

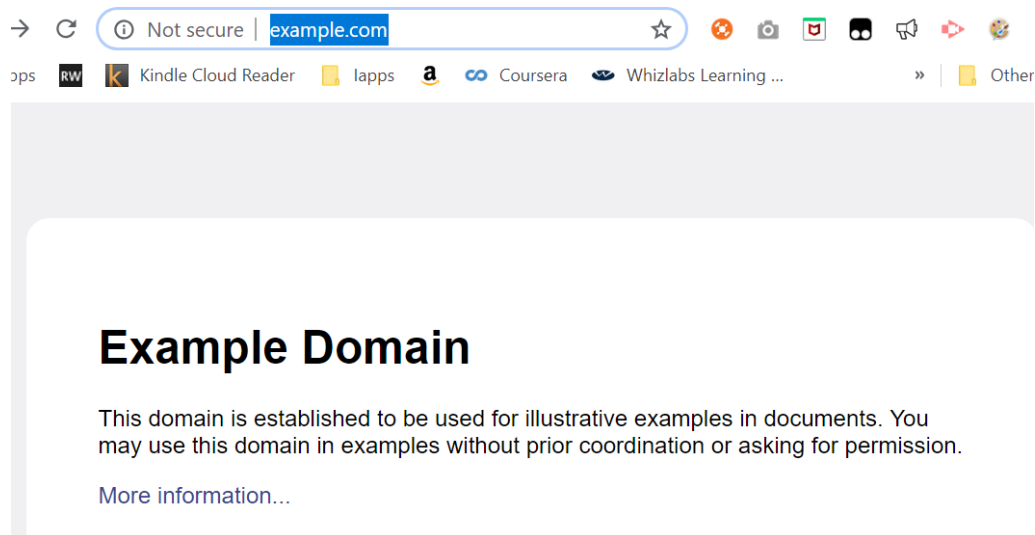
## Practical 06

### 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

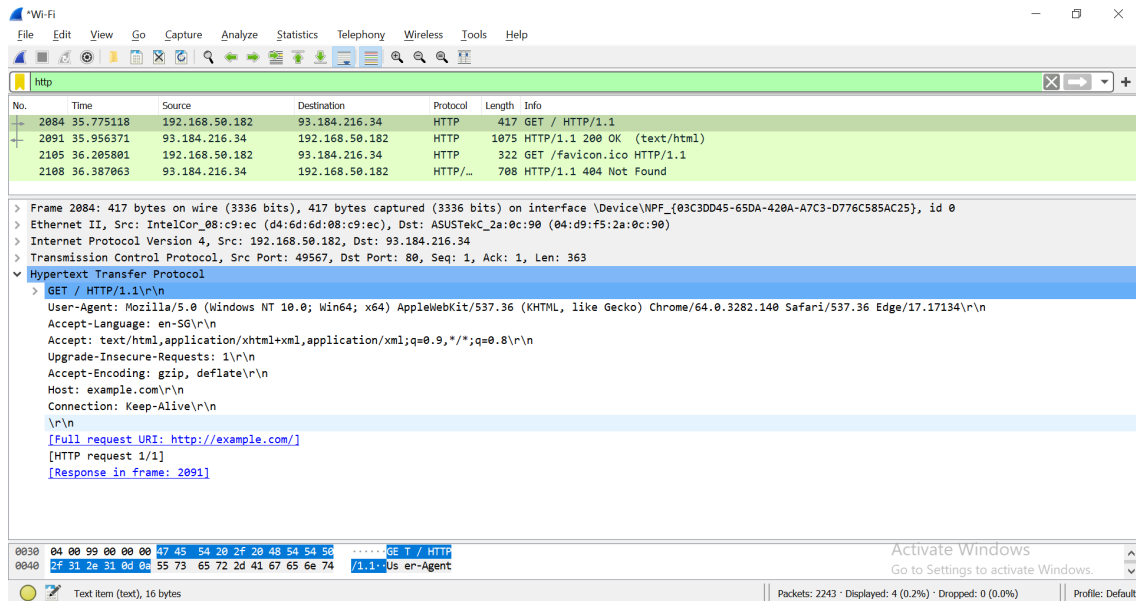
1. Open a new browser tab.
2. Start a Wireshark capture.
3. Browse the web page <http://example.com>.



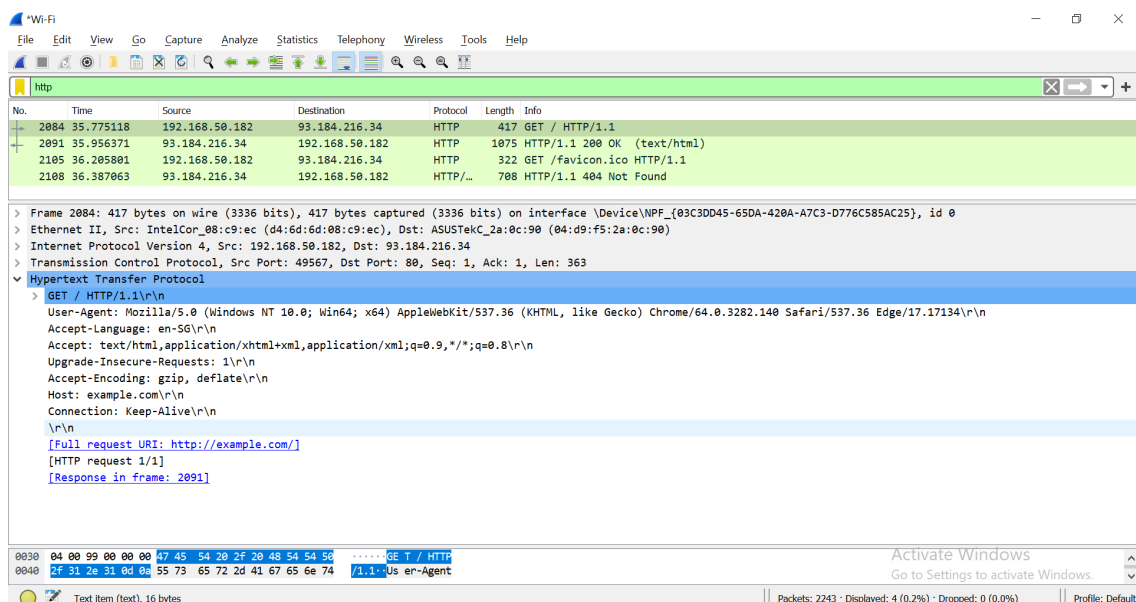
4. Stop Wireshark capture.

## B. Analyze HTTP Traffic

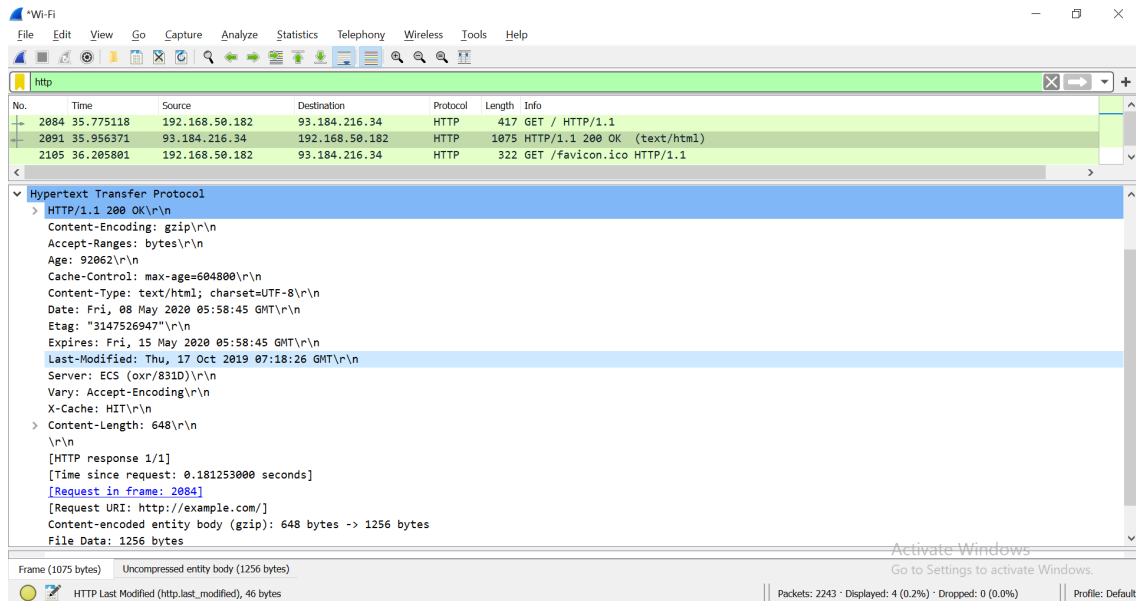
1. Observe the traffic captured in the top Wireshark packet list pane. To view only HTTP traffic, type `tcp.port == 80` (lower case) or **http** in the Filter box and press Enter.
2. Select the HTTP packet labelled “*GET / HTTP/1.1*”



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

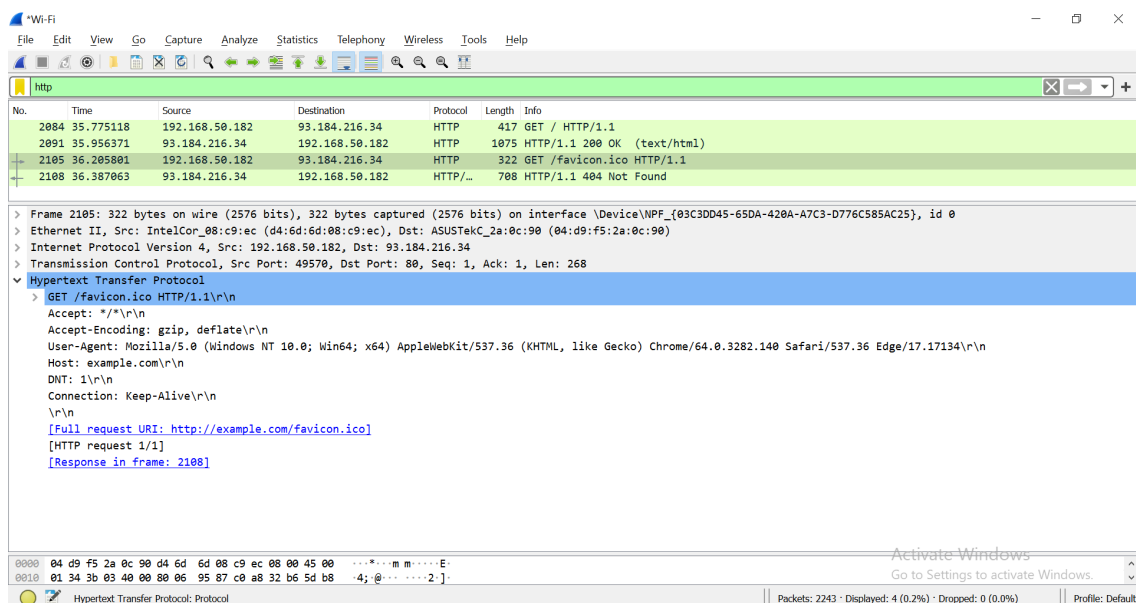
[Expert Info (Chat/Sequence): GET /SGX/LCWL/Windows/sgx\_white\_list\_cert.bin HTTP/1.0\r\n]

Request Method: GET

Request URI: /SGX/LCWL/Windows/sgx\_white\_list\_cert.bin

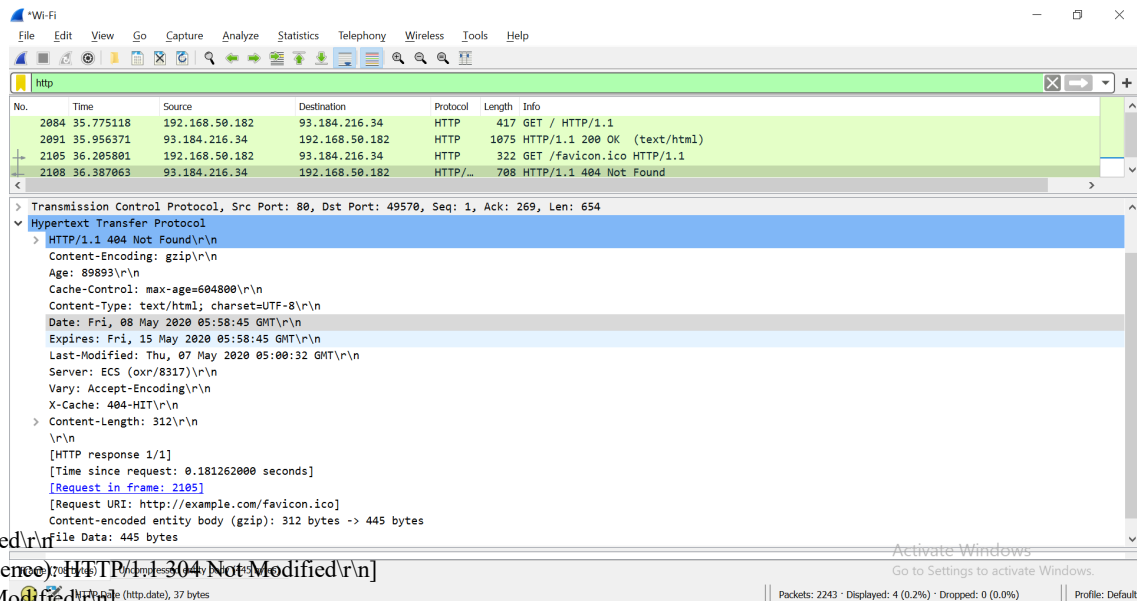
Request Version: HTTP/1.0

## 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

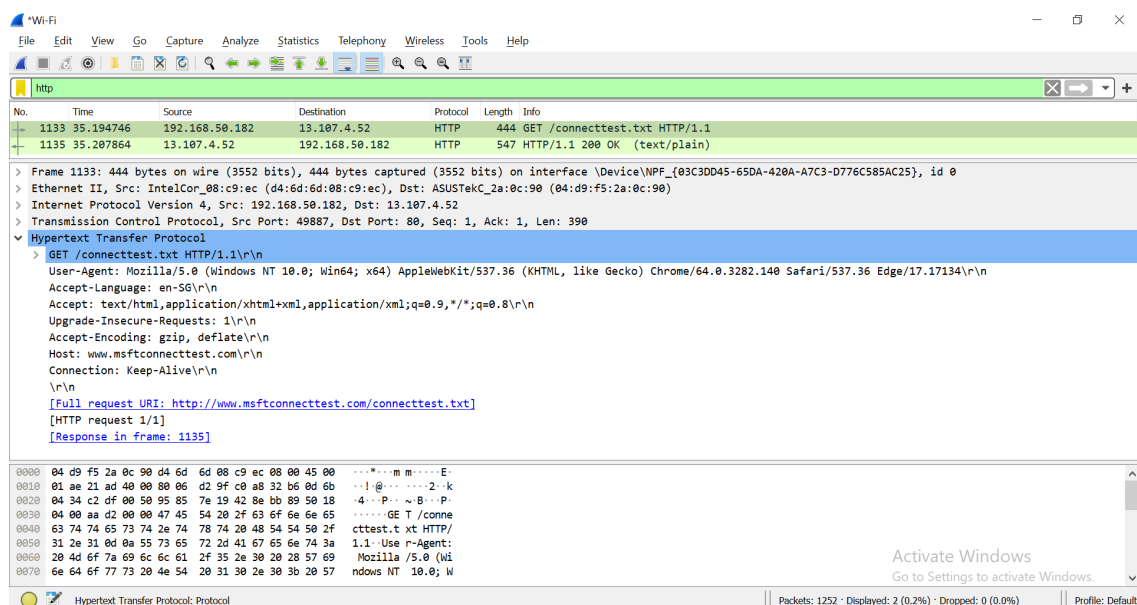
What is the HTTP response code for the request?

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.

Wireshark capture showing an HTTP response. The packet list shows two packets: a GET request (1133) and a 200 OK response (1135). The packet details pane shows the response structure:

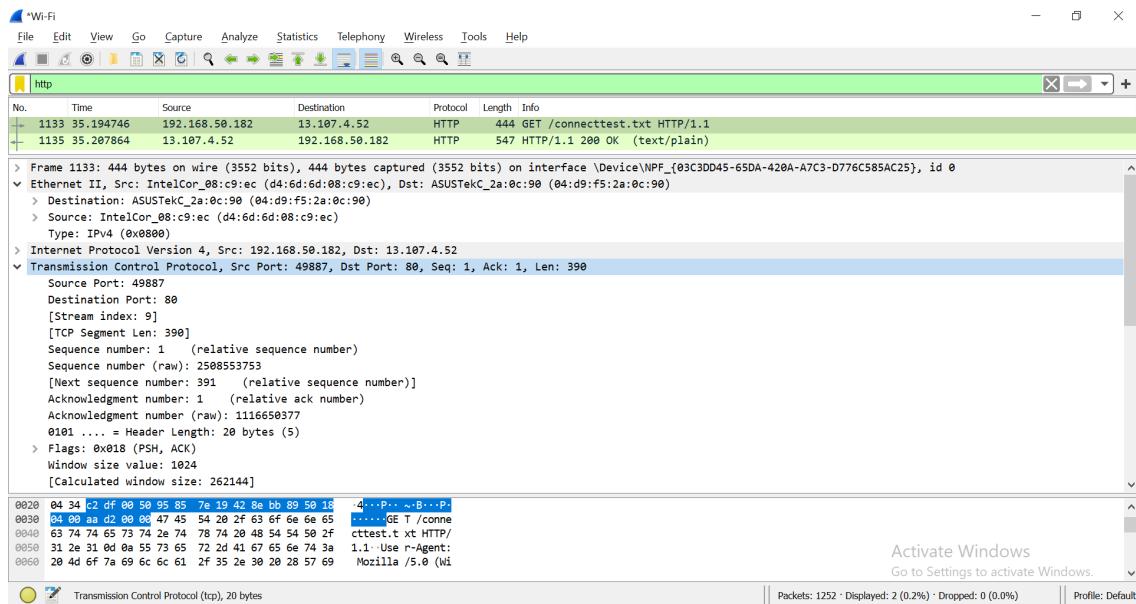
```

> Frame 1135: 547 bytes on wire (4376 bits), 547 bytes captured (4376 bits) on interface \Device\NPF_{03C3DD45-65DA-420A-A7C3-D776C585AC25}, id 0
> Ethernet II, Src: ASUSTekC_2a:0c:90 (04:d9:f5:2a:0c:90), Dst: IntelCor_08:c9:ec (d4:6d:6d:08:c9:ec)
> Internet Protocol Version 4, Src: 13.107.4.52, Dst: 192.168.50.182
> Transmission Control Protocol, Src Port: 80, Dst Port: 49887, Seq: 1, Ack: 391, Len: 493
< Hypertext Transfer Protocol
  < HTTP/1.1 200 OK\r\n
    Cache-Control: no-store\r\n
    Content-Length: 22\r\n
    Content-Type: text/plain; charset=utf-8\r\n
    Last-Modified: Mon, 04 May 2020 17:29:28 GMT\r\n
    Accept-Ranges: bytes\r\n
    ETag: 0x8D343F9E96C9DAC\r\n
    Access-Control-Allow-Origin: *\r\n
    Access-Control-Expose-Headers: X-MSEdge-Ref\r\n
    Timing-Allow-Origin: *\r\n
    X-Content-Type-Options: nosniff\r\n
    X-MSEdge-Ref: Ref A: C58DA8063BE84B9EBF6992D8B349F776 Ref B: SG2EDGE0312 Ref C: 2020-05-08T06:56:29Z\r\n
    Date: Fri, 08 May 2020 06:56:28 GMT\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.013118000 seconds]
    [Request in frame: 1133]
    [Request URI: http://www.msftconnecttest.com/connecttest.txt]
    File Data: 22 bytes
  
```

The status bar at the bottom indicates: Packets: 1252 · Displayed: 2 (0.2%) · Dropped: 0 (0.0%) · Profile: Default

## C. Analyze TCP Packet containing HTTP Traffic

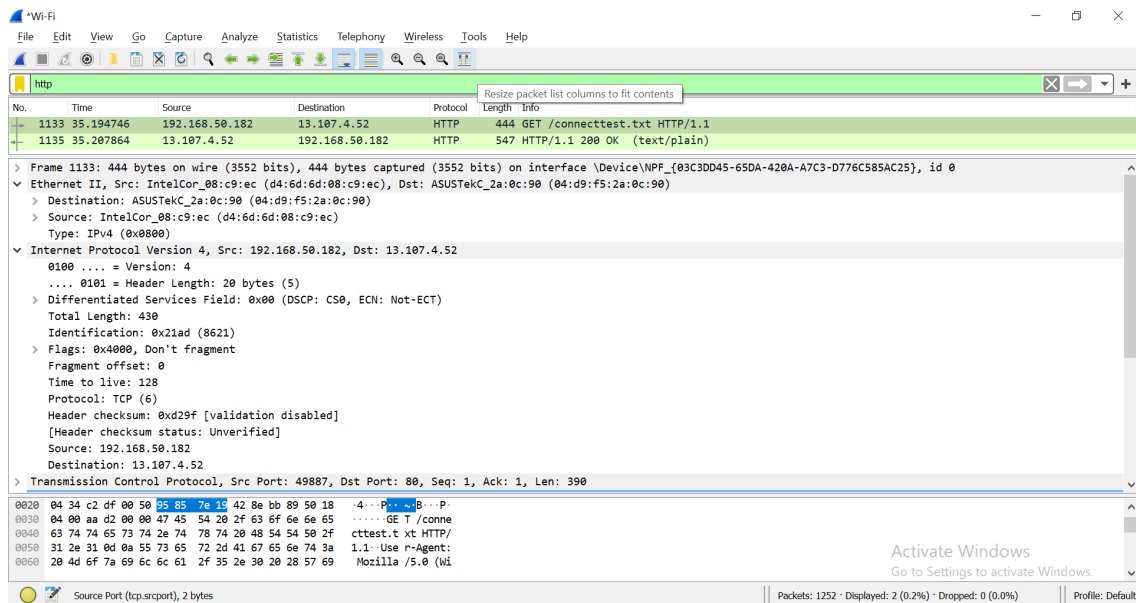
### 1. Examine the HTTP request labelled as “GET /connecttest.txt HTTP/1.1”



### 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
<a href="http://www.msftconnecttest.com/">http://www.msftconnecttest.com/</a>	13.107.4.52

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

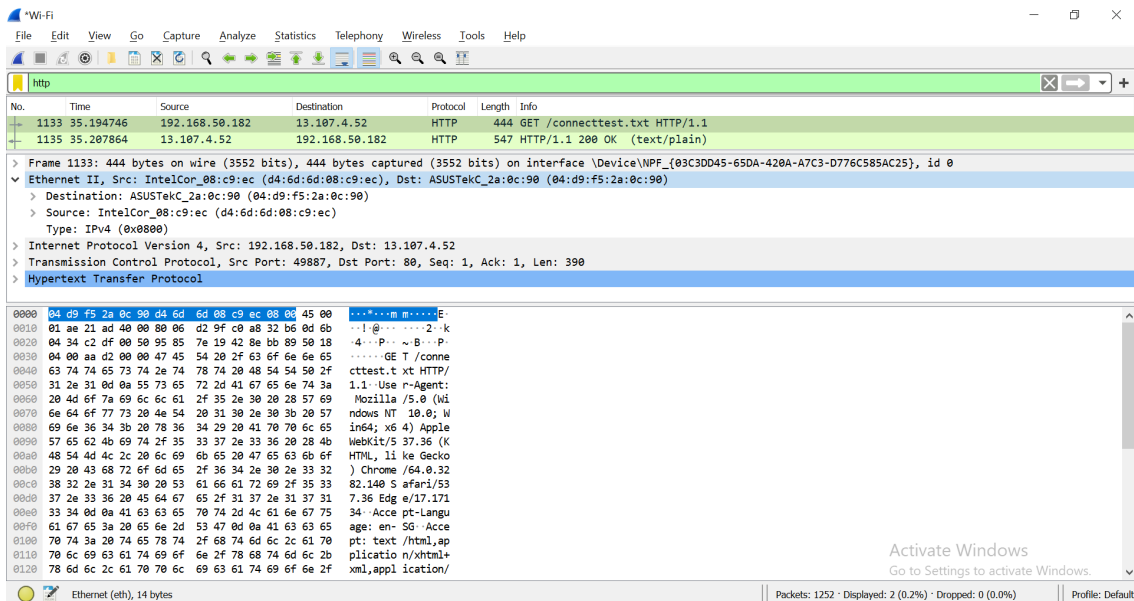
Source MAC Address	8c:16:45:f3:7c:64
Destination MAC Address	Ethernet II, Src: LCFCHFe_f3:7c:64 (8c:16:45:f3:7c:64), Dst: TP-Link_6d:b5:b8 (10:27:f5:6d:b5:b8)

**(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.



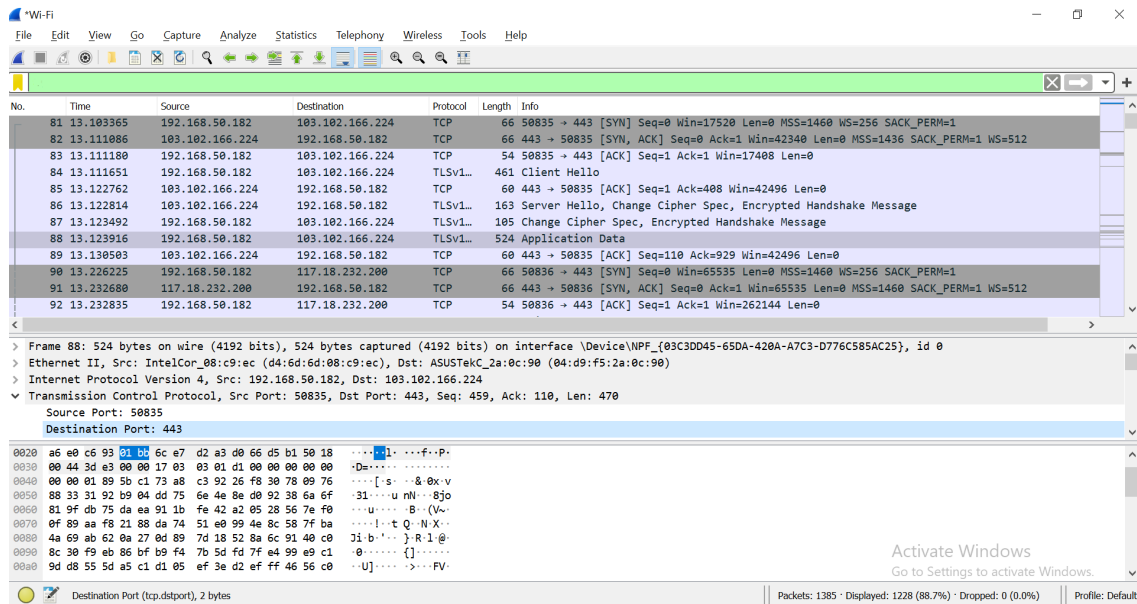
6. Observe the Destination and Source fields. The destination should be your default gateway's MAC address and the source should be your MAC address. You can use `ipconfig /all` and `arp -a` to confirm.



**(OPTIONAL)****D. Analyze TCP Packet containing HTTPS Traffic**

<https://en.wikiiversity.org/wiki/Wireshark/HTTPS>

1. Open a new web browser window or tab.
2. Start a Wireshark capture.
3. Navigate to <https://en.wikiiversity.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](https://en.wikiiversity.org/wiki/Wireshark/HTTPS)

**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*