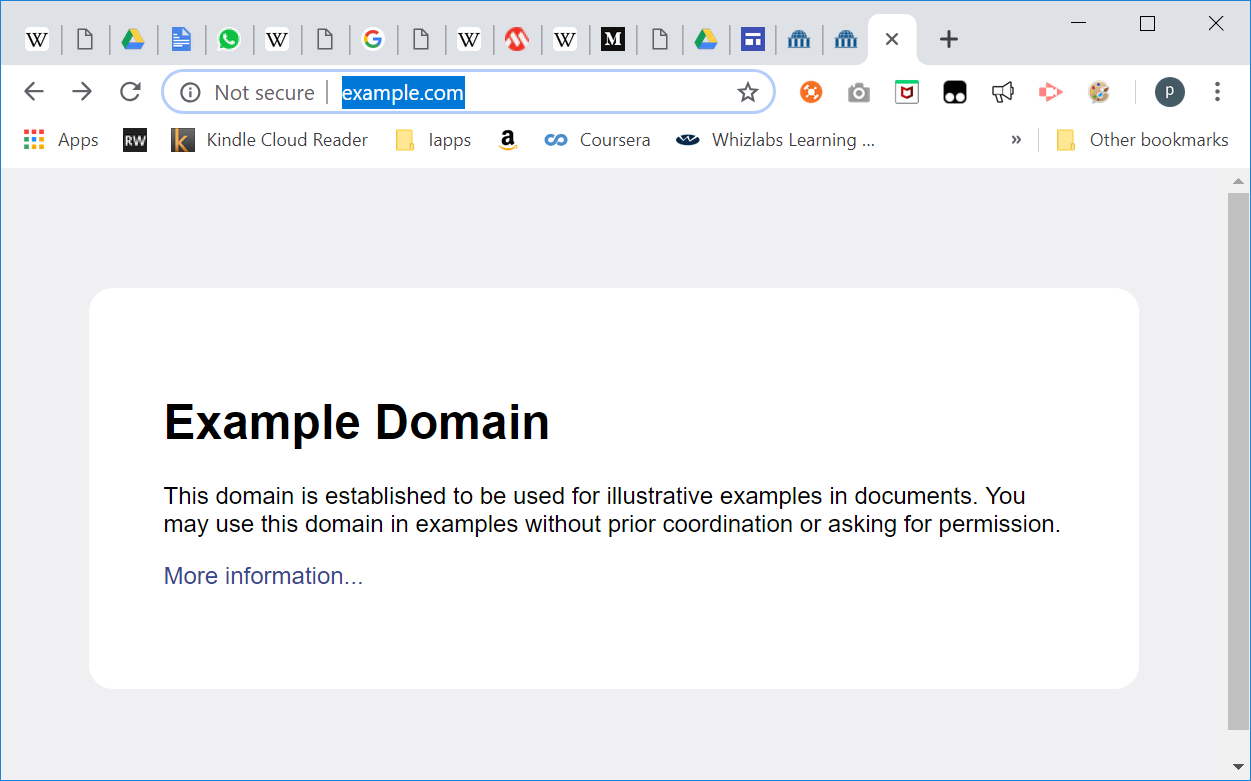
**Practical 06**

**Capture HTTP Traffic and IP Traffic**

1. Capture HTTP Traffic
2. Analyze HTTP Request Traffic
3. Analyze HTTP Response Traffic
4. Analyze HTTPS Traffic
5. **Capture HTTP Traffic**
6. Open a new browser tab.
7. [Start a Wireshark capture](https://en.wikiversity.org/wiki/Wireshark/Start).
8. Browse the web page [http://example.com](http://example.com/).



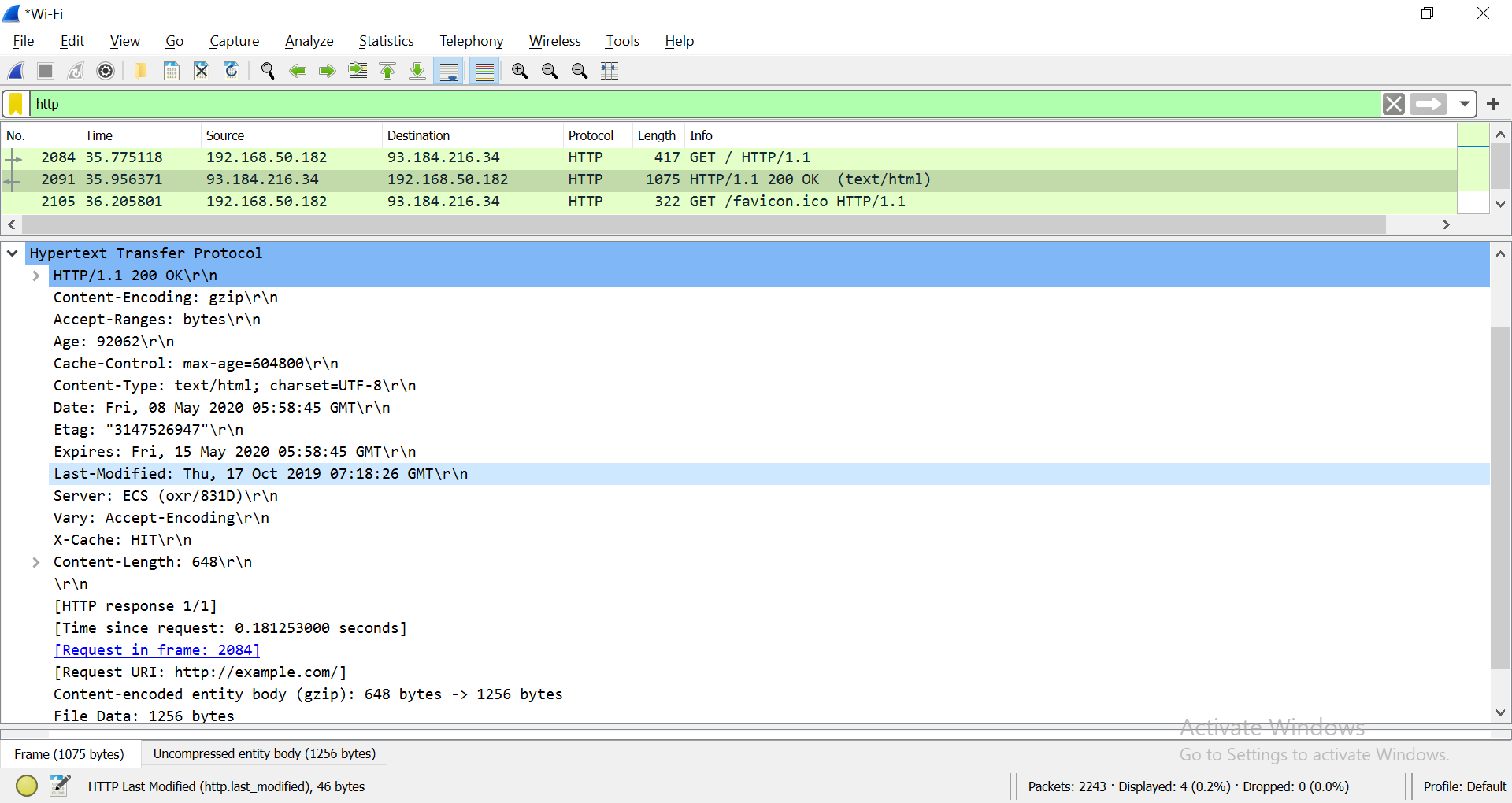
1. Stop Wireshark capture.
2. **Analyze HTTP Traffic**
3. Observe the traffic captured in the top Wireshark packet list pane. To view only HTTP traffic, type tcp.port == 80 (lower case) or **http** in the Filter box and press Enter.
4. Select the HTTP packet labelled “*GET / HTTP/1.1*”



1. 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.
2. Observe the HTTP request.



1. Observe the HTTP response.



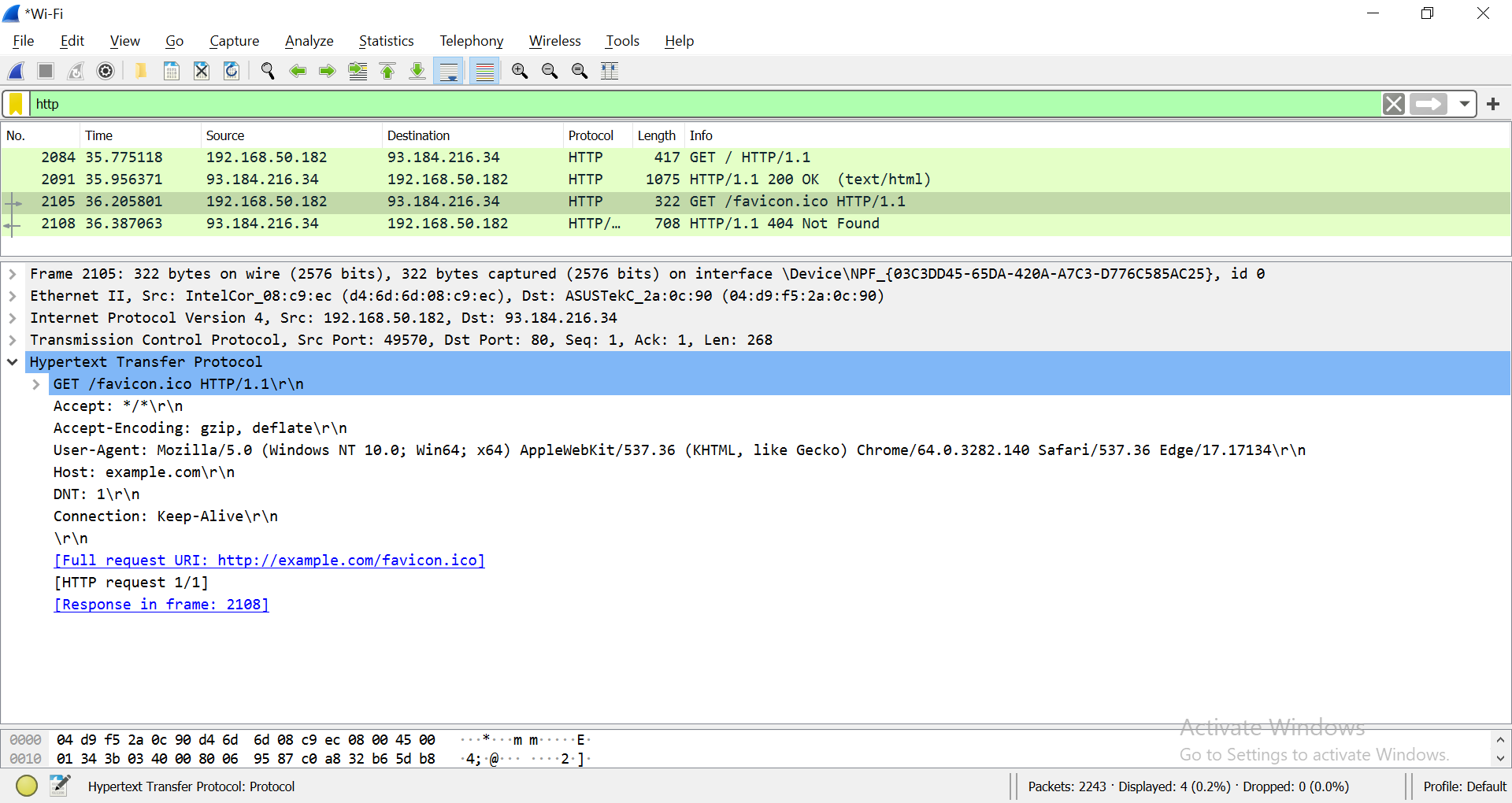
What is the HTTP response code for the request?

HT TP/1.1 200 OK..

A screenshot of a computer

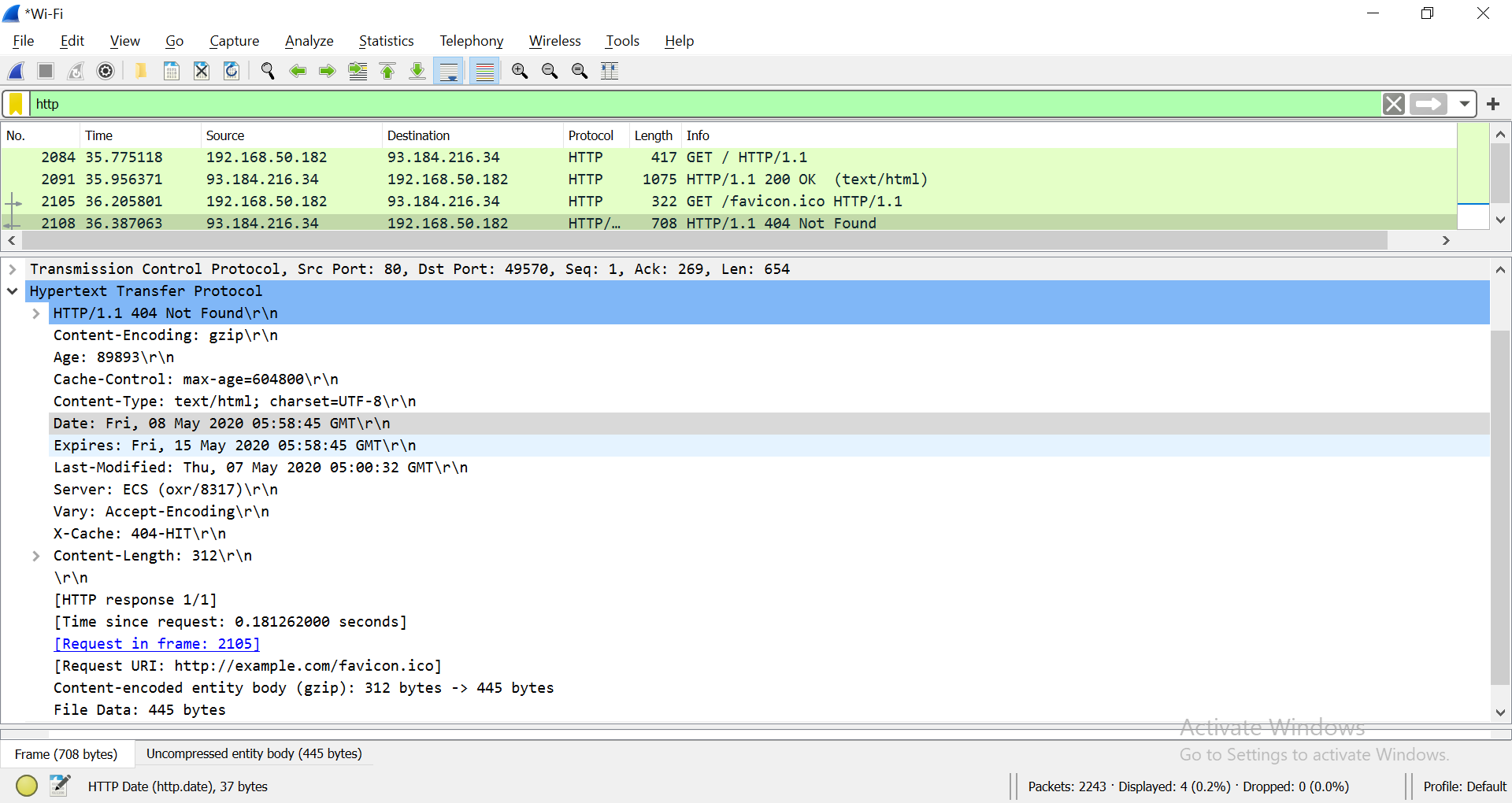
Description automatically generated

1. 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.



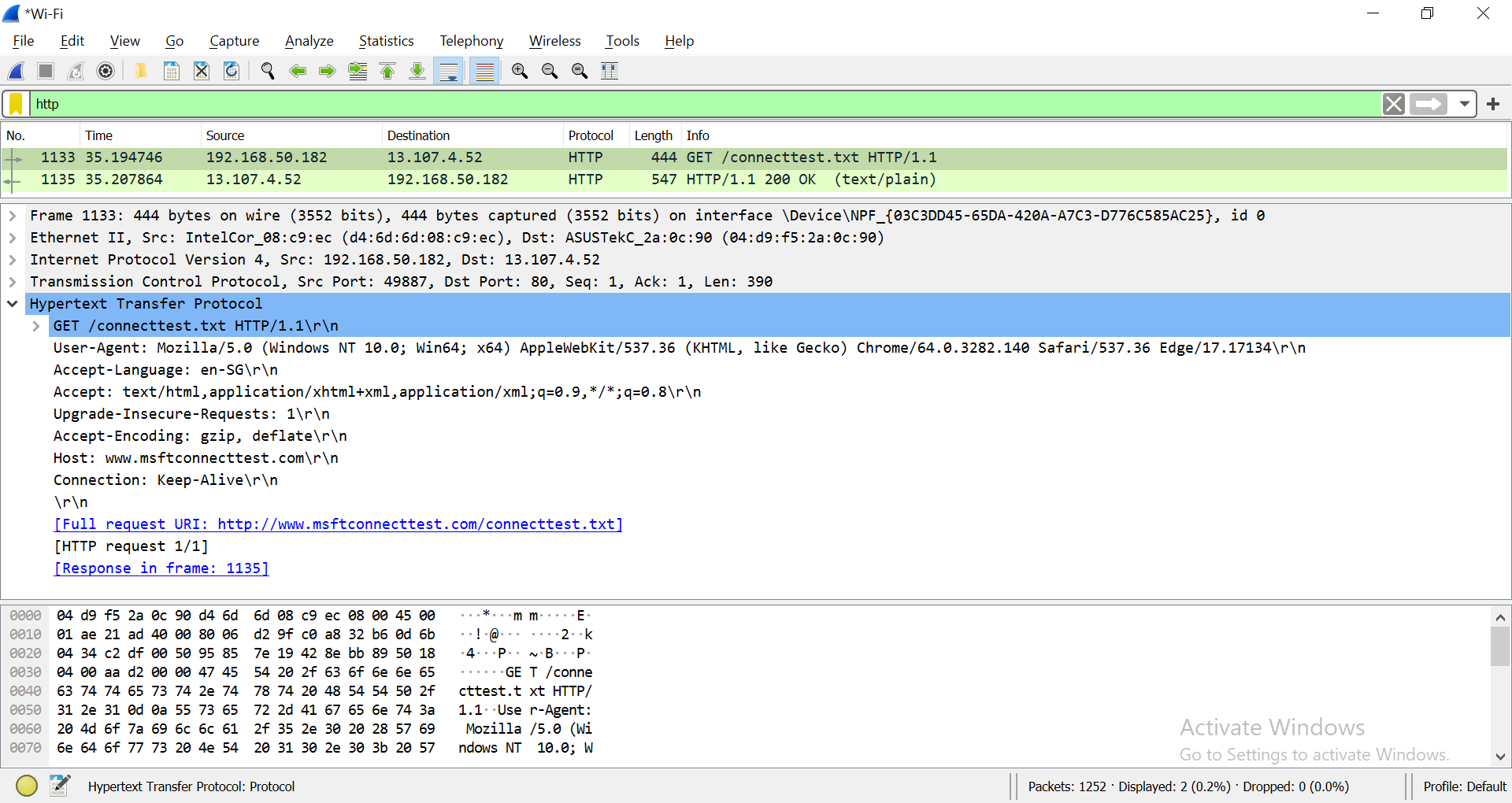
What is the HTTP response code for the request?

HT TP/1.1 404 Not F ound..

A screenshot of a computer

Description automatically generated

1. 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 | keep-alive\r\n |

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

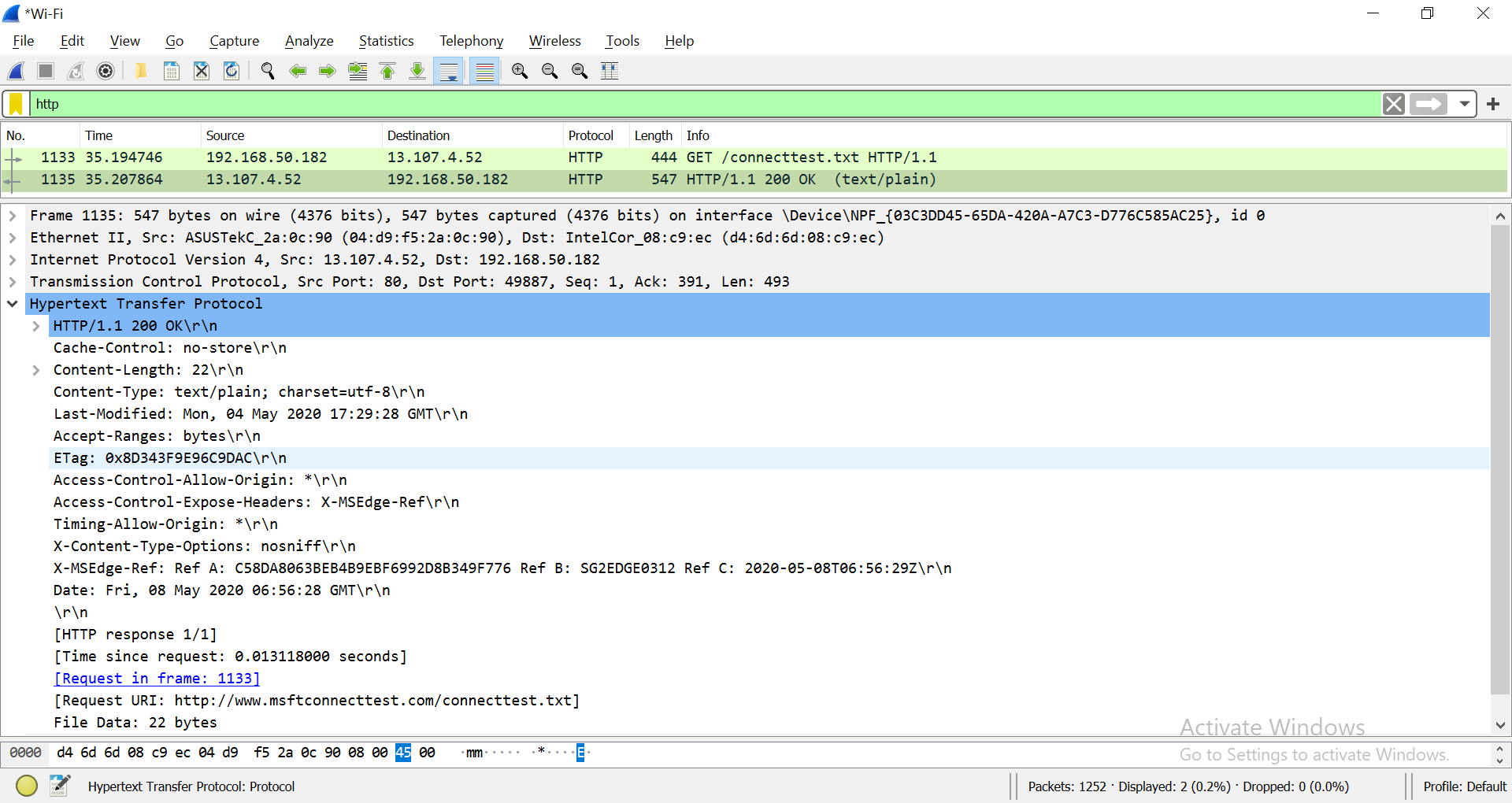
|  |  |
| --- | --- |
| User-Agent | Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.0.0 Safari/537.36\r\n |
| Type of browser | Mozilla, Apple WebKit, Chrome, Safari |

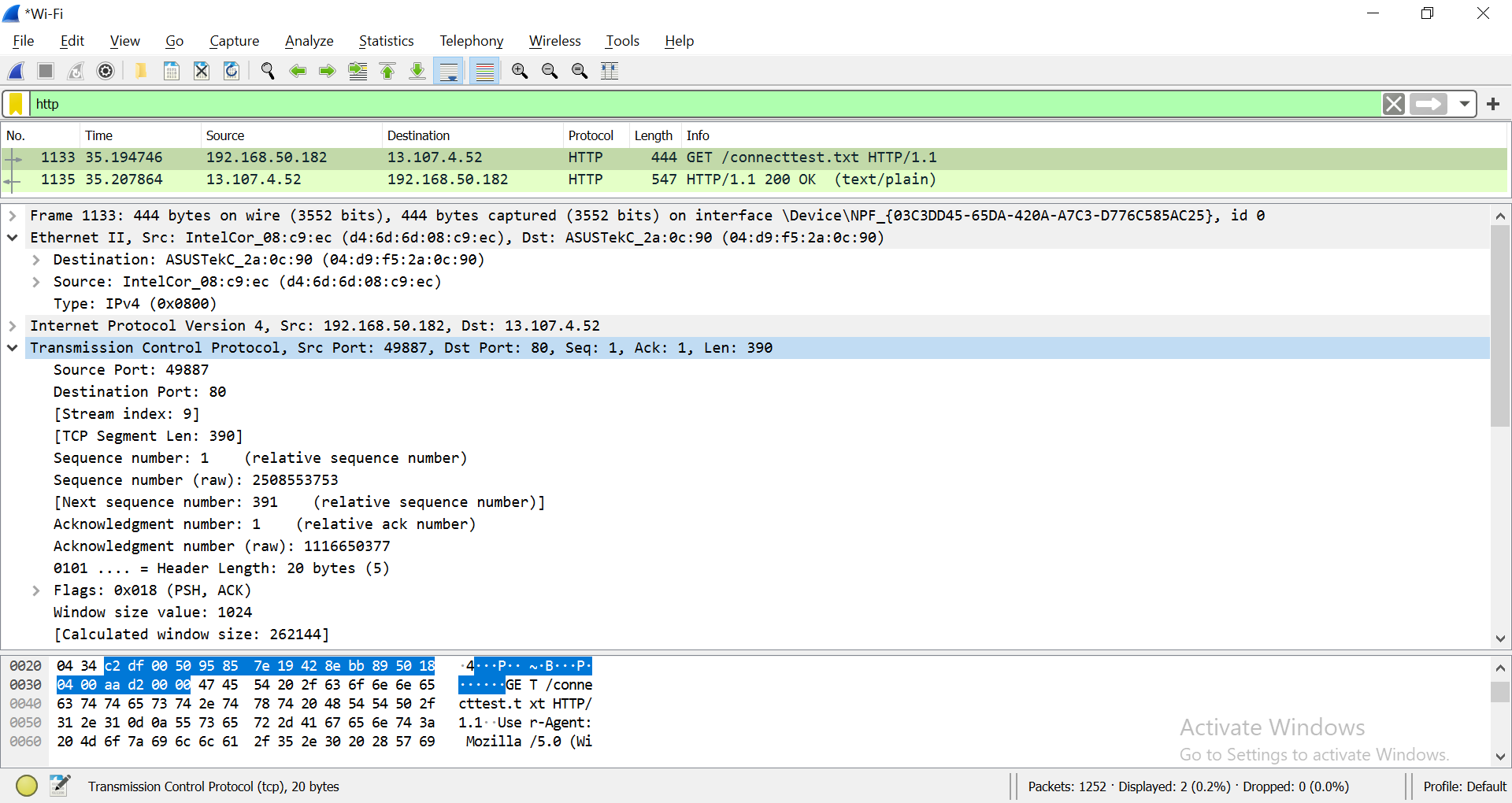
**A screenshot of a computer

Description automatically generated**

[**User-Agent**](https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/User-Agent)

Observe the HTTP response.



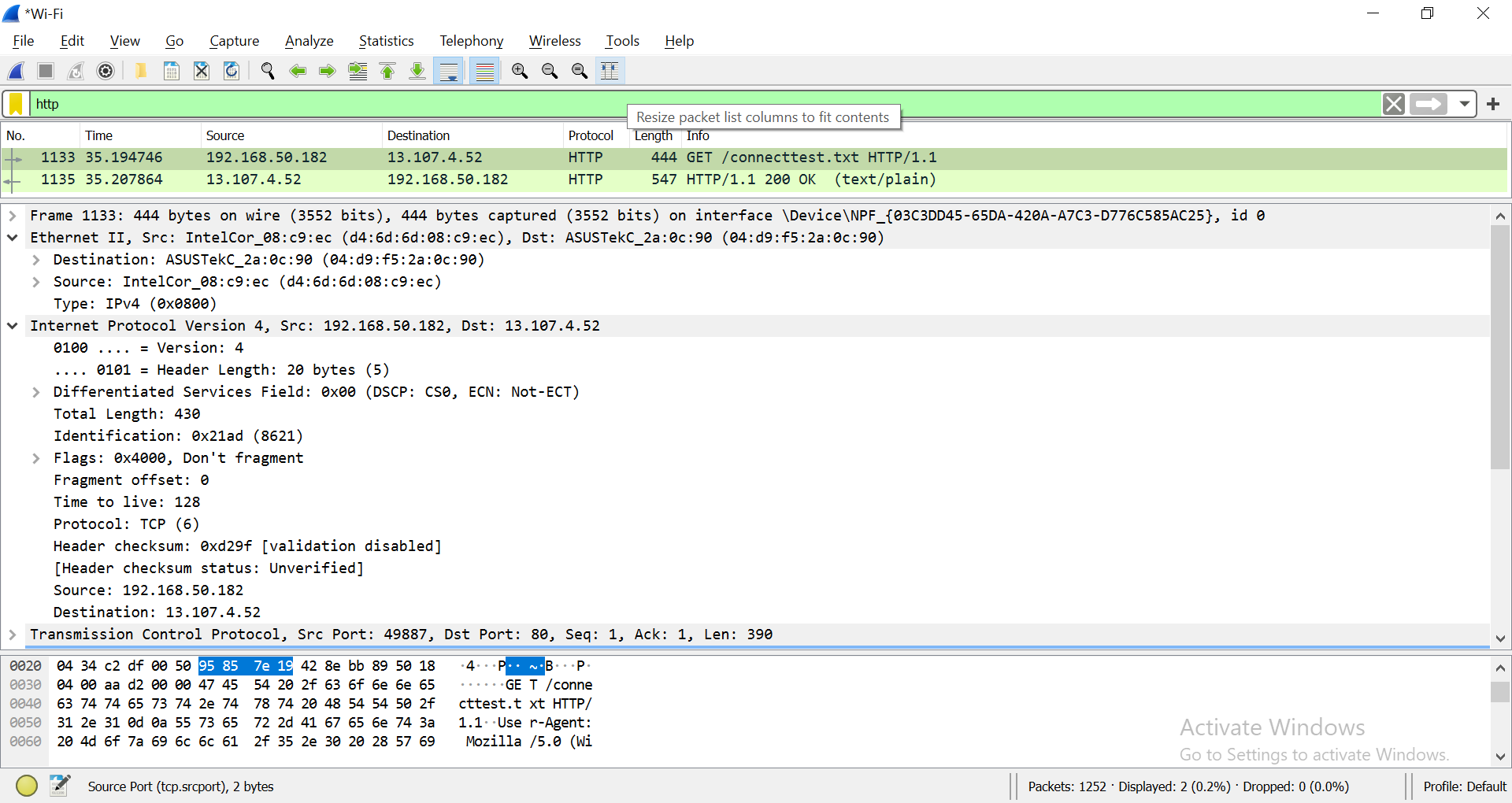
1. **Analyze TCP Packet containing HTTP Traffic**
2. Examine the HTTP request labelled as “*GET /connecttest.txt HTTP/1.1*”
3. Write down the source and destination Port Number.

|  |  |  |  |
| --- | --- | --- | --- |
|  | Hex | Binary | Decimal |
| Source port | EA 7F | 1110 1010 0111 1111 | 60031 |
| Destination port | 00 50 | 0000 0000 0101 0000 | 80 |

A screenshot of a computer

Description automatically generated

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



|  |  |
| --- | --- |
| Source IP address | 192.168.1.77 |
| Is the source IP address, your IP address? (true or false) | True |

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

|  |  |
| --- | --- |
| Domain Name | IP Address |
| http://www.msftconnecttest.com/ | 23.75.23.171 |

A screenshot of a computer

Description automatically generated

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

|  |  |
| --- | --- |
| Source MAC Address | 64:bc:58:73:be:dc |
| Destination MAC Address | c0:bc:9a:8b:e1:50 |

A screenshot of a computer

Description automatically generated

**(OPTIONAL)**

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

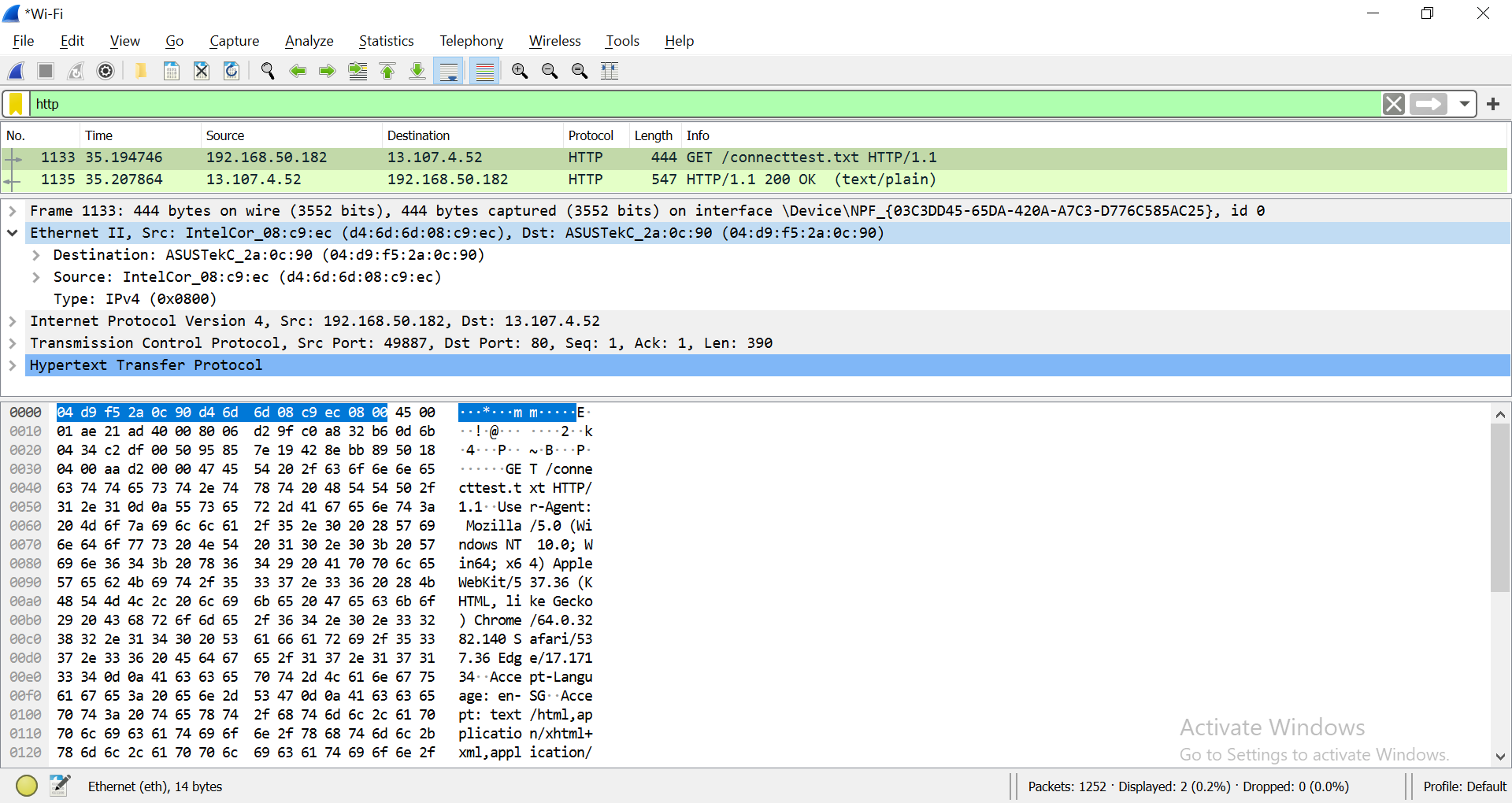
|  |  |
| --- | --- |
| Destination IP address | 23.75.23.171 |
| Is the destination IP address your DNS Server? (true or false) | False |

A screenshot of a computer

Description automatically generated

A screenshot of a computer program

Description automatically generated

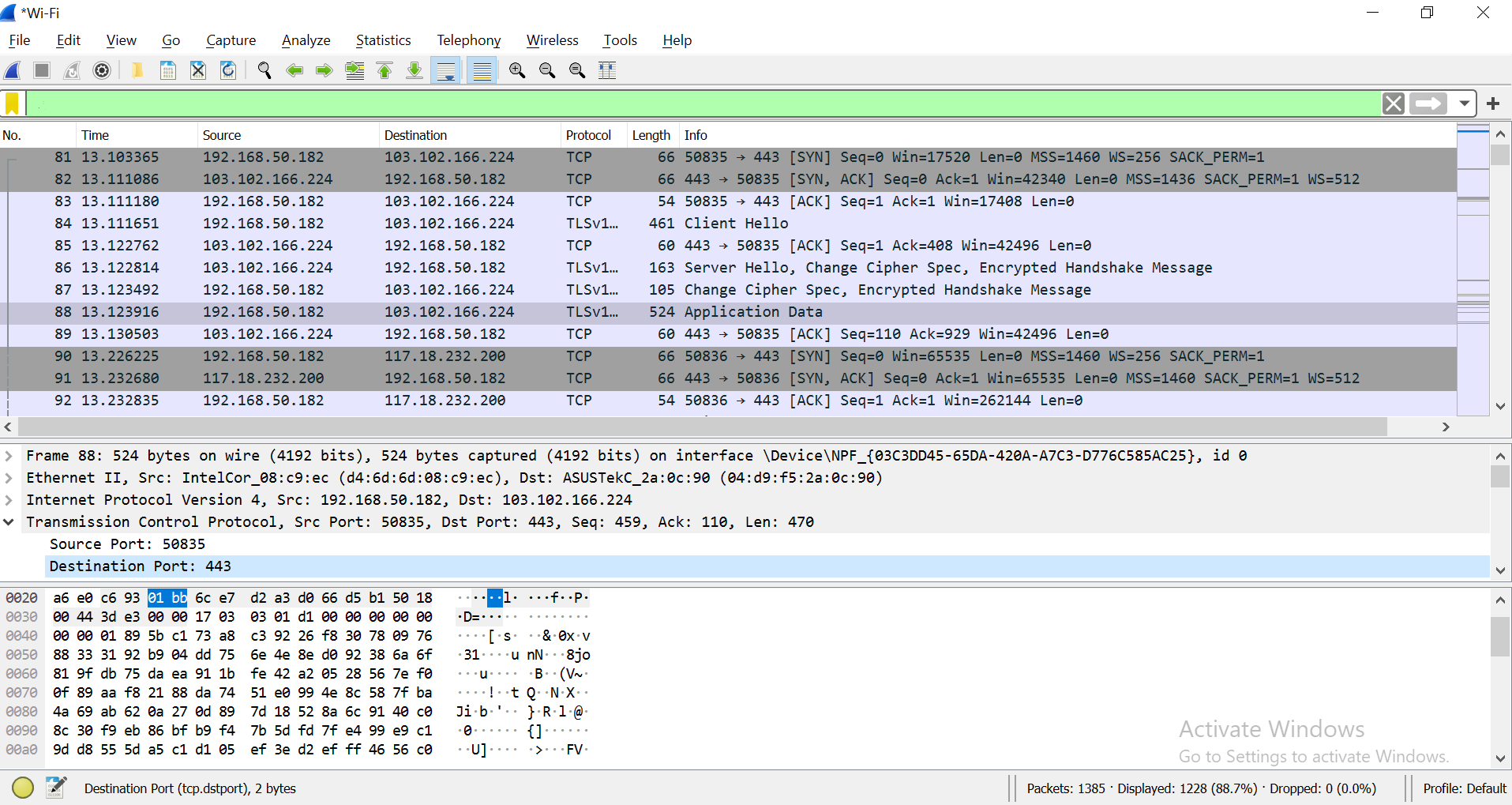
1. Expand Ethernet II to view Ethernet details.
2. Observe the Destination and Source fields. The destination should be your default gateway's MAC address and the source should be your MAC address. You can use [ipconfig /all](https://en.wikiversity.org/wiki/Ipconfig/All) and [arp -a](https://en.wikiversity.org/wiki/Computer_Networks/Management/Utilities/Arp/View) to confirm.

**(OPTIONAL)**

1. **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](https://en.wikiversity.org/wiki/Wireshark/Start).
3. Navigate to [https://en.wikiversity.org](https://en.wikiversity.org/).
4. Stop the Wireshark capture.



1. Write down the source and destination Port Number.

|  |  |  |  |
| --- | --- | --- | --- |
|  | Hex | Binary | Decimal |
| Source port | C693 | 1100 0110 1001 0011 | 50835 |
| Destination port | 1BB | 0001 1011 1011 | 443 |

Reference: [HTTP/HTTPS Analysis Using Wireshark](https://medium.com/devops-world/http-https-analysis-using-wireshark-cbe07c23520)

*End of Practical*