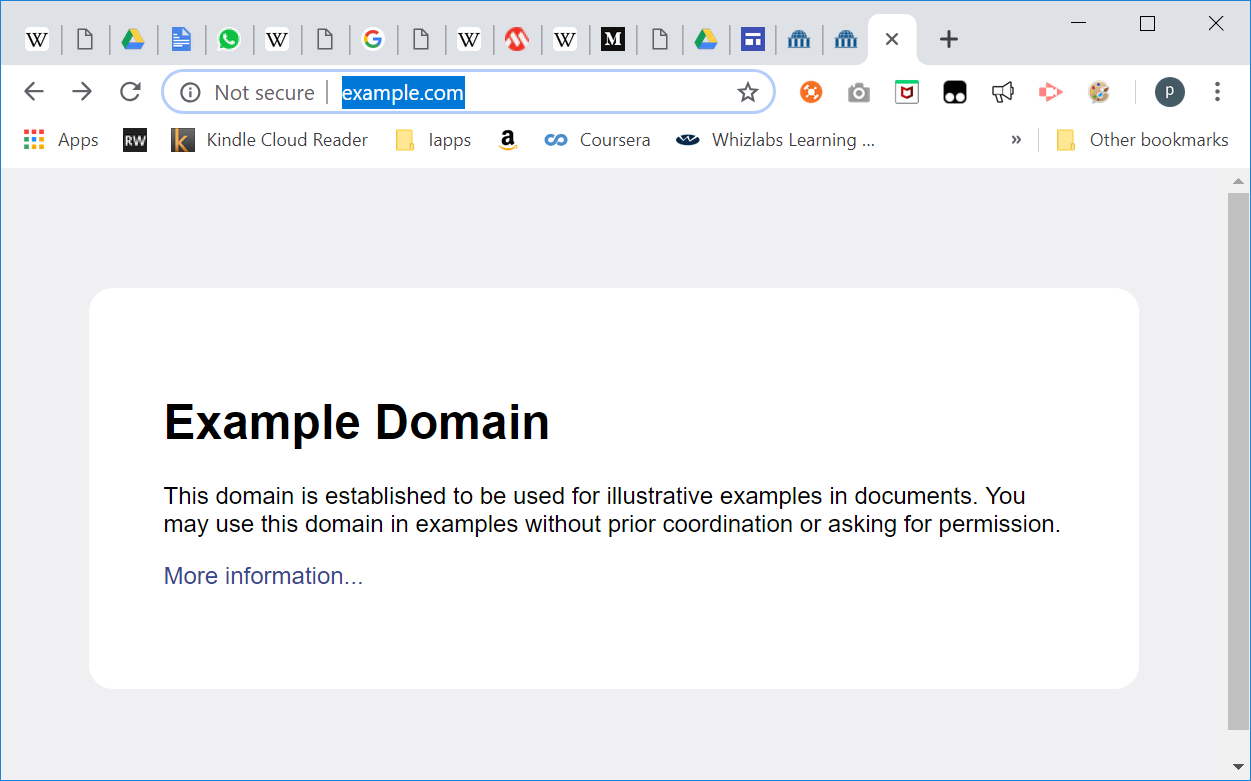
**Practical 06**

**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/).



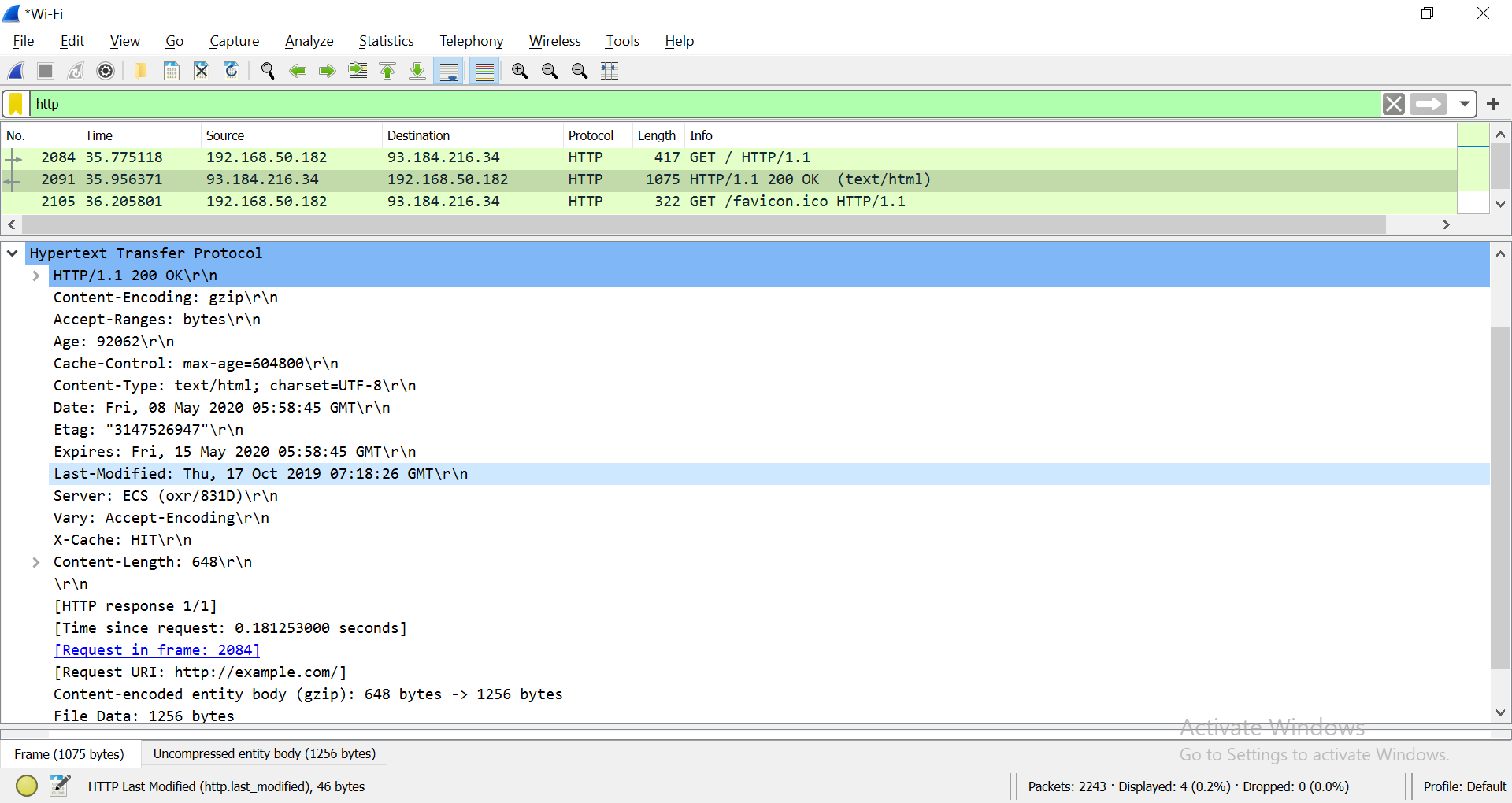
1. Stop Wireshark capture.
2. **Analyze HTTP Traffic**
3. Observe the traffic captured in the top Wireshark packet list pane. To view only HTTP traffic, type tcp.port == 80 (lower case) or **http** in the Filter box and press Enter.
4. Select the HTTP packet labelled “*GET / HTTP/1.1*”



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.

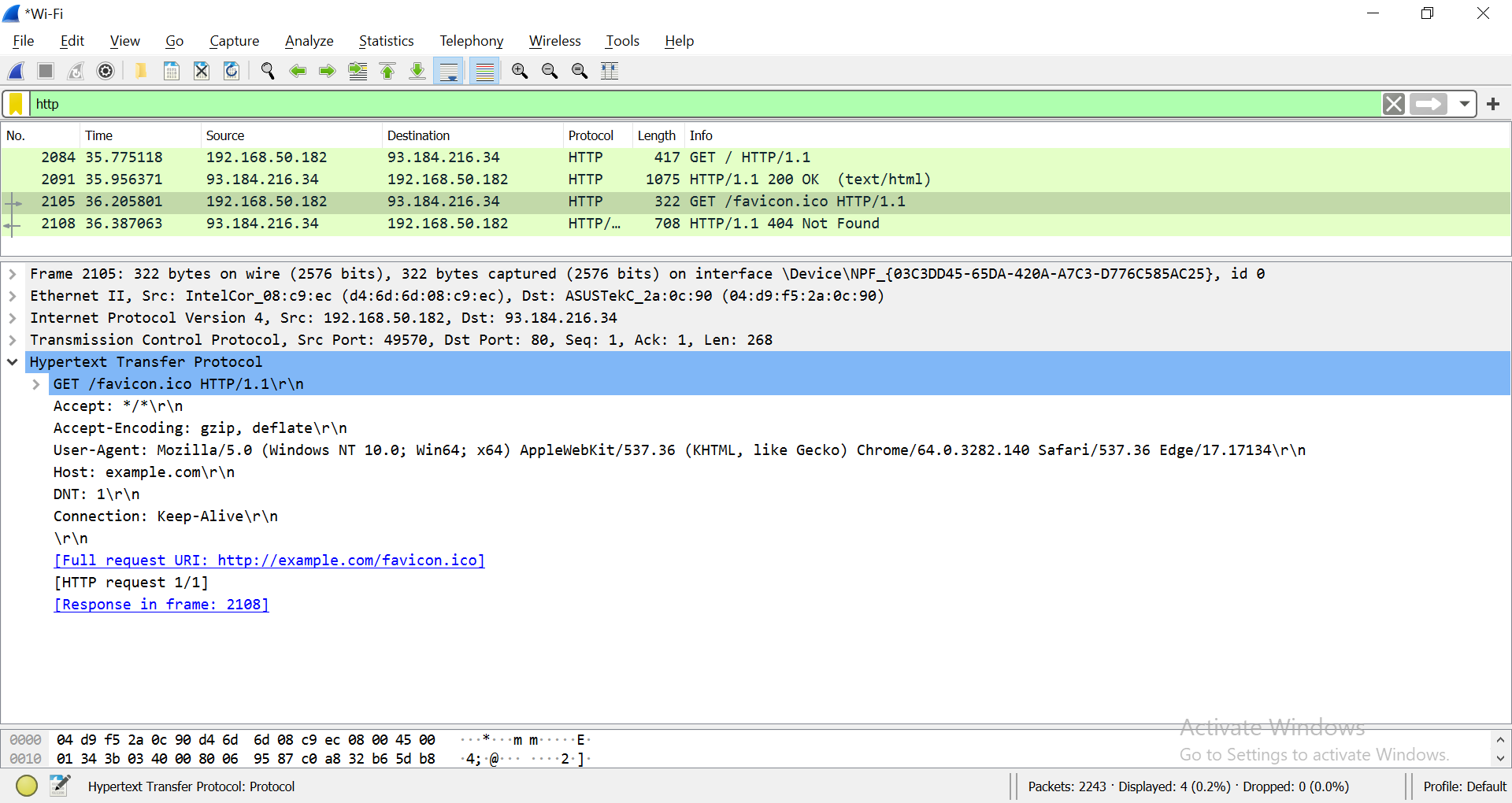


1. Observe the HTTP response.



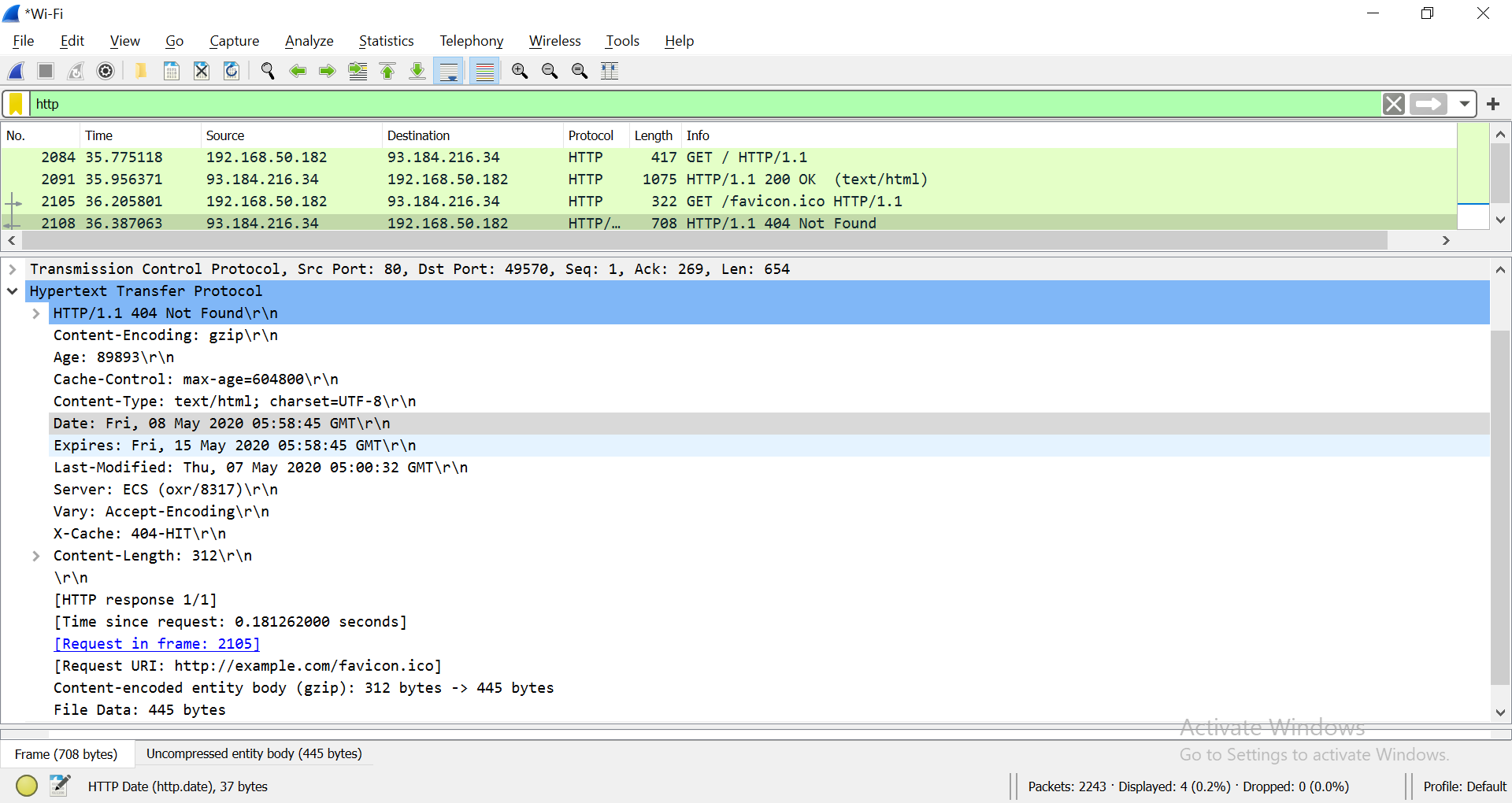
What is the HTTP response code for the request?

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



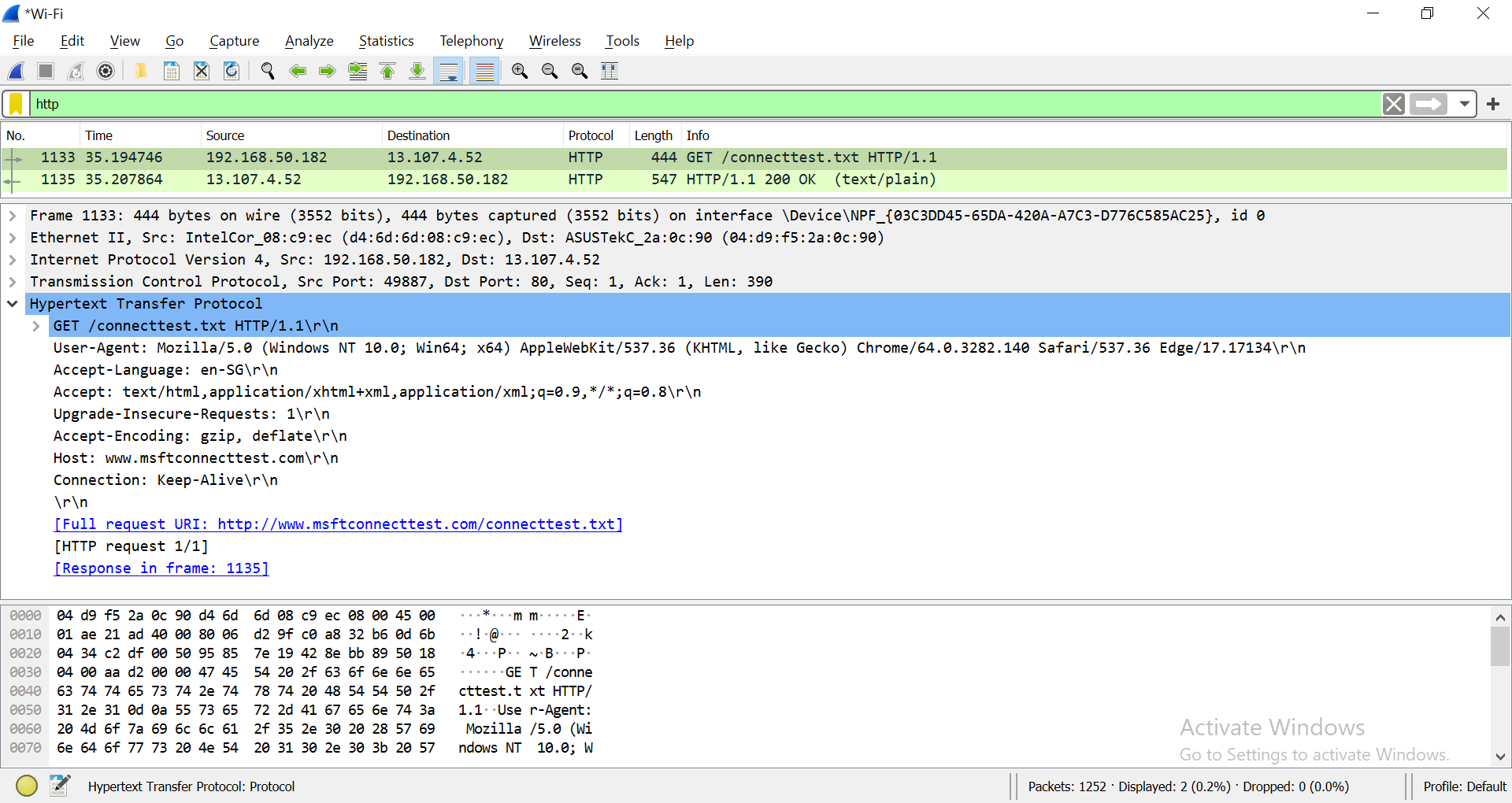
**Note:** If you don’t have the above HTTP request in Wireshark, you can use another browser to send request to example.com again.

Observe the HTTP response.



What is the HTTP response code for the request?

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?

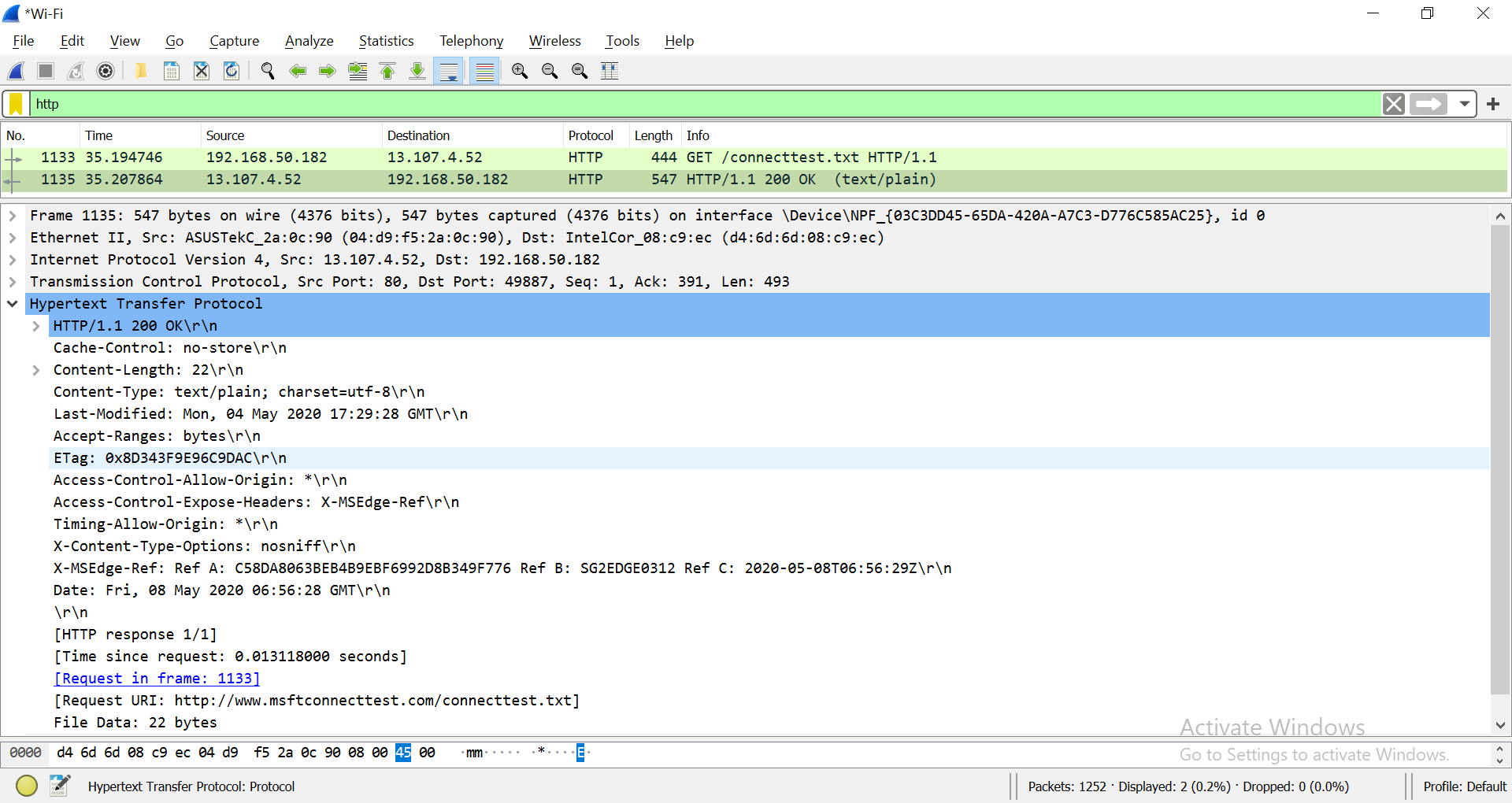
|  |  |
| --- | --- |
| Requested resource | Request URI: /connecttest.txt |

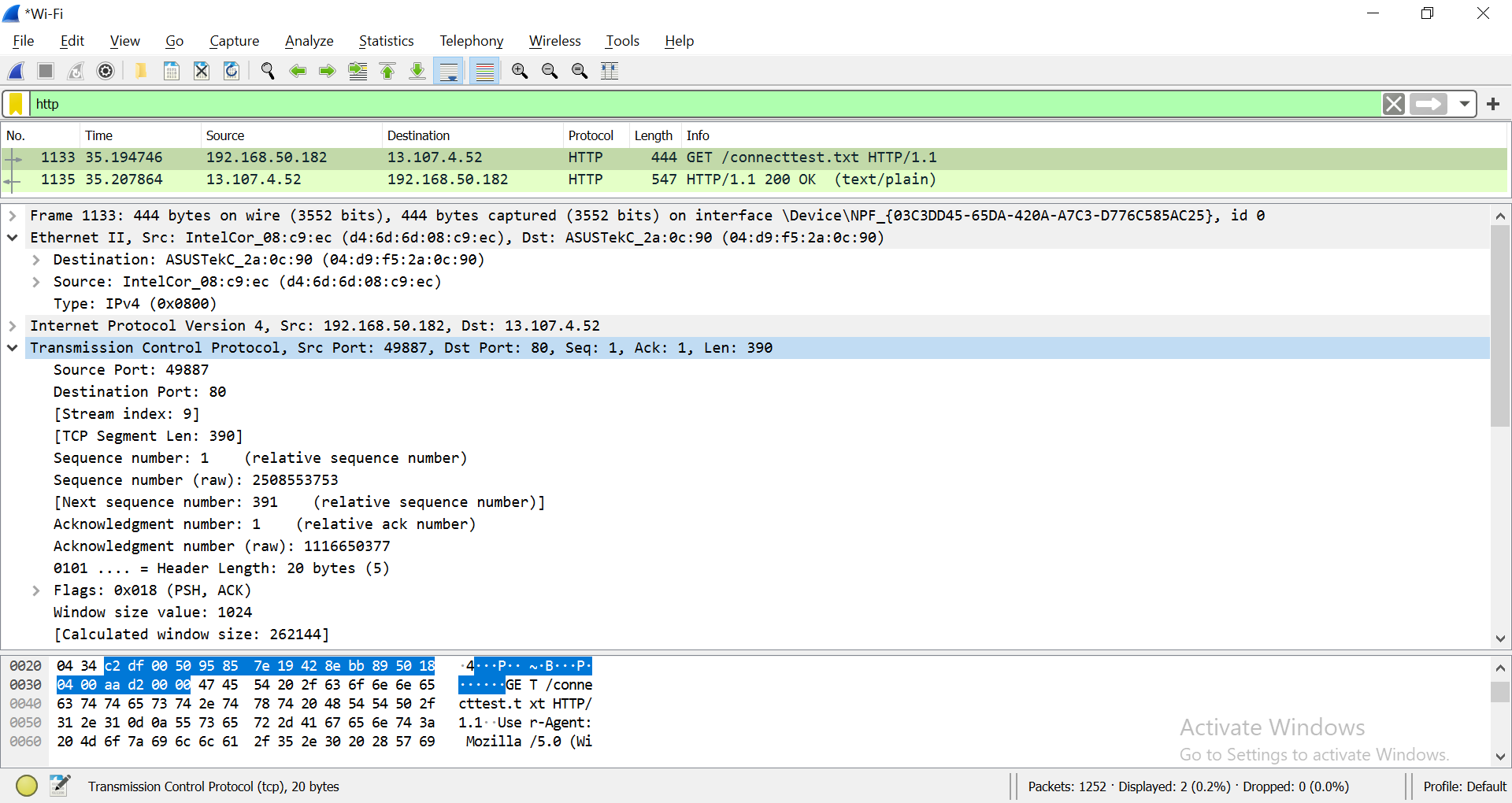
Based on the User-Agent field in the HTTP header, what is the type of browser?

|  |  |
| --- | --- |
| User-Agent | **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 | **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** |

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

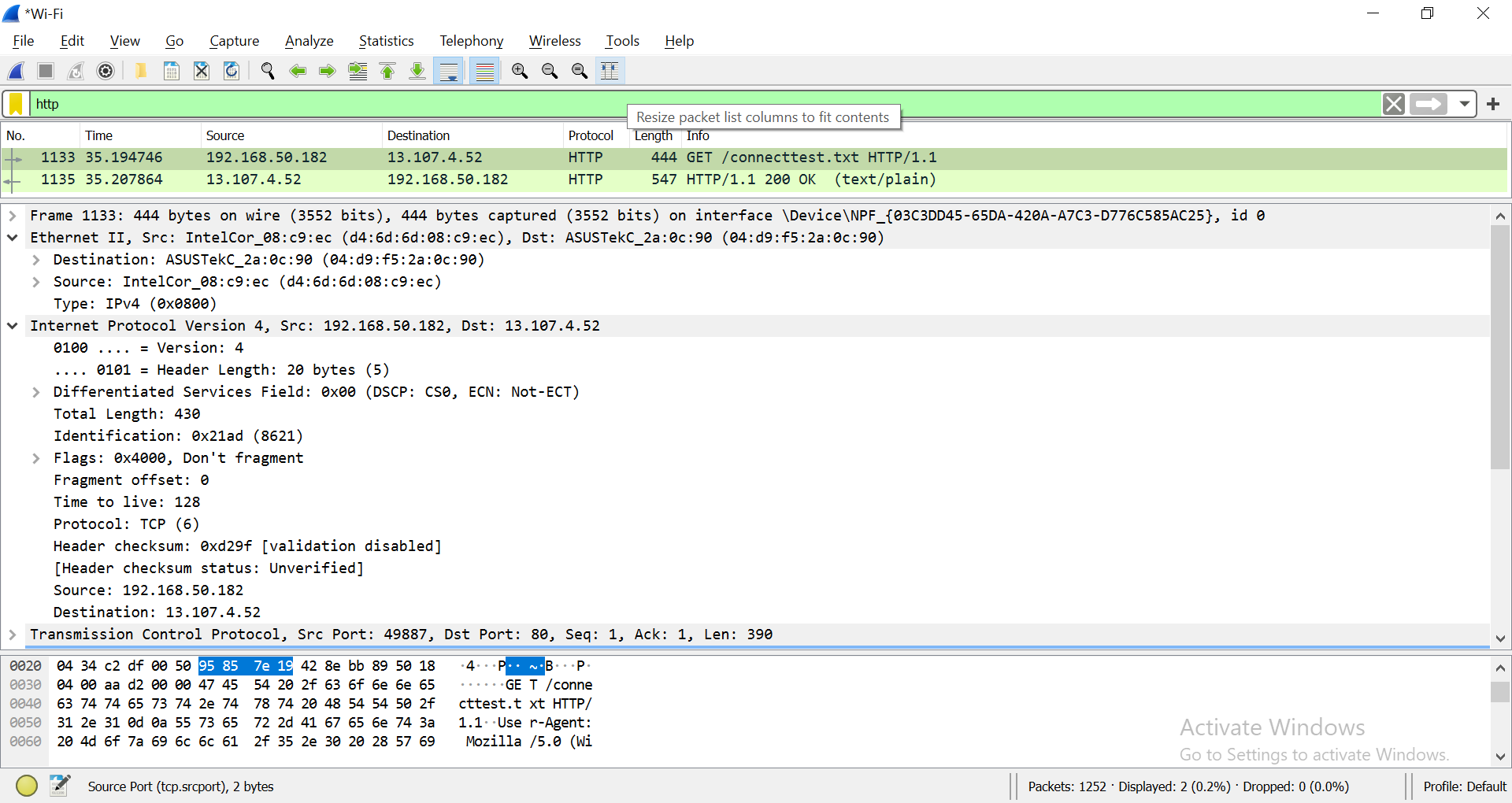
Observe the HTTP response.



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 | 0000 74 97 79 80 61 4b 28 74 f5 d6 02 01 08 00 45 28  0010 00 e8 02 d4 40 00 3d 06 0c 99 7c 9b de 30 c0 a8  0020 12 07 00 50 b4 48 26 06 d3 3a bc dc 33 c2 50 18  0030 01 f5 97 be 00 00 48 54 54 50 2f 31 2e 31 20 32  0040 30 30 20 4f 4b 0d 0a 43 6f 6e 74 65 6e 74 2d 4c  0050 65 6e 67 74 68 3a 20 32 32 0d 0a 44 61 74 65 3a  0060 20 57 65 64 2c 20 32 32 20 4d 61 79 20 32 30 32  0070 34 20 30 33 3a 30 37 3a 34 36 20 47 4d 54 0d 0a  0080 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70  0090 2d 61 6c 69 76 65 0d 0a 43 6f 6e 74 65 6e 74 2d  00a0 54 79 70 65 3a 20 74 65 78 74 2f 70 6c 61 69 6e  00b0 0d 0a 43 61 63 68 65 2d 43 6f 6e 74 72 6f 6c 3a  00c0 20 6d 61 78 2d 61 67 65 3d 33 30 2c 20 6d 75 73  00d0 74 2d 72 65 76 61 6c 69 64 61 74 65 0d 0a 0d 0a  00e0 4d 69 63 72 6f 73 6f 66 74 20 43 6f 6e 6e 65 63  00f0 74 20 54 65 73 74 | 0050 | 80 |
| Destination port | 0000 74 97 79 80 61 4b 28 74 f5 d6 02 01 08 00 45 28  0010 00 e8 02 d4 40 00 3d 06 0c 99 7c 9b de 30 c0 a8  0020 12 07 00 50 b4 48 26 06 d3 3a bc dc 33 c2 50 18  0030 01 f5 97 be 00 00 48 54 54 50 2f 31 2e 31 20 32  0040 30 30 20 4f 4b 0d 0a 43 6f 6e 74 65 6e 74 2d 4c  0050 65 6e 67 74 68 3a 20 32 32 0d 0a 44 61 74 65 3a  0060 20 57 65 64 2c 20 32 32 20 4d 61 79 20 32 30 32  0070 34 20 30 33 3a 30 37 3a 34 36 20 47 4d 54 0d 0a  0080 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70  0090 2d 61 6c 69 76 65 0d 0a 43 6f 6e 74 65 6e 74 2d  00a0 54 79 70 65 3a 20 74 65 78 74 2f 70 6c 61 69 6e  00b0 0d 0a 43 61 63 68 65 2d 43 6f 6e 74 72 6f 6c 3a  00c0 20 6d 61 78 2d 61 67 65 3d 33 30 2c 20 6d 75 73  00d0 74 2d 72 65 76 61 6c 69 64 61 74 65 0d 0a 0d 0a  00e0 4d 69 63 72 6f 73 6f 66 74 20 43 6f 6e 6e 65 63  00f0 74 20 54 65 73 74 | B4 48 | 46152 |

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



|  |  |
| --- | --- |
| Source IP address | Source Address: 192.168.18.7 |
| 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/ | 124.155.222.48 |

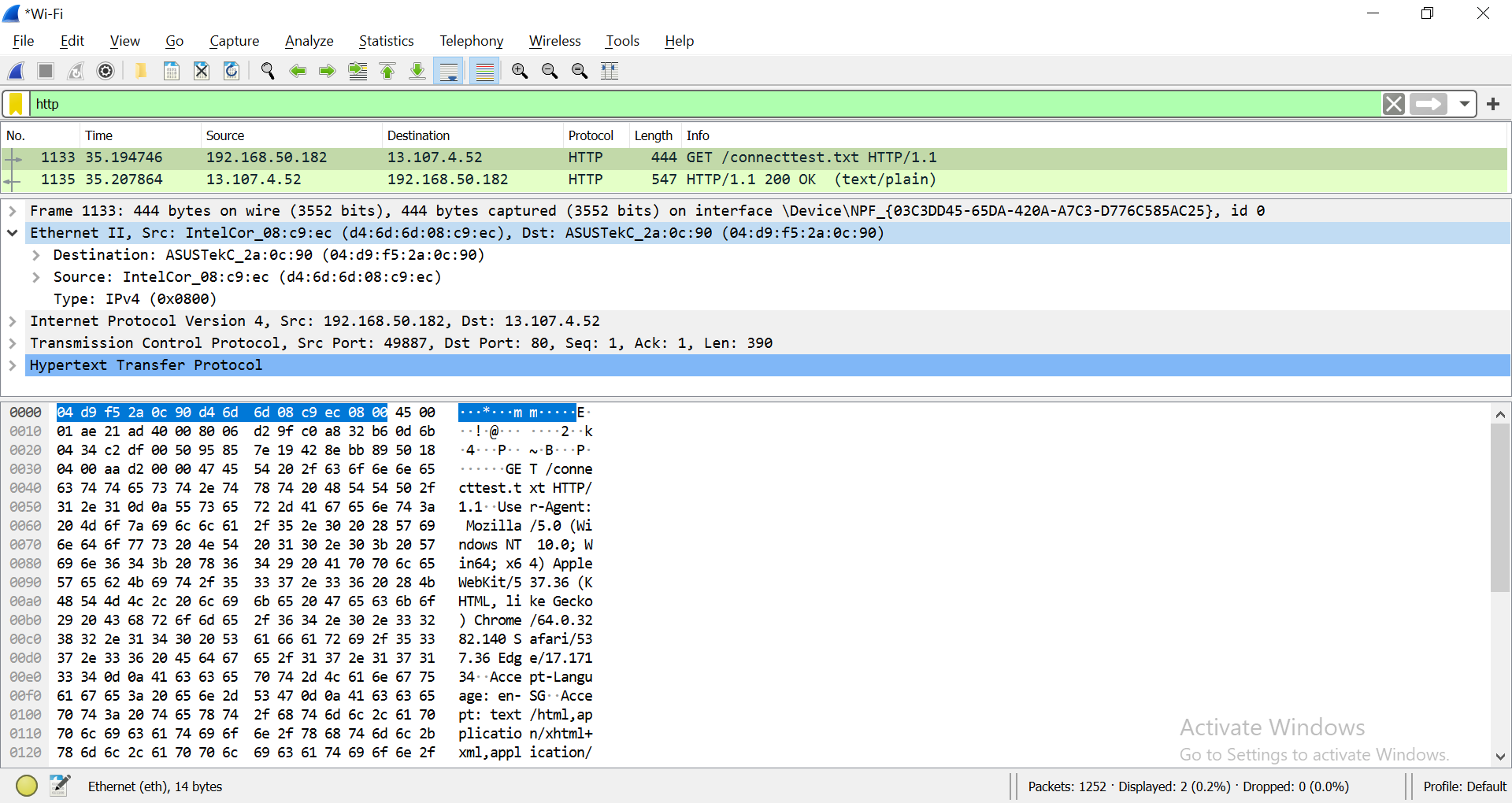
Expand Ethernet II to view Ethernet details. Find the source MAC Address and destination MAC Address of the frame.

|  |  |
| --- | --- |
| Source MAC Address | CloudNetwork\_80:61:4b (74:97:79:80:61:4b) |
| Destination MAC Address | NokiaSolutio\_d6:02:01 (28:74:f5:d6:02:01) |

**(OPTIONAL)**

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

|  |  |
| --- | --- |
| Destination IP address | 124.155.222.48 |
| Is the destination IP address your DNS Server? (true or false) | False |

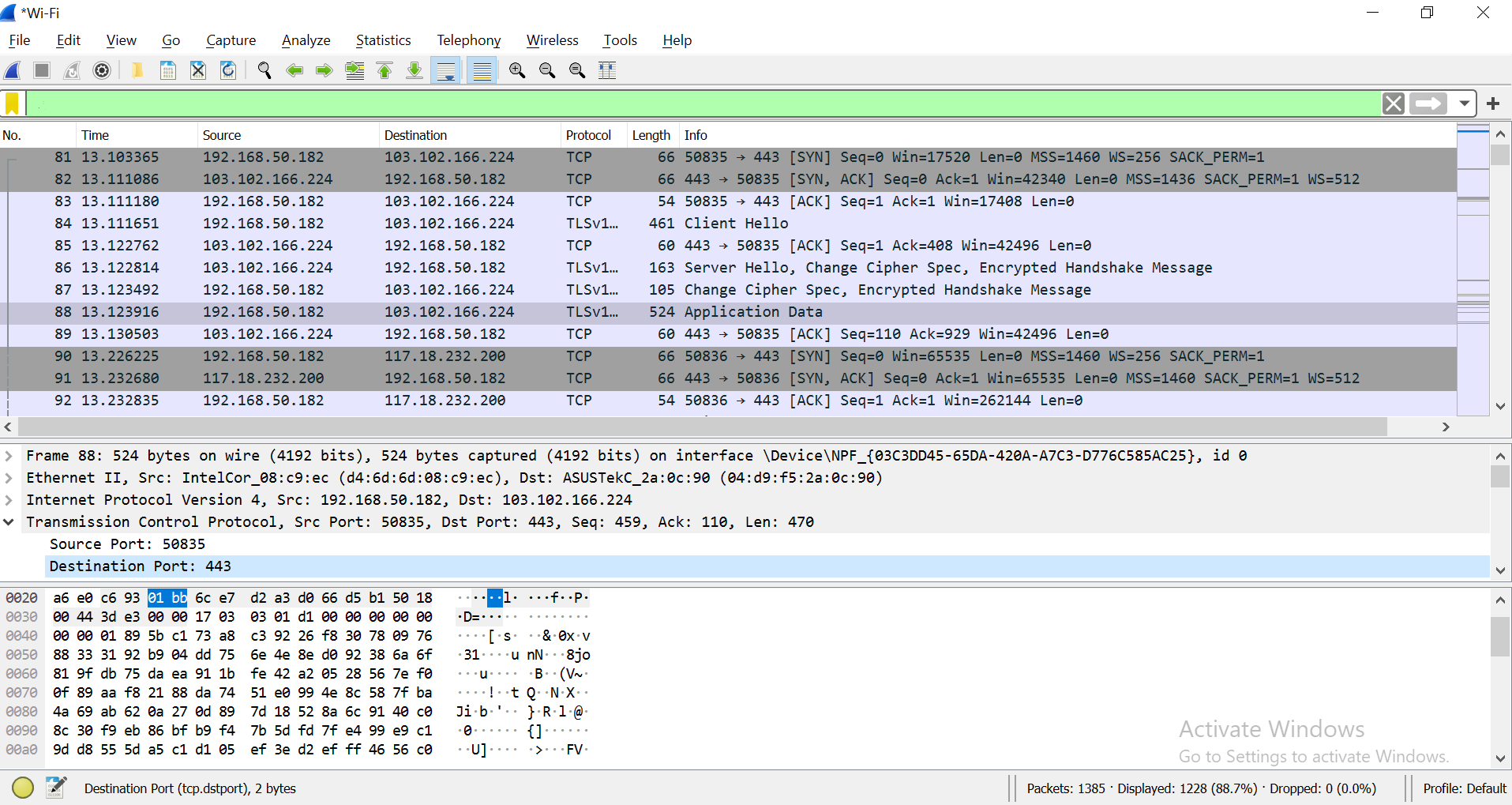
1. Expand Ethernet II to view Ethernet details.
2. Observe the Destination and Source fields. The destination should be your default gateway's MAC address and the source should be your MAC address. You can use [ipconfig /all](https://en.wikiversity.org/wiki/Ipconfig/All) and [arp -a](https://en.wikiversity.org/wiki/Computer_Networks/Management/Utilities/Arp/View) 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 | 0000 74 97 79 80 61 4b 28 74 f5 d6 02 01 08 00 45 28  0010 00 e8 02 d4 40 00 3d 06 0c 99 7c 9b de 30 c0 a8  0020 12 07 00 50 b4 48 26 06 d3 3a bc dc 33 c2 50 18  0030 01 f5 97 be 00 00 48 54 54 50 2f 31 2e 31 20 32  0040 30 30 20 4f 4b 0d 0a 43 6f 6e 74 65 6e 74 2d 4c  0050 65 6e 67 74 68 3a 20 32 32 0d 0a 44 61 74 65 3a  0060 20 57 65 64 2c 20 32 32 20 4d 61 79 20 32 30 32  0070 34 20 30 33 3a 30 37 3a 34 36 20 47 4d 54 0d 0a  0080 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70  0090 2d 61 6c 69 76 65 0d 0a 43 6f 6e 74 65 6e 74 2d  00a0 54 79 70 65 3a 20 74 65 78 74 2f 70 6c 61 69 6e  00b0 0d 0a 43 61 63 68 65 2d 43 6f 6e 74 72 6f 6c 3a  00c0 20 6d 61 78 2d 61 67 65 3d 33 30 2c 20 6d 75 73  00d0 74 2d 72 65 76 61 6c 69 64 61 74 65 0d 0a 0d 0a  00e0 4d 69 63 72 6f 73 6f 66 74 20 43 6f 6e 6e 65 63  00f0 74 20 54 65 73 74 | 0050 | 80 |
| Destination port | 0000 28 74 f5 d6 02 01 74 97 79 80 61 4b 08 00 45 00  0010 00 28 fe c5 40 00 80 06 03 d1 c0 a8 12 07 a2 9f  0020 82 ea b0 9b 01 bb 35 a1 39 7e 02 a2 7a 60 50 10  0030 03 ff 15 24 00 00 | (tõÖtyaKE(þÅ@ÑÀ¨¢ê°»5¡9~¢z`Pÿ$ | 25182 |

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

*End of Practical*