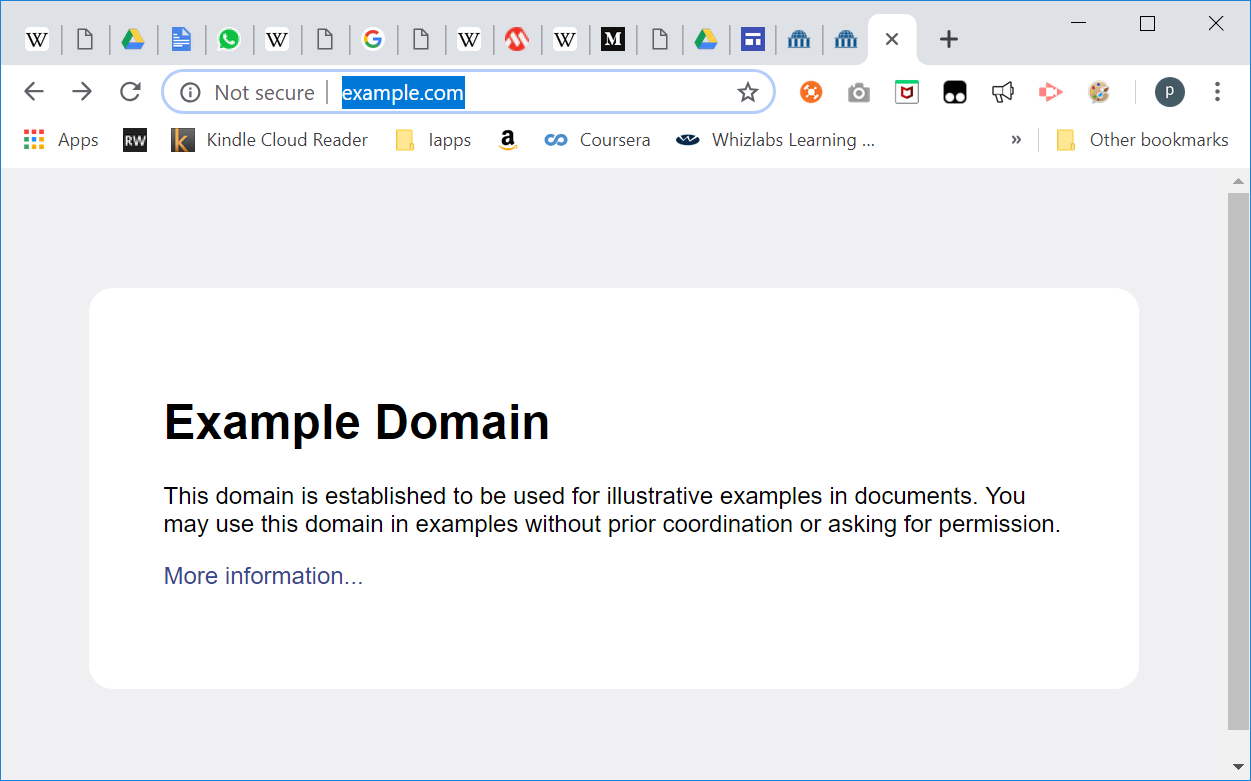
**Practical 06**

**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/).



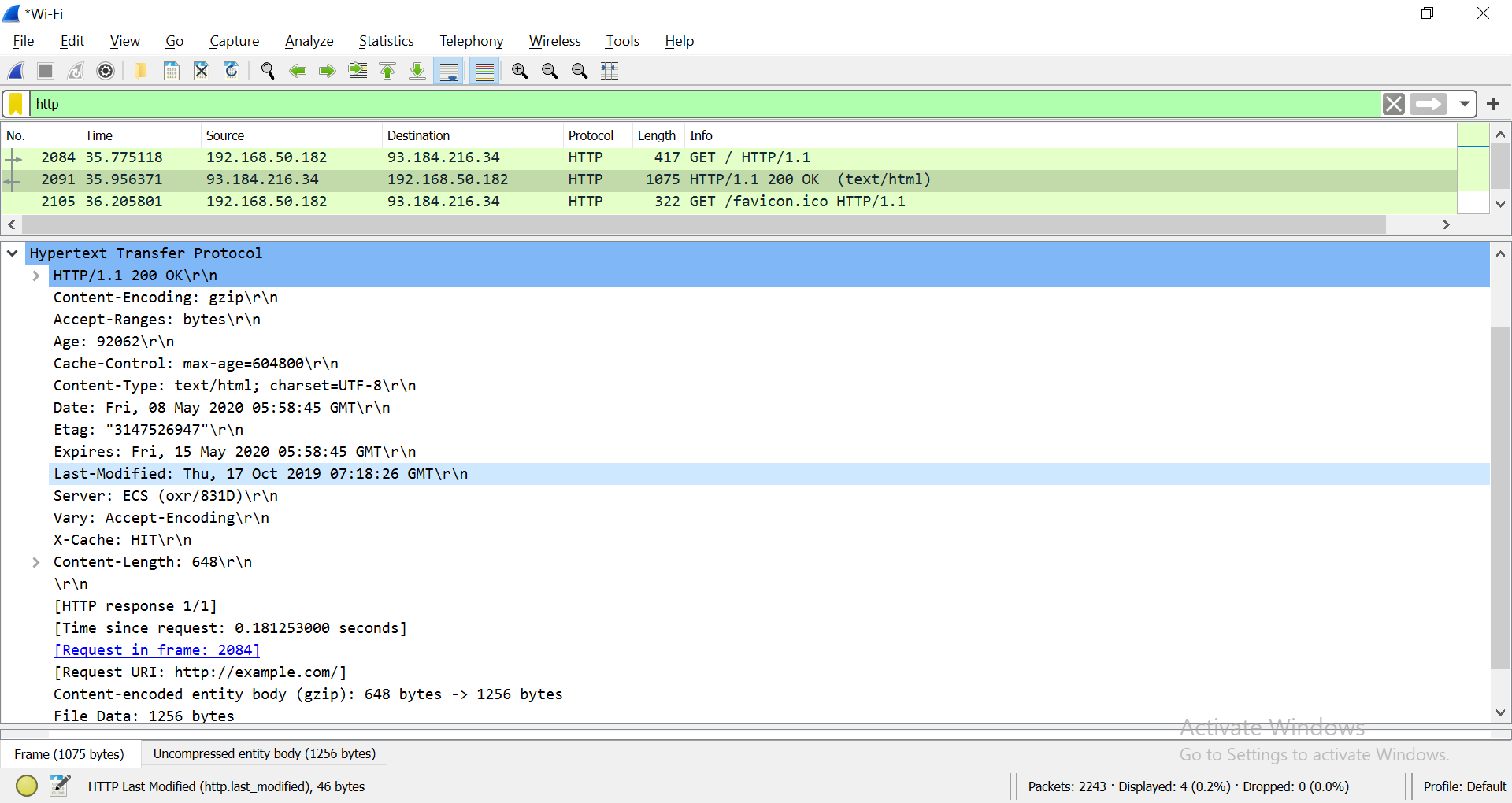
1. Stop Wireshark capture.
2. **Analyze HTTP Traffic**
3. Observe the traffic captured in the top Wireshark packet list pane. To view only HTTP traffic, type tcp.port == 80 (lower case) or **http** in the Filter box and press Enter.
4. Select the HTTP packet labelled “*GET / HTTP/1.1*”



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. (TCP IP Protocl Stack)
2. Observe the HTTP request.



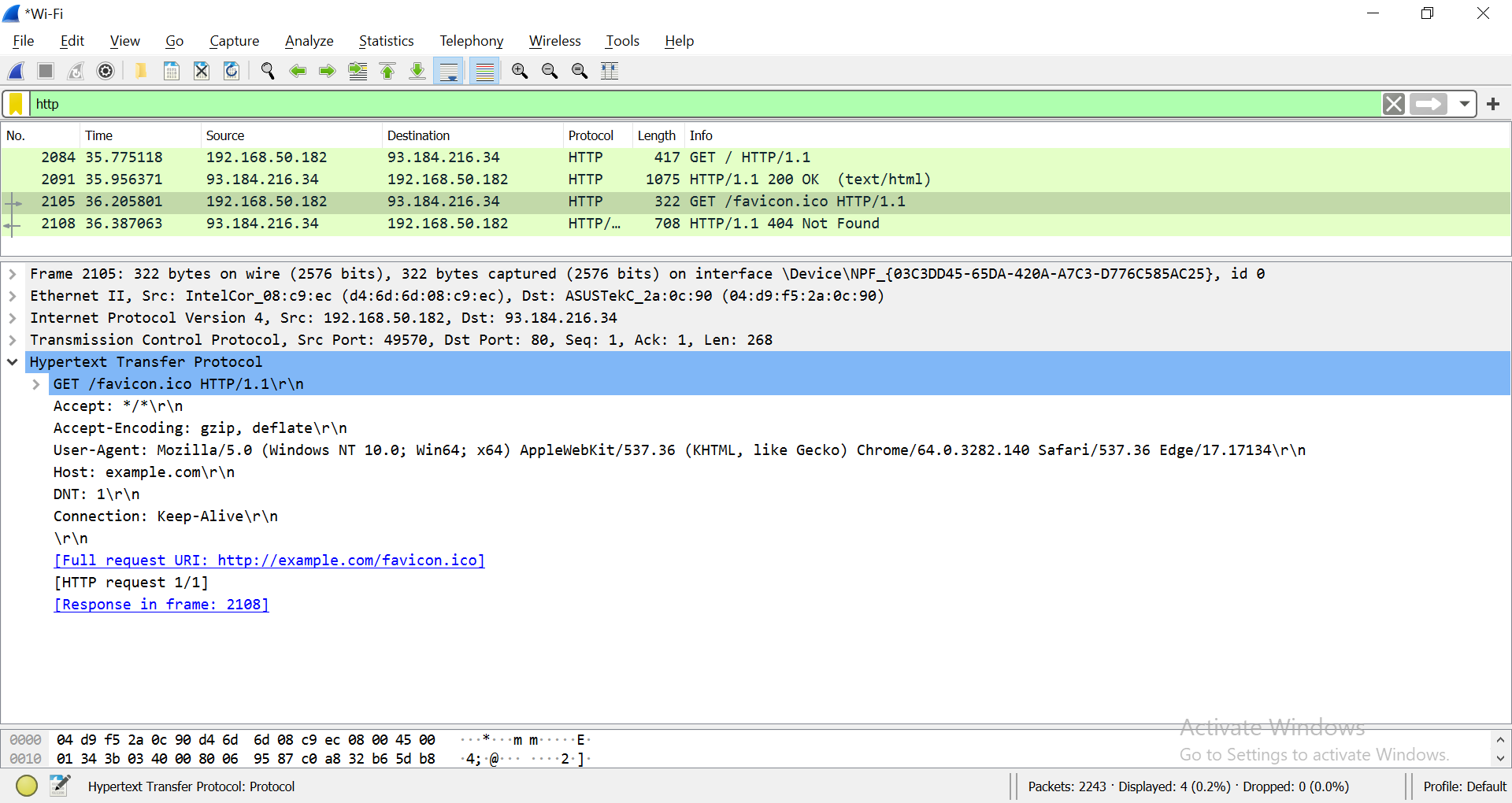
1. Observe the HTTP response.



What is the HTTP response code for the request?

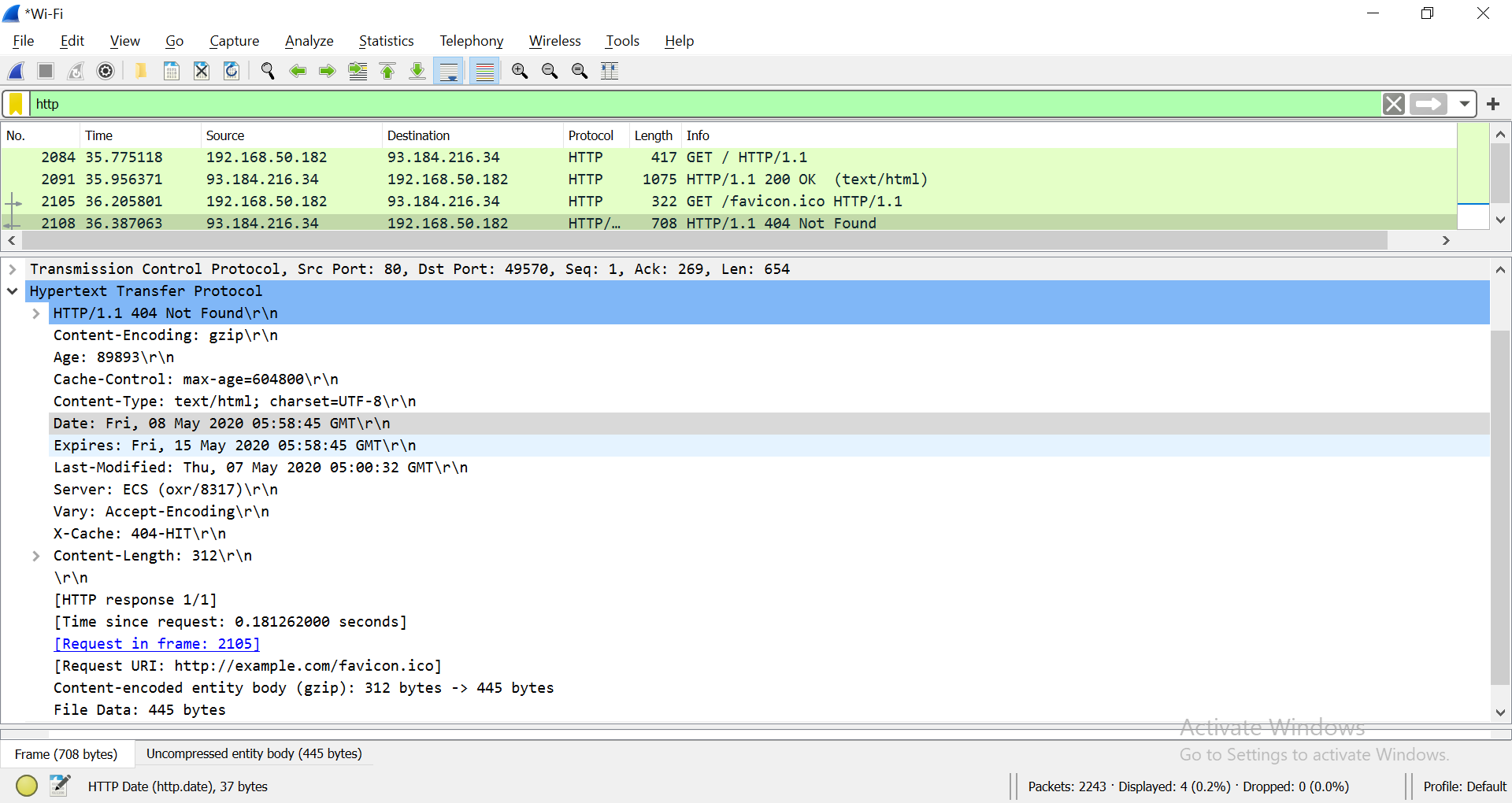
200

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.

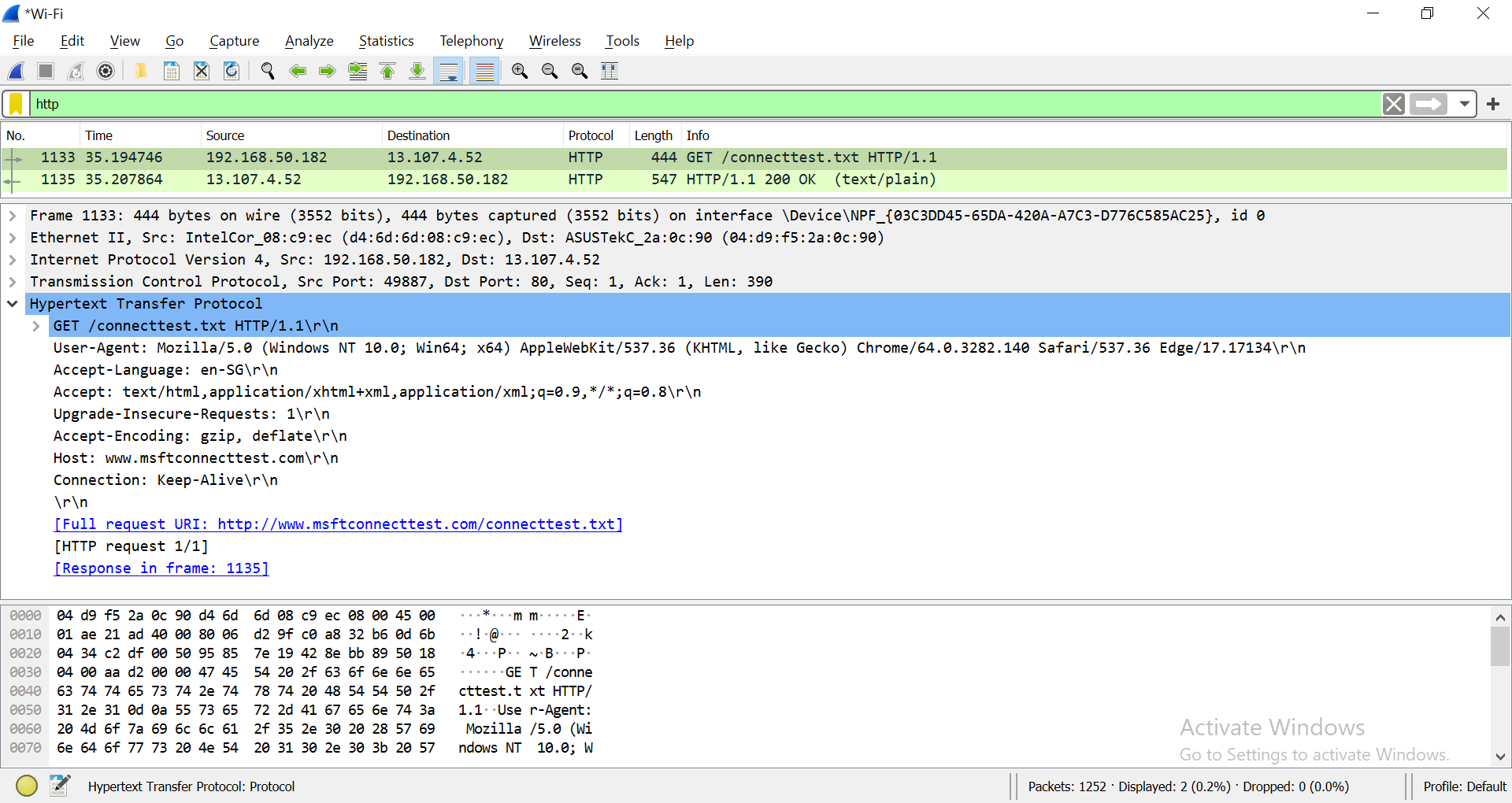
Observe the HTTP response.



What is the HTTP response code for the request?

404

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?

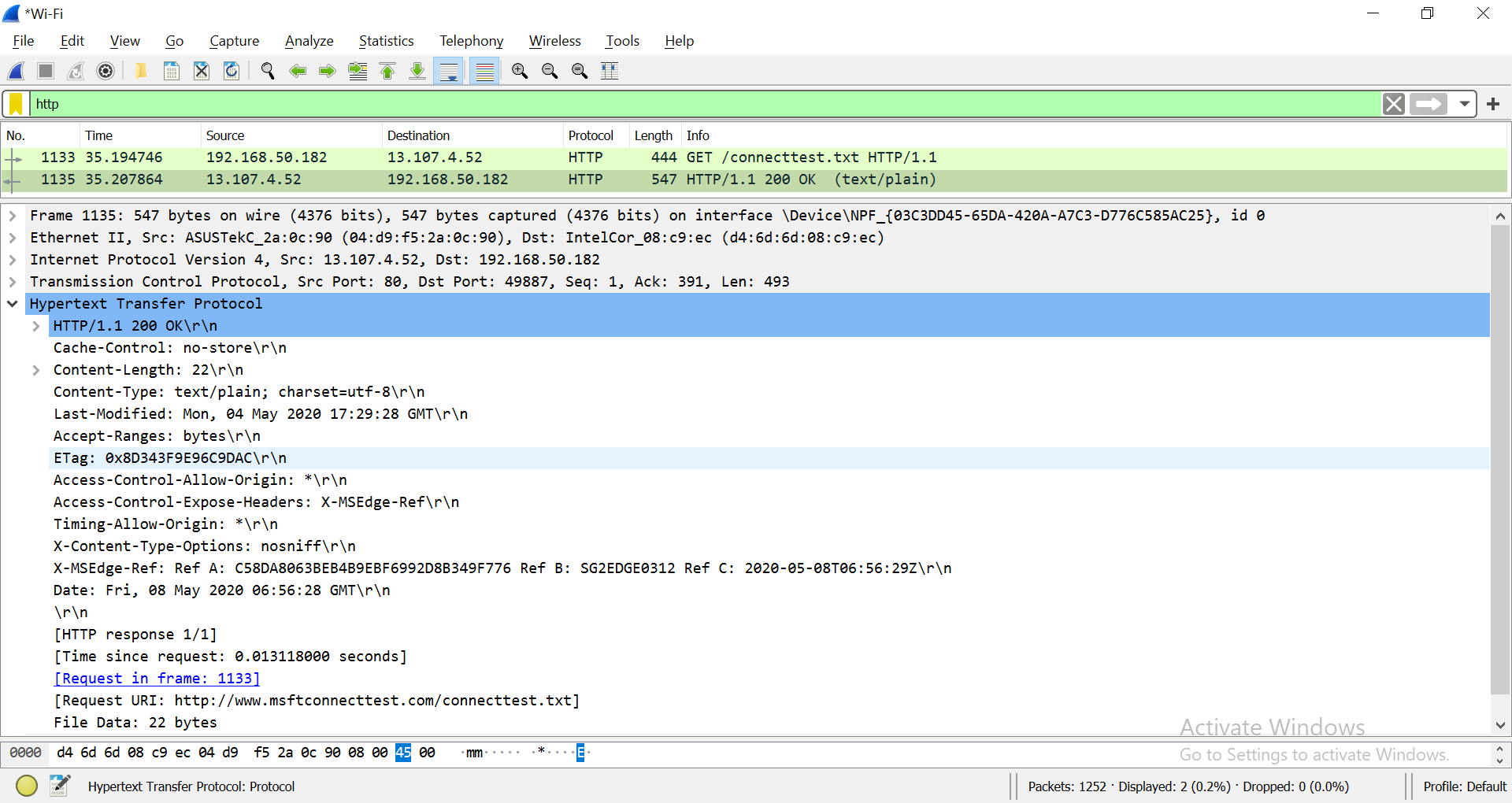
|  |  |
| --- | --- |
| Requested resource | /connecttest.txt |

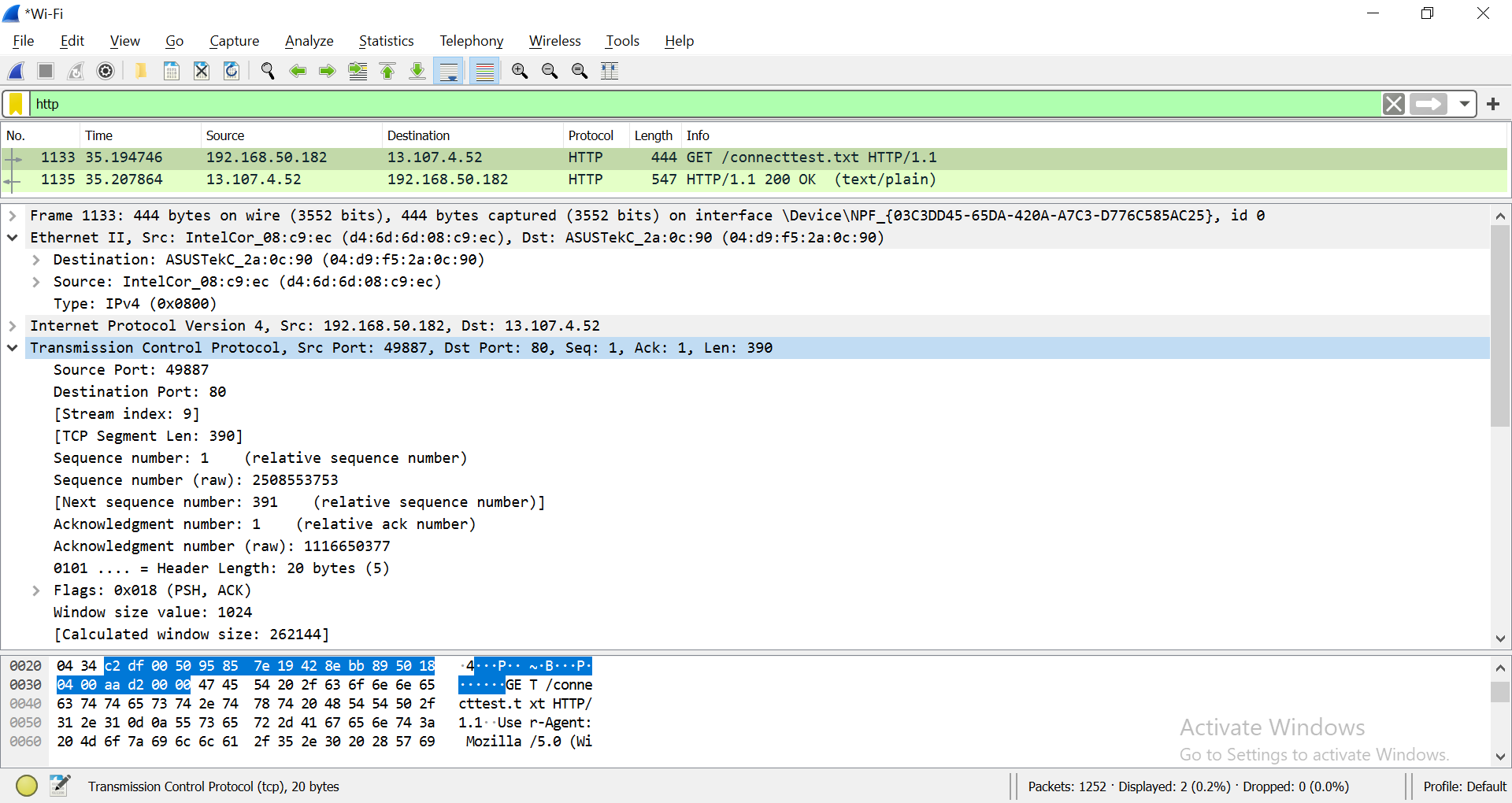
Based on the User-Agent field in the HTTP header, what is the type of browser?

|  |  |
| --- | --- |
| User-Agent | **Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36** |
| Type of browser | **Chrome** |

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

Observe the HTTP response.

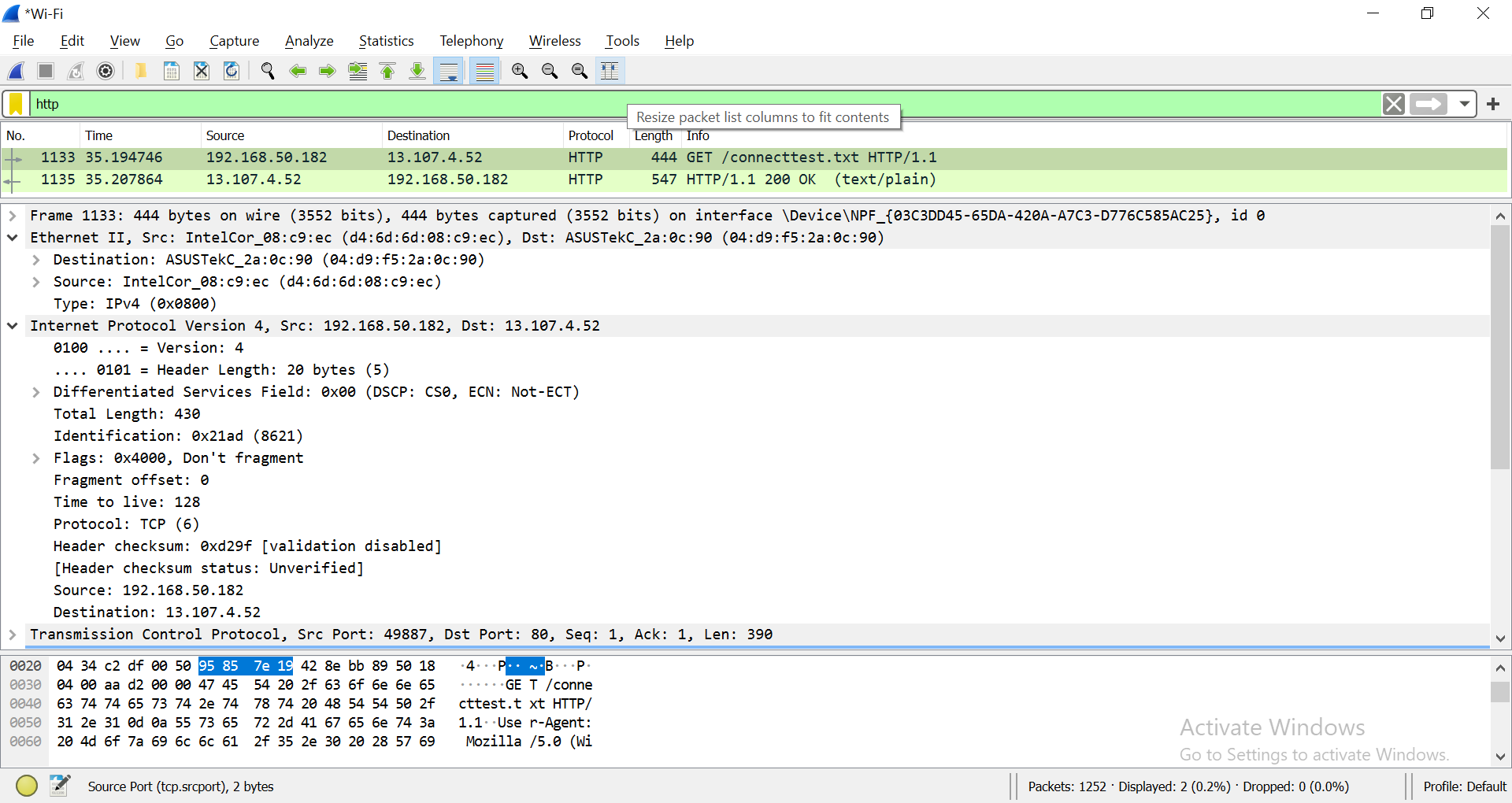


1. **Analyze TCP Packet containing HTTP Traffic**
2. Examine the HTTP request labelled as “*GET /connecttest.txt HTTP/1.1*”
3. Write down the source and destination Port Number.

|  |  |  |  |
| --- | --- | --- | --- |
|  | Hex | Binary | Decimal |
| Source port | f1 7a | 1111 0001 0111 1010 | 61818 |
| Destination port | 00 50 | 0101 0000 | 80 |

|  |  |
| --- | --- |
| 0000 (0) | 1000 (8) |
| 0001 (1) | 1001 (9) |
| 0010 (2) | 1010 (10) |
| 0011 (3) | 1011 (11) |
| 0100 (4) | 1100 (12) |
| 0101 (5) | 1101 (13) |
| 0110 (6) | 1110 (14) |
| 0111 (7) | 1111 (15) |

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



|  |  |
| --- | --- |
| Source IP address | 192.168.0.189 |
| Is the source IP address, your IP address? (true or false) | True |

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

|  |  |
| --- | --- |
| Domain Name | IP Address |
| <http://www.msftconnecttest.com/connecttest.txt> | 13.107.4.52 |

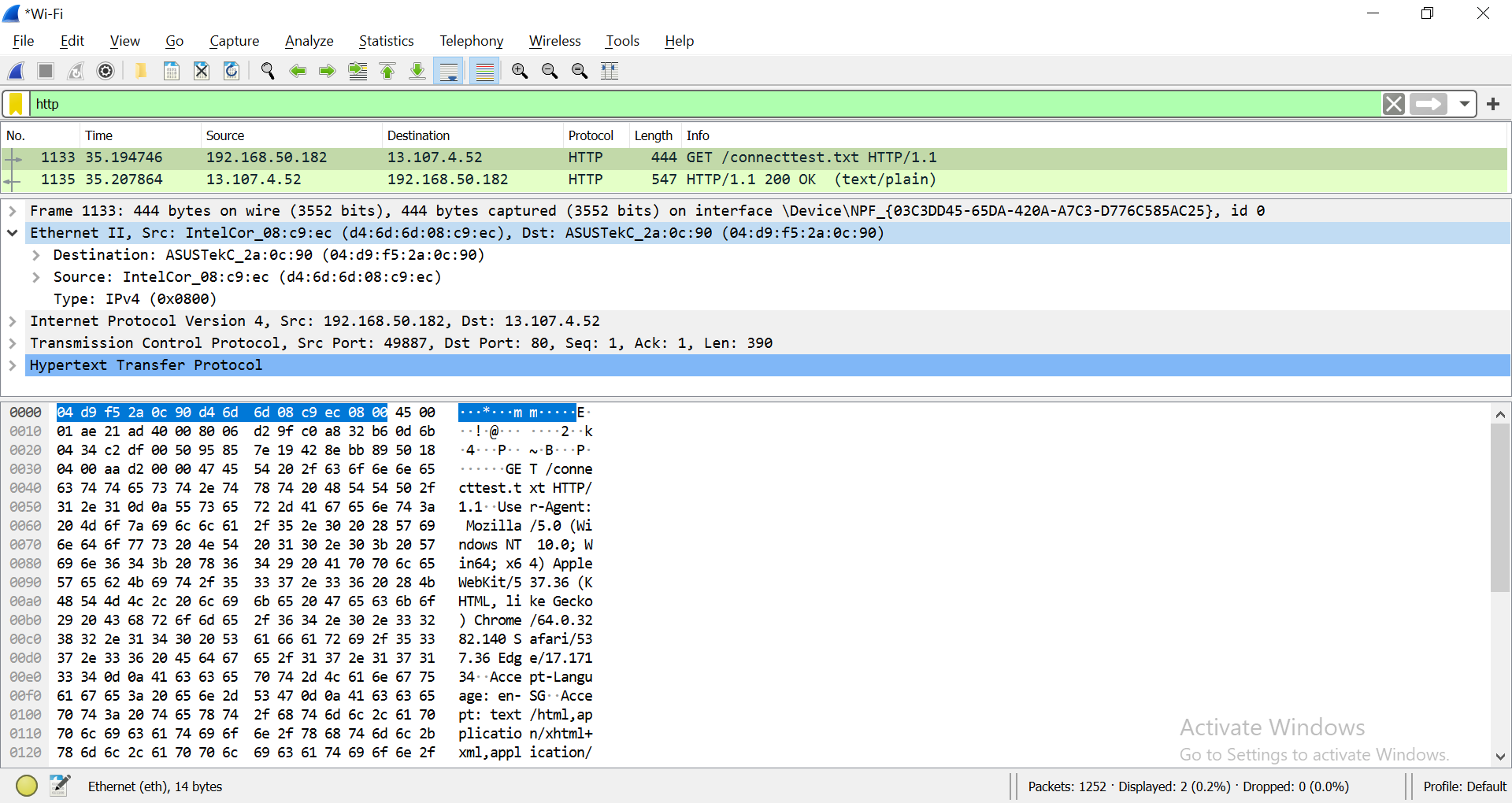
Expand Ethernet II to view Ethernet details. Find the source MAC Address and destination MAC Address of the frame.

|  |  |
| --- | --- |
| Source MAC Address | c8:09:a8:cd:f5:b9 |
| Destination MAC Address | 0c:80:63:a0:84:f1 |

**(OPTIONAL)**Apply the dns filter

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

|  |  |
| --- | --- |
| Destination IP address | 2001:4860:4860:8888 |
| Is the destination IP address your DNS Server? (true or false) | True |

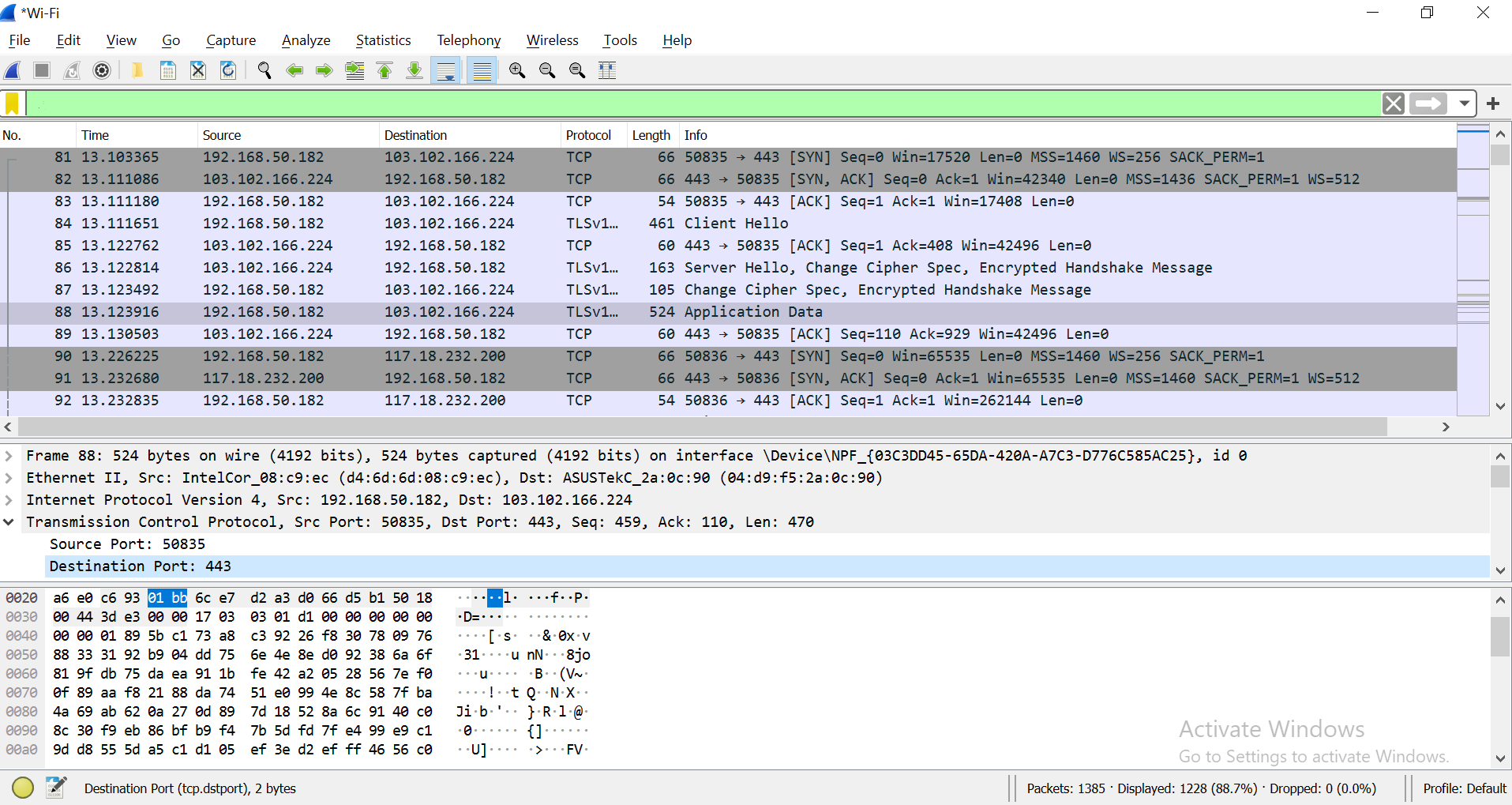
1. Expand Ethernet II to view Ethernet details.
2. Observe the Destination and Source fields. The destination should be your default gateway's MAC address and the source should be your MAC address. You can use [ipconfig /all](https://en.wikiversity.org/wiki/Ipconfig/All) and [arp -a](https://en.wikiversity.org/wiki/Computer_Networks/Management/Utilities/Arp/View) 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 | c2 a3 | 1100 0010 1010 0011 | 49827 |
| Destination port | 01 bb | 0001 1011 1011 | 443 |

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

*End of Practical*

1. What have you learnt?

Today, I have learnt more about packers and how even by just visiting a website on the internet, it sends packets for confirmation and responses all in a matter of a few milliseconds. I also learned a lot about protocols, namely http , tcp and dns.

1. Difficulties encountered and how you solved the problems?

One difficulty I encountered was when refreshing the page manually with the mouse, I could not actually get wireshark to correctly capture the right amount of things I needed. I then managed to solve this problem by ctrl + f5, what my teacher said. To my curiosity, I wondered what the difference was between the two and found that ctrl + f5 forces the cache to be restarted where as a normal refresh would load the cache thus saving time. With ctrl + f5, I then managed to get wireshark to properly capture everything I needed.