

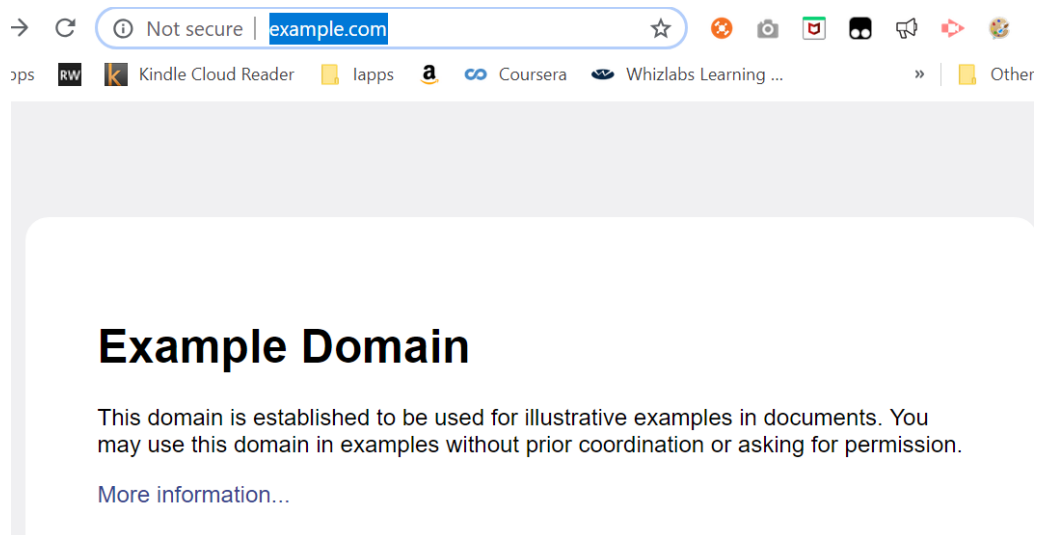
Practical 06

Capture HTTP Traffic and IP Traffic

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

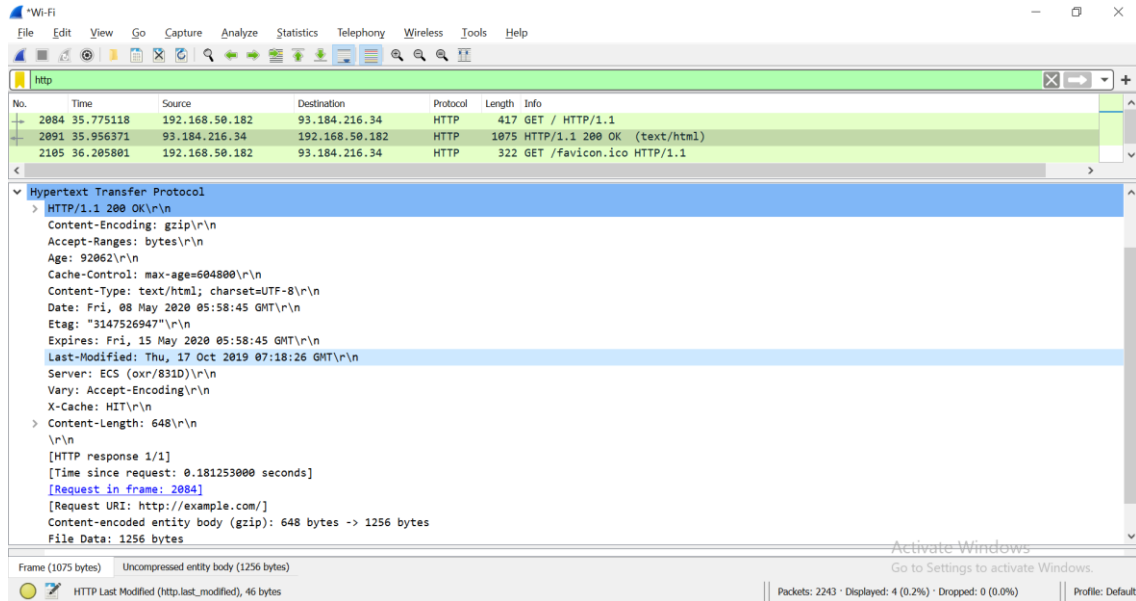
A. Capture HTTP Traffic

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



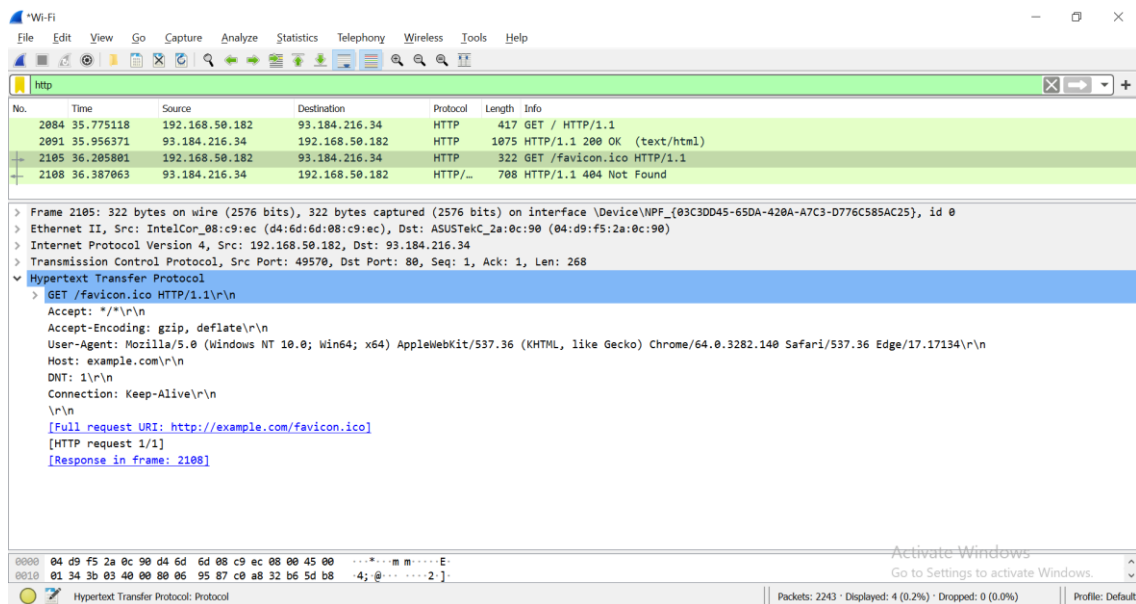
4. Stop Wireshark capture.

5. Observe the HTTP response.



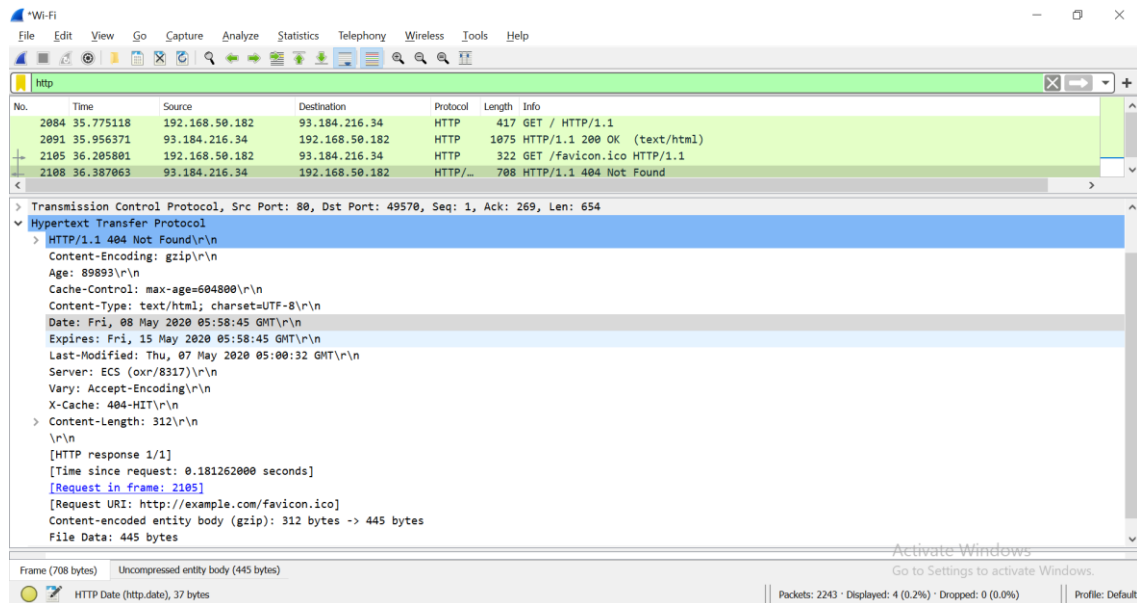
What is the HTTP response code for the request?

6. Examine the HTTP packet labelled as “GET /favicon.ico HTTP/1.1”.



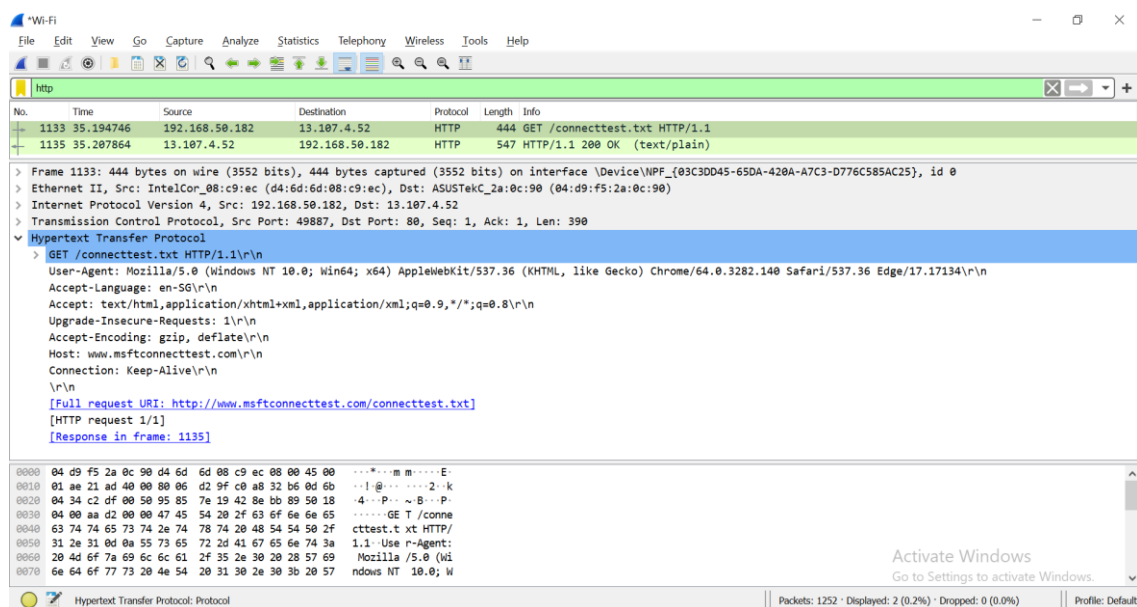
Note: If you don't have the above HTTP request in Wireshark, you can use another browser to send request to example.com again.

Observe the HTTP response.



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	
--------------------	--

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

User-Agent	
Type of browser	

User-Agent

Observe the HTTP response.

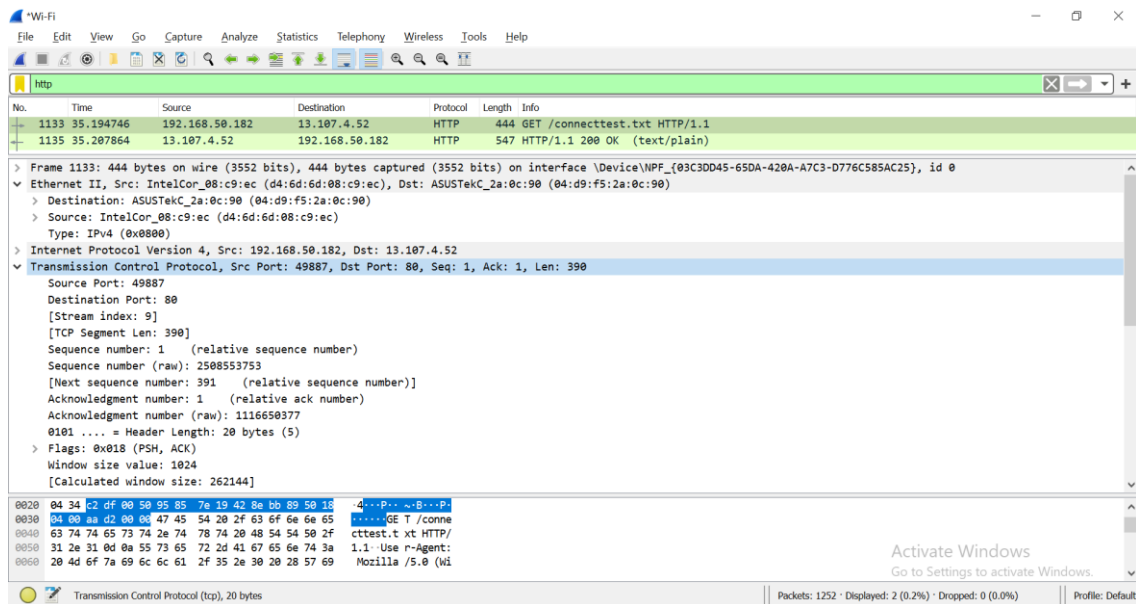
The screenshot shows a Wireshark packet capture of an HTTP response. The packet list pane shows two packets: a GET request (1133) and a 200 OK response (1135). The packet details pane for packet 1135 shows the following structure:

- 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: C58DA8063BEB489EBF6992D8B349F776 Ref B: 5G2EDGE0312 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 packet bytes pane shows the raw data of the packet, and the packet hex pane shows the hexadecimal representation of the data.

C. Analyze TCP Packet containing HTTP Traffic

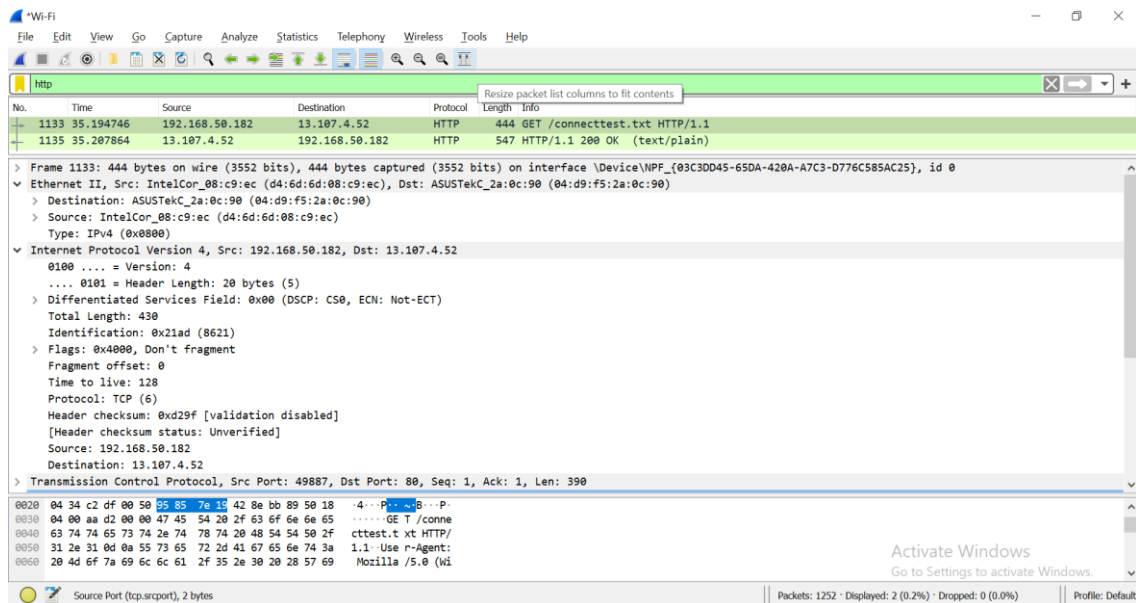
1. Examine the HTTP request labelled as “GET /connecttest.txt HTTP/1.1”



2. Write down the source and destination Port Number.

	Hex	Binary	Decimal
Source port			
Destination port			

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



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

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

Domain Name	IP Address
http://www.msftconnecttest.com/	

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

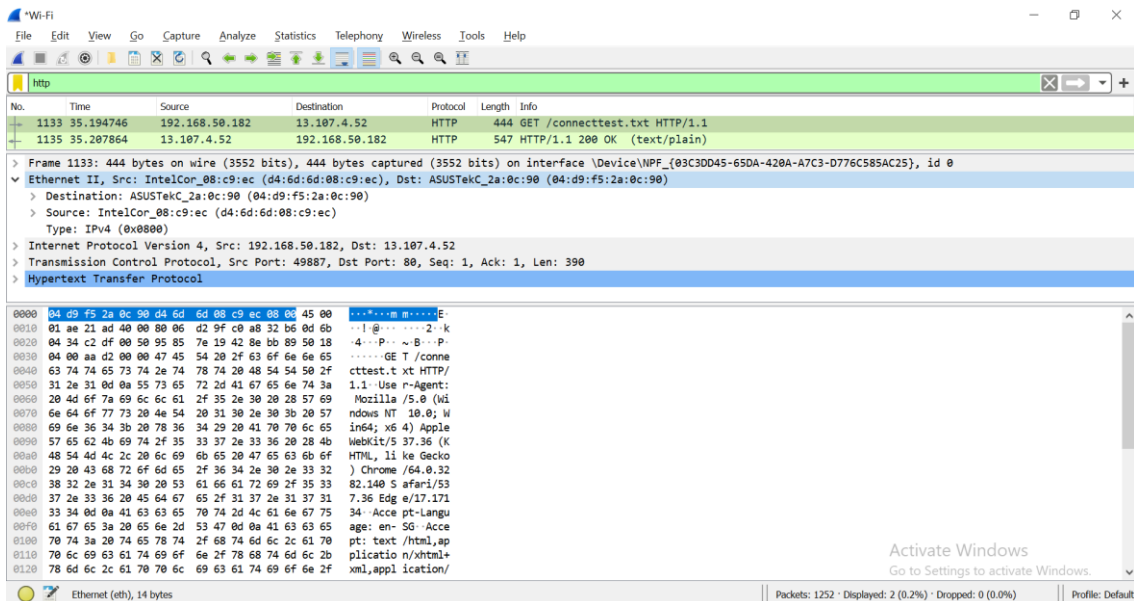
Source MAC Address	
Destination MAC Address	

(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.

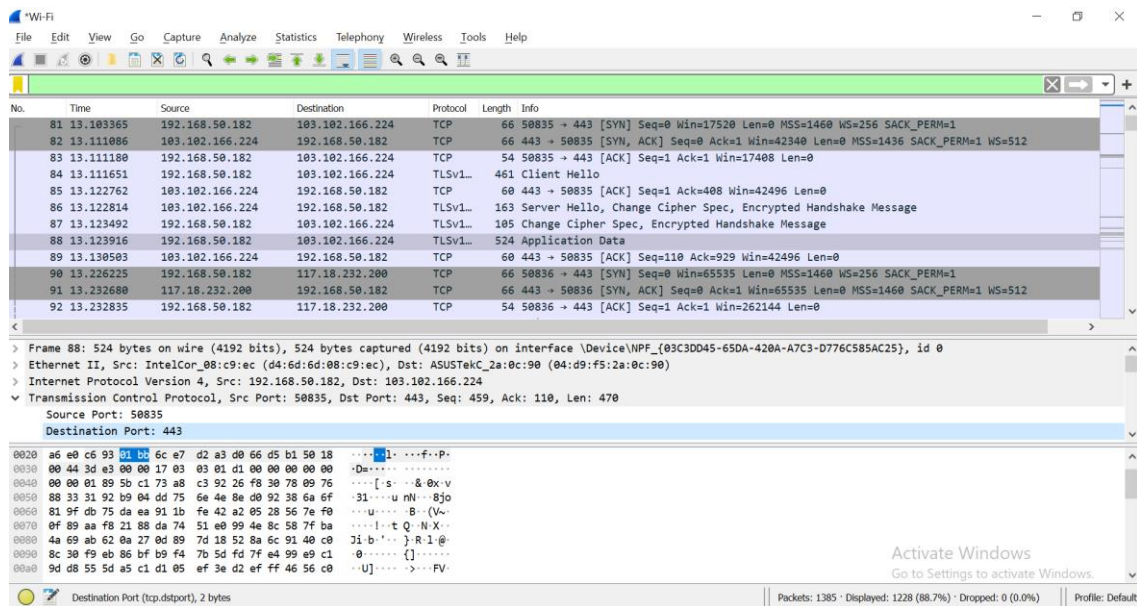


6. Observe the Destination and Source fields. The destination should be your default gateway's MAC address and the source should be your MAC address. You can use `ipconfig /all` and `arp -a` to confirm.

(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)

End of Practical