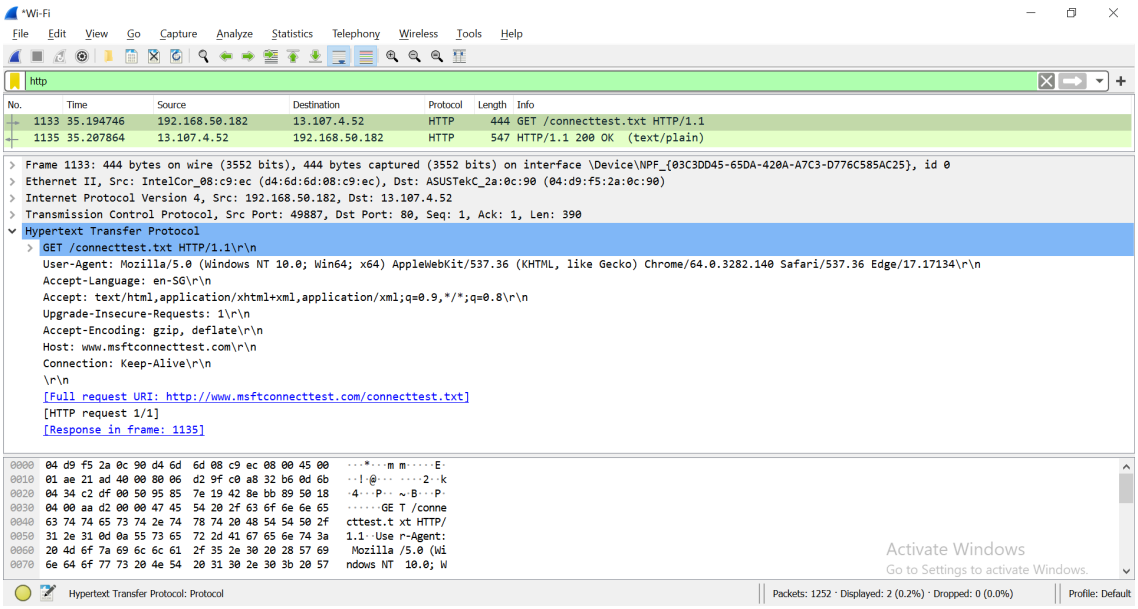
Observe the HTTP response.




HTTP/1.1 304 Not Modified\r\n
[Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]
[HTTP/1.1 304 Not Modified\r\n]
[Severity level: Chat]
[Group: Sequence]
Response Version: HTTP/1.1
Status Code: 304
[Status Code Description: Not Modified]
Response Phrase: Not Modified

What is the HTTP response code for the request?

7. Start Wireshark capture.
Browse the web page http://www.msftconnecttest.com/connecttest.txt.
Stop Wireshark capture.
Examine the HTTP request labelled as "*GET /connecttest.txt HTTP/1.1*"



What resource is the browser requesting for?

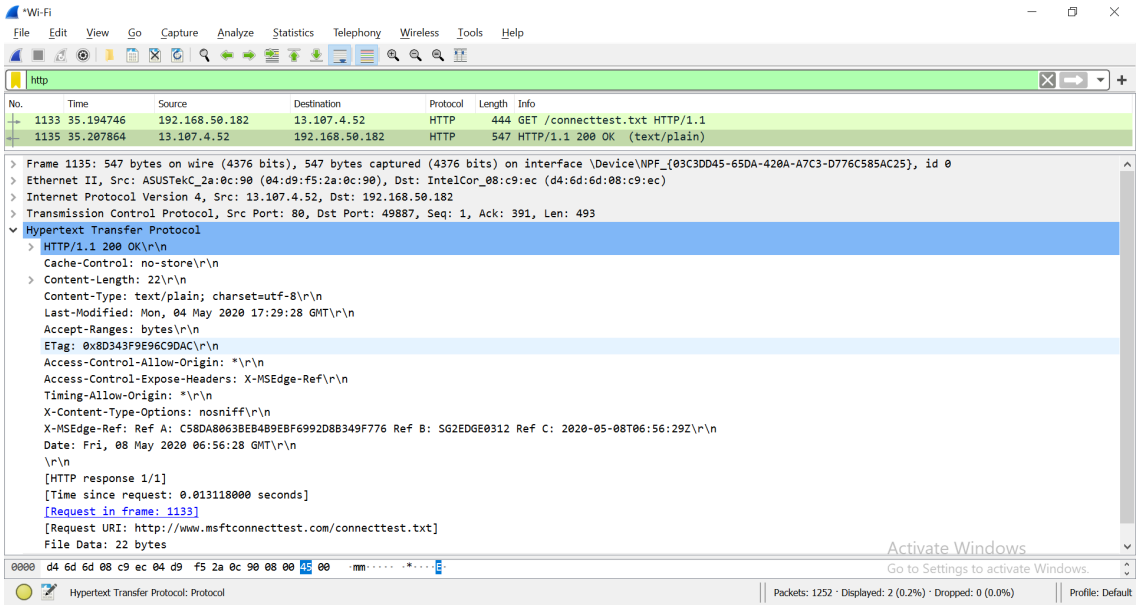
| | |
|---|---|
| Requested resource | /msdownload/update/v3/static/trustedr/en/authrootstl.cab?0ac88760a4c84671 |

Based on the User-Agent field in the HTTP header, what is the type of browser?

| | |
|---|---|
| User-Agent | Microsoft-CryptoAPI/10.0 |
| Type of browser | Microsoft Edge |

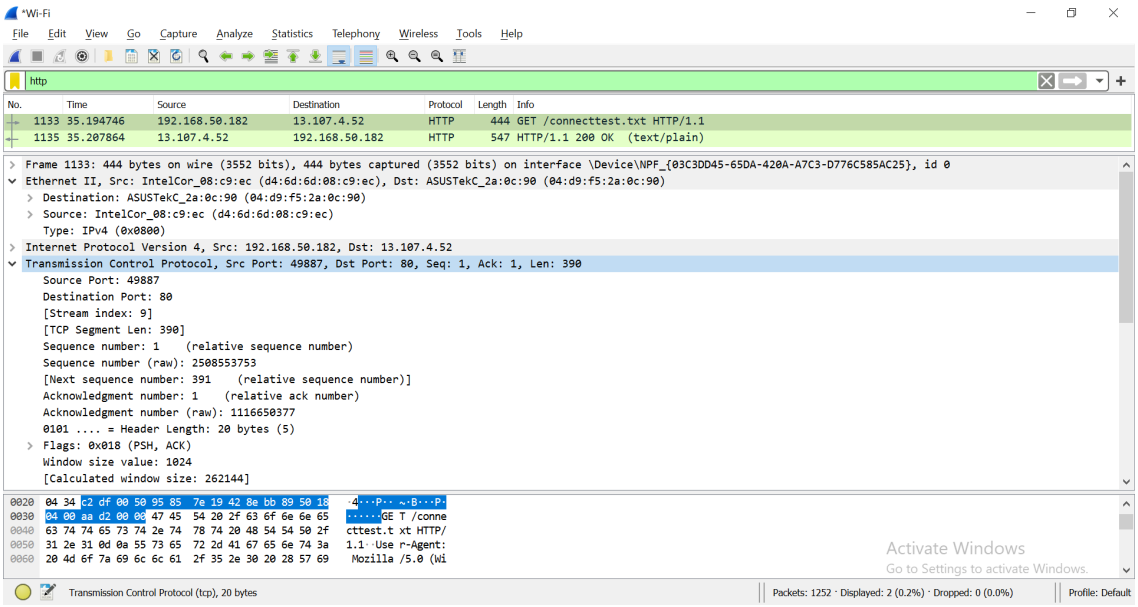
**User-Agent**

Observe the HTTP response.



## C. Analyze TCP Packet containing HTTP Traffic

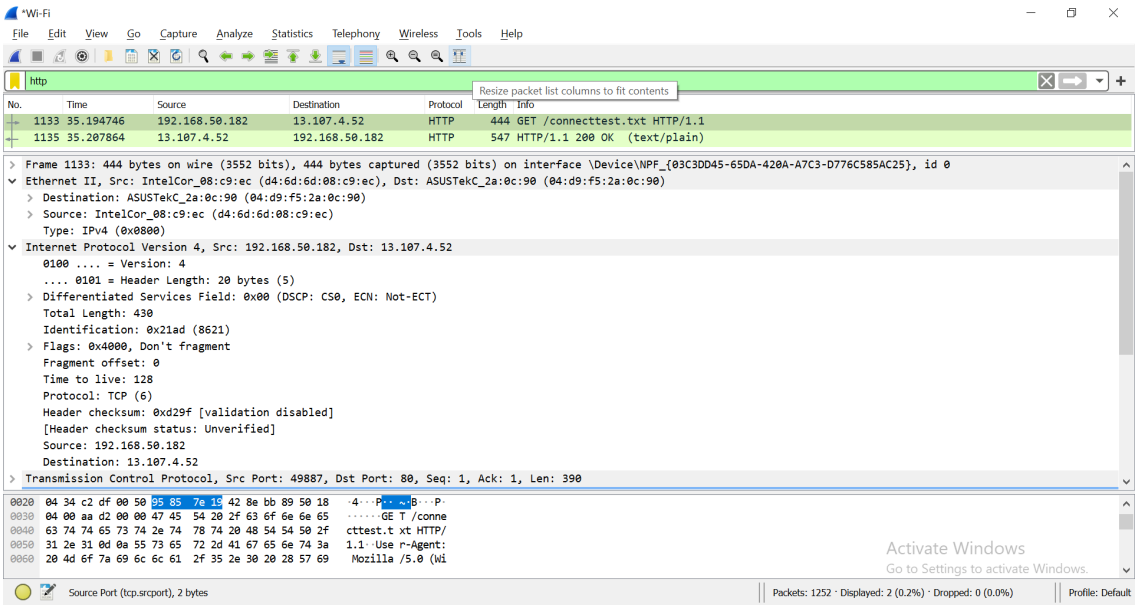
1. Examine the HTTP request labelled as "*GET /connecttest.txt HTTP/1.1*"




2. Write down the source and destination Port Number.

| | Hex | Binary | Decimal |
|---|---|---|---|
| Source port | c3 | 0000 | 27 |
| Destination port | .P | 0000 | 00 50 |

3. Expand Internet Protocol Version 4 to view IP Details. Observe the Source IP address and Destination IP address.




| | |
|---|---|
| Source IP address | 13.107.4.52 |
| Is the source IP address, your IP address? (true or false) | false |

What is the IP address of *http://www.msftconnecttest.com*?

| Domain Name | IP Address |
|---|---|
| http://www.msftconnecttest.com/ | 13.107.4.52 |

Expand Ethernet II to view Ethernet details. Find the source MAC Address and destination MAC Address of the frame.

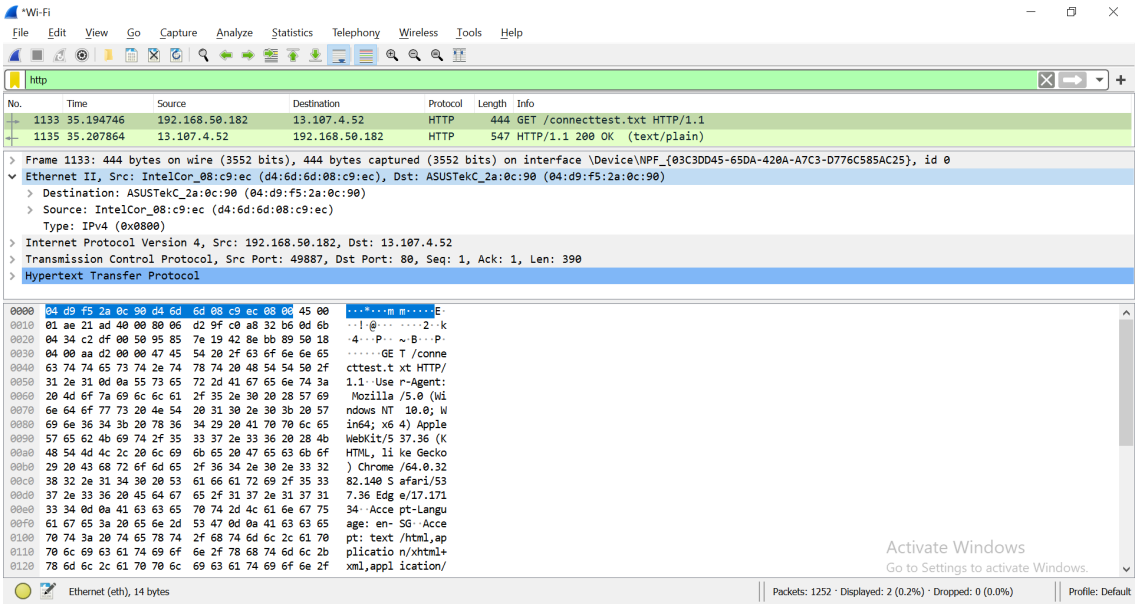
| | |
|---|---|
| Source MAC Address | 8c:16:45:f3:7c:64 |
| Destination MAC Address | Ethernet II, Src: LCFCHeFe_f3:7c:64 (8c:16:45:f3:7c:64), Dst: TP-Link_6d:b5:b8 (10.27.f5.6d.b5.b8) |

**(OPTIONAL)**

4. Observe the Destination address. Notice that the destination address is the IP address of the DNS server.

| | |
|---|---|
| Destination IP address | |
| Is the destination IP address your DNS Server? (true or false) | |

5. Expand Ethernet II to view Ethernet details.



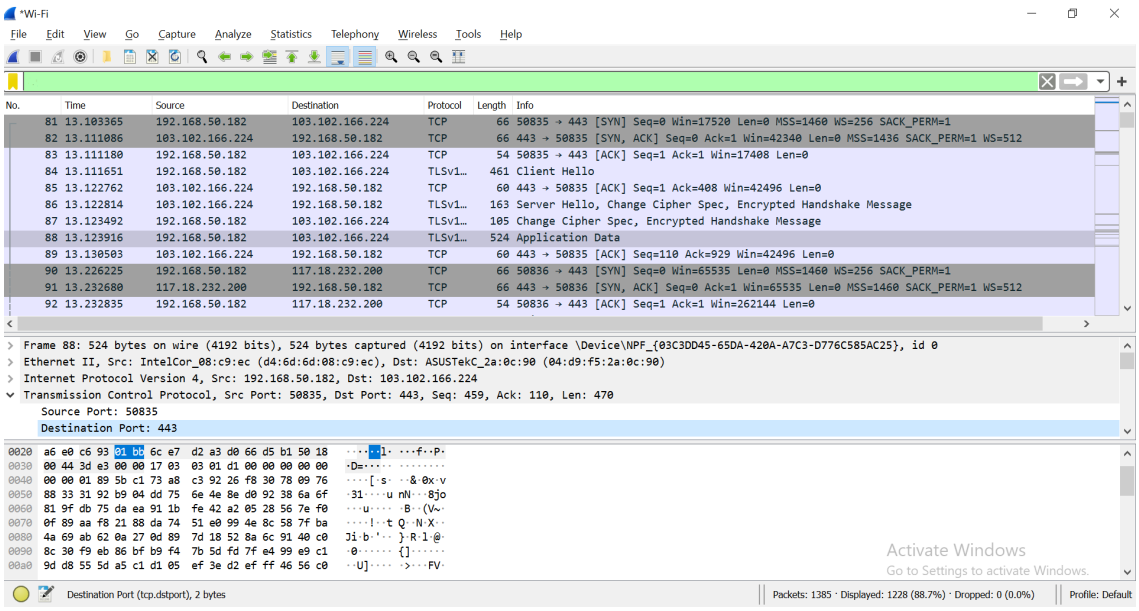

6. Observe the Destination and Source fields. The destination should be your default gateway's MAC address and the source should be your MAC address. You can use ipconfig /all and arp -a to confirm.

**(OPTIONAL)**

## D. Analyze TCP Packet containing HTTPS Traffic

https://en.wikiversity.org/wiki/Wireshark/HTTPS

1. Open a new web browser window or tab.
2. Start a Wireshark capture.
3. Navigate to https://en.wikiversity.org.
4. Stop the Wireshark capture.




5. Write down the source and destination Port Number.

| | Hex | Binary | Decimal |
|---|---|---|---|
| Source port | | | |
| Destination port | | | |

Reference: HTTP/HTTPS Analysis Using Wireshark

**Practical Reflection**

Suggested contents:

1. What have you learnt?
2. Any difficulties encountered and how you solved the problems?

1. How to see the source of the IP address
2. Yes cannot find some of the things, so I restart my laptop

*End of Practical*