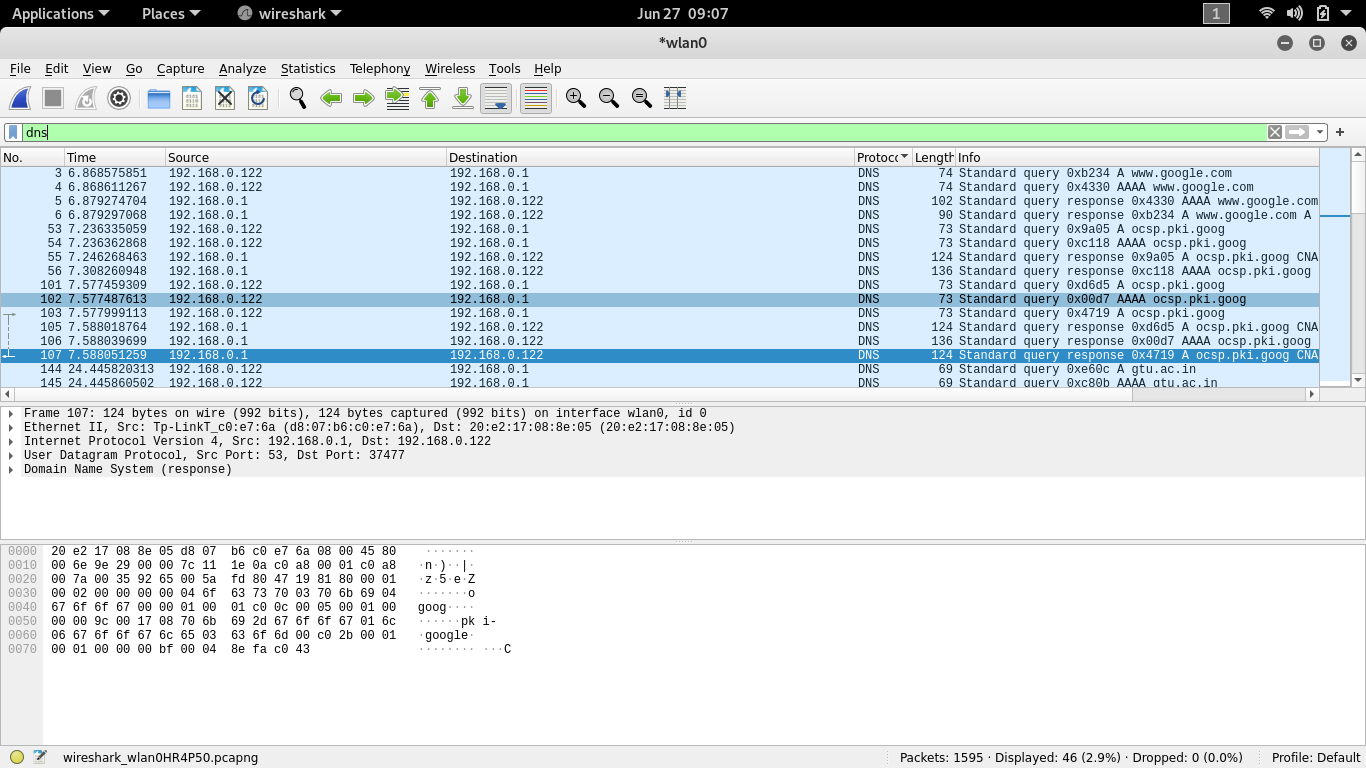
**1. List up to IO different protocols that appear in the protocol column in the unfiltered**

**packet-listing window.**

ANS 🡪 During the capturing time I found 8 Protocols…..which I mentioned a protocol images as below(screenshots)

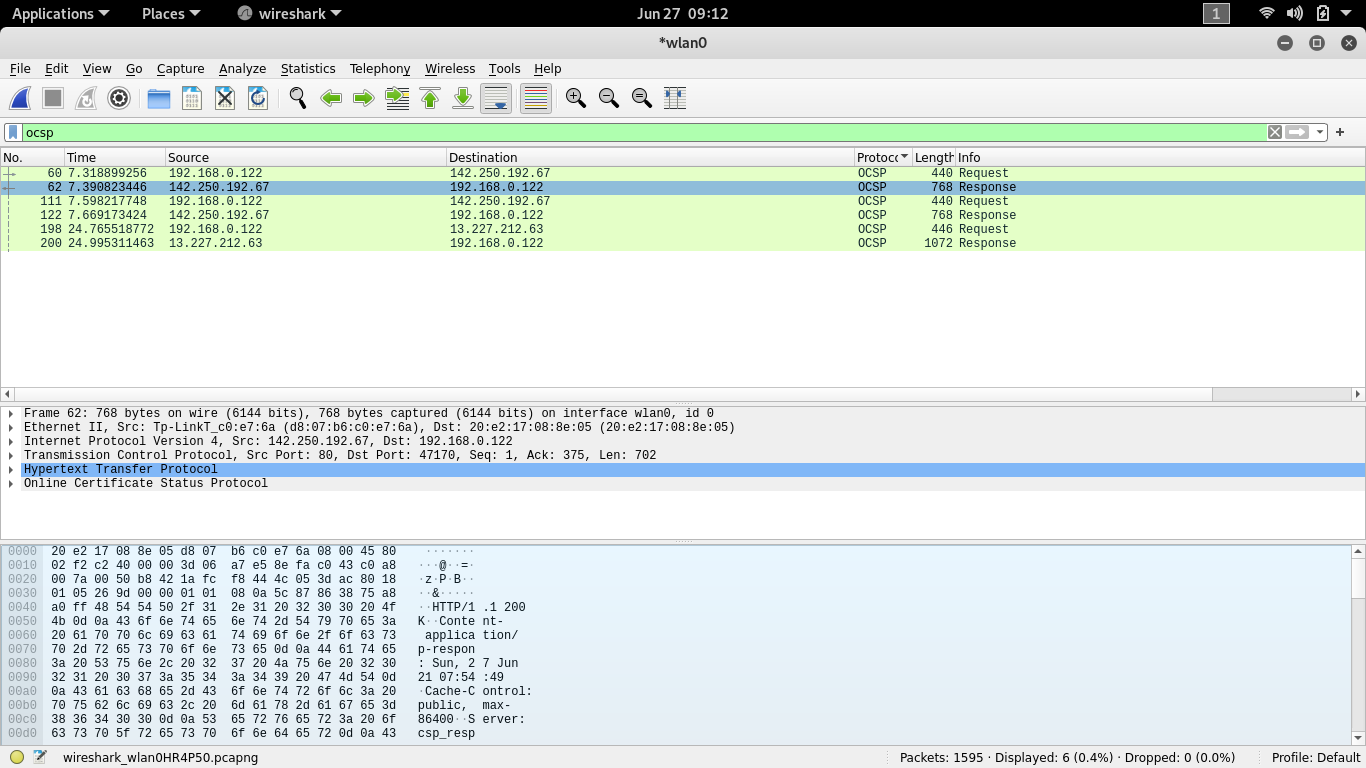
**DNS** -:



There are total 46 DNS Requests

DNS 🡪 The Domain Name System is a hierarchical and decentralized naming system for computers, services, or other resources connected to the Internet or a private network.

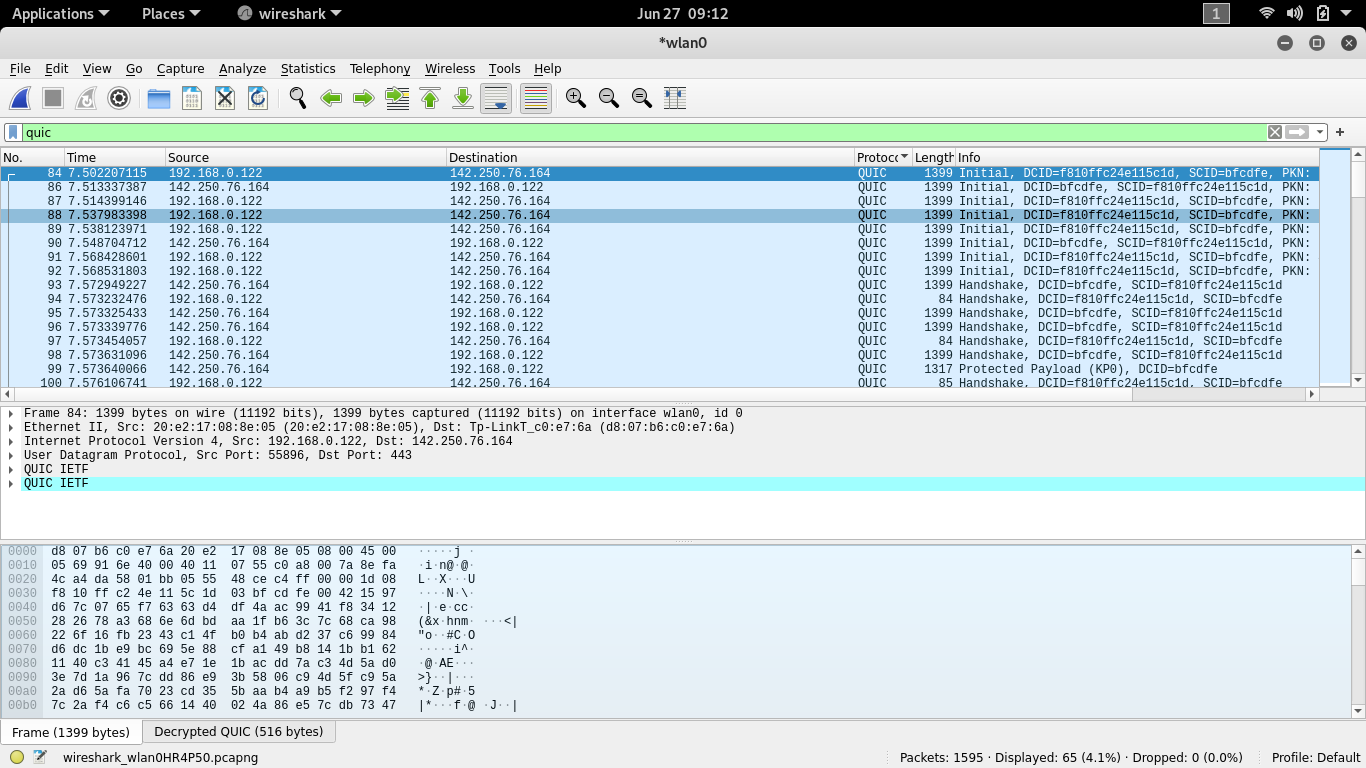
**OCSP -:**



Total 6 OCSP Requests

OSCP 🡪 The Online Certificate Status Protocol is an Internet protocol used for obtaining the revocation status of an X.509 digital certificate. It is described in RFC 6960

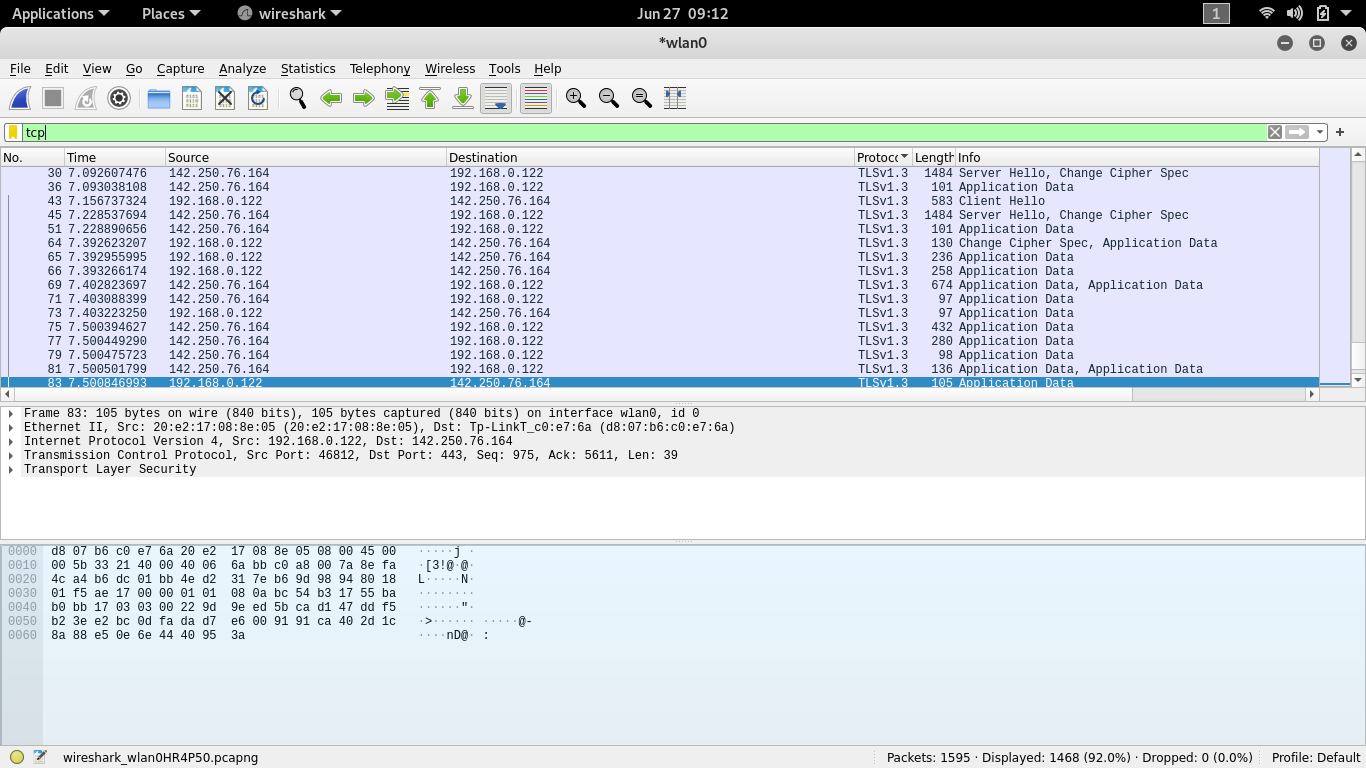
**QUIC -:**



There are Total 65 QUIC Requests

QUIC 🡪 QUIC is a general-purpose transport layer network protocol initially designed by Jim Roskind at Google, implemented, and deployed in 2012, announced publicly in 2013 as experimentation broadened

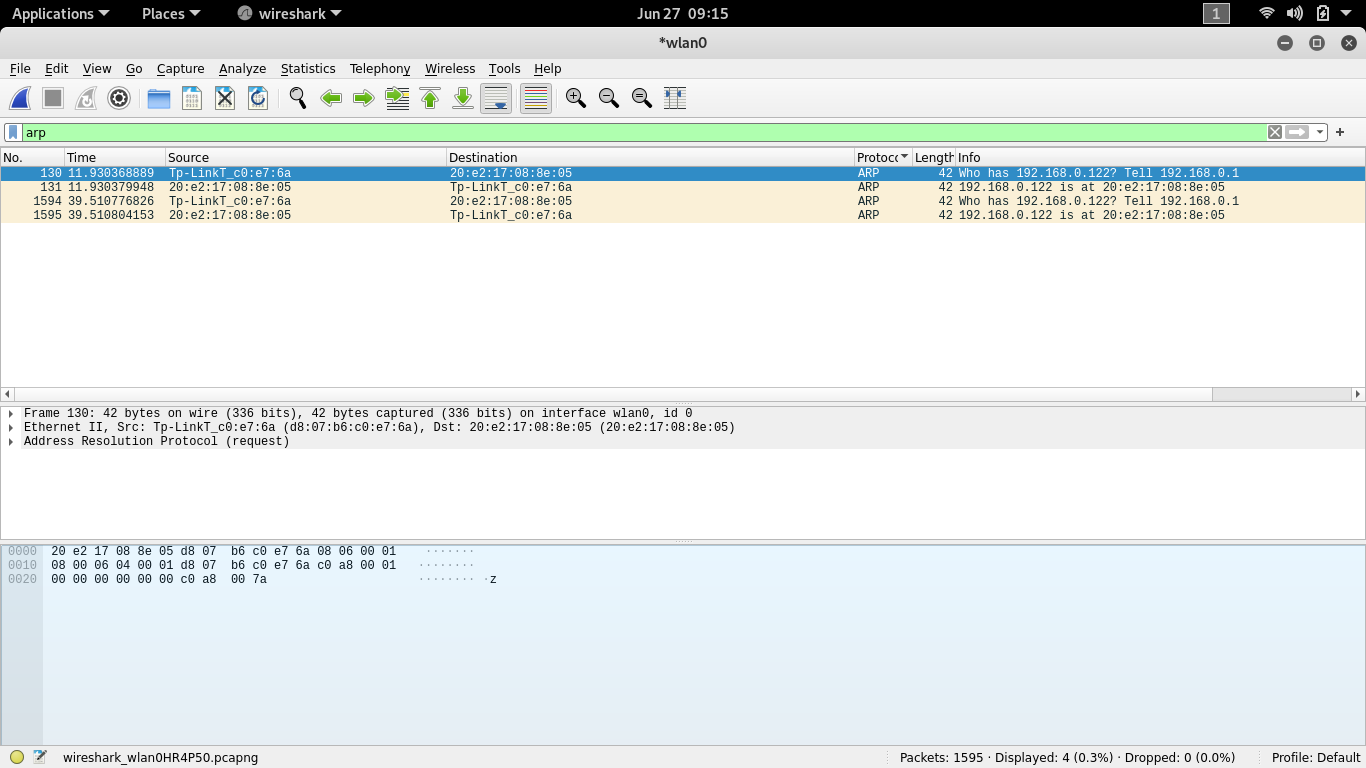
**TCP -:**

****

There are total 1448 TCP Requests

TCP 🡪 The Transmission Control Protocol is one of the main protocols of the Internet protocol suite. It originated in the initial network implementation in which it complemented the Internet Protocol. Therefore, the entire suite is commonly referred to as TCP/IP.

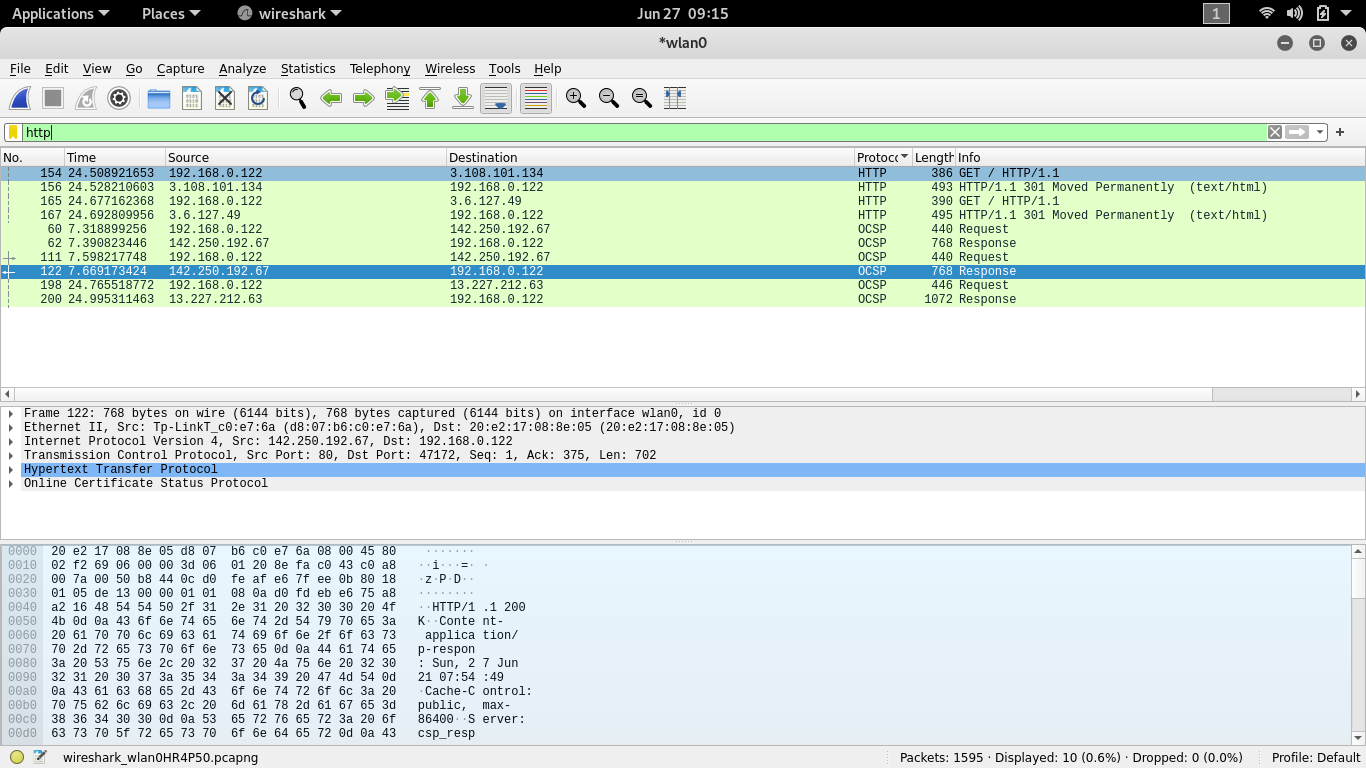
ARP -:



Total 4 ARP Requests

ARP 🡪 The Address Resolution Protocol is a communication protocol used for discovering the link layer address, such as a MAC address, associated with a given internet layer address, typically an IPv4 address. This mapping is a critical function in the Internet protocol suite

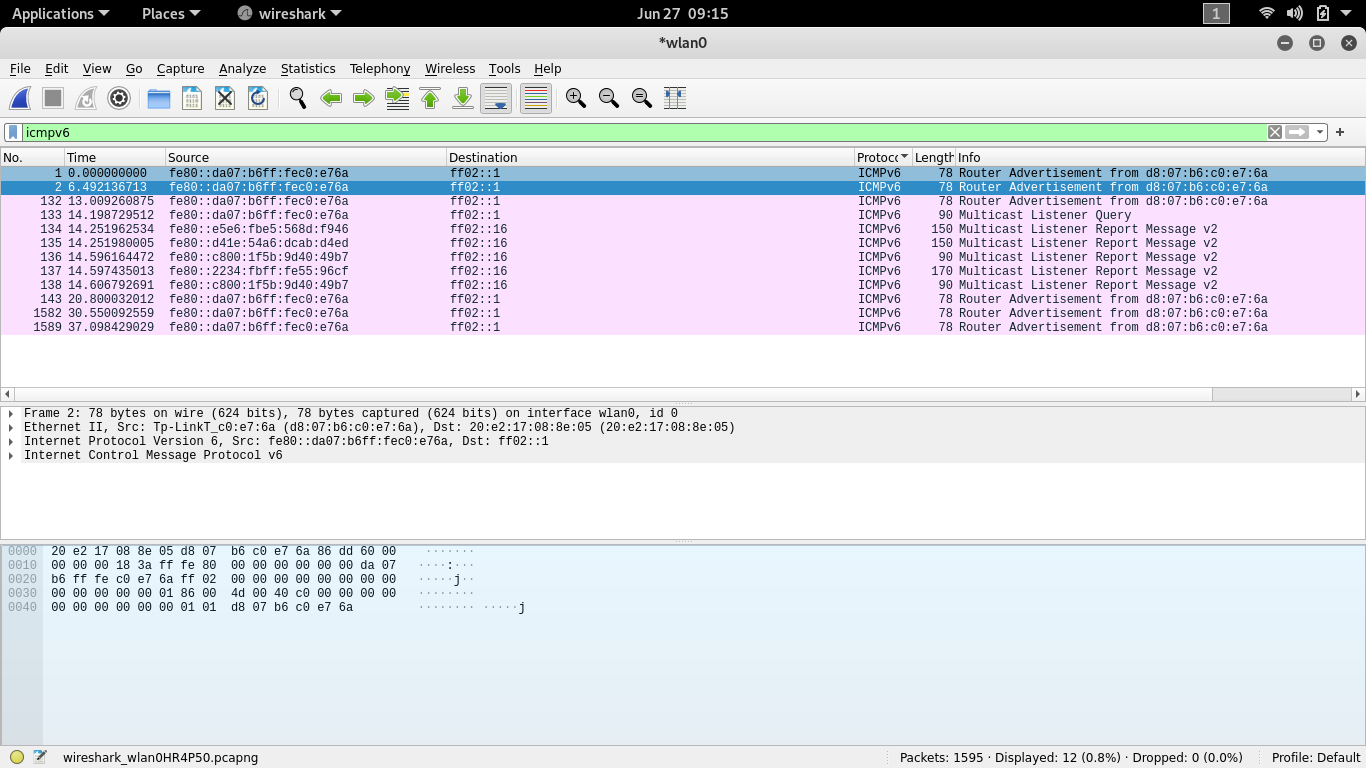
HTTP -:



There are Total 10 http Requests

Http 🡪 **HTTP** is a **protocol** which allows the fetching of resources, such as HTML documents. It is the foundation of any data exchange on the Web and it is a client-server **protocol**, which means requests are initiated by the recipient, usually the Web browser

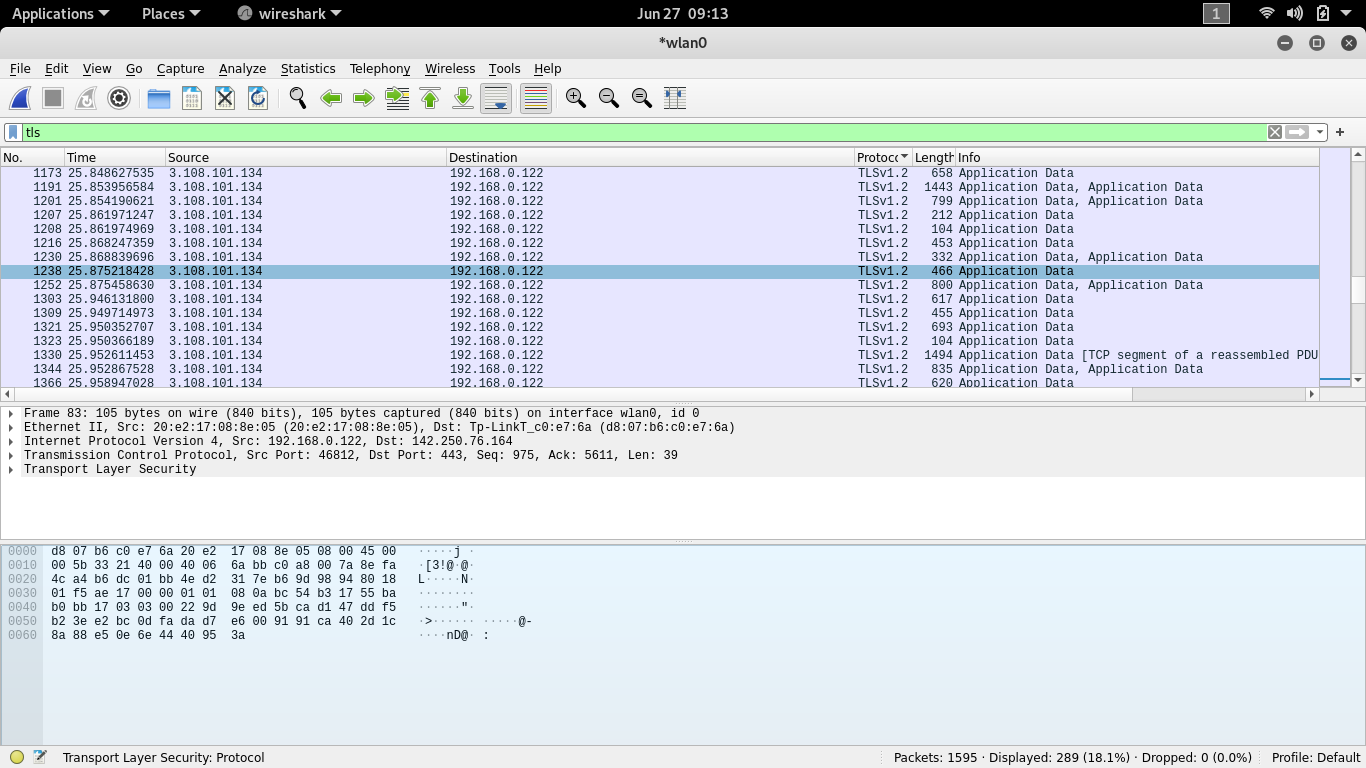
ICMPV6 -:



There total 12 ICmpv6 Requests

Icmpv6 🡪 Internet Control Message Protocol version 6 is the implementation of the Internet Control Message Protocol for Internet Protocol version 6. ICMPv6 is defined in RFC 4443

TSLV1.2 and TLSC1.3 -:



Total 289 Protocols of TSLV1.2 And 1.3

TSLV 🡪 Currently  **TLSv1**. **2** is the newest SSL **protocol** version supported by OpenSSH on z/VSE. It introduces new SSL/TLS cipher suites that use the SHA-256 hash algorithm instead of the SHA-1 function, which adds significant strength to the data integrity.

**2. How long did it take from when the HTTP GET message was sent until the HTTP**

**OK reply was received? (By default, the value of the Time column in the packet listing**

**window is the amount of time, in seconds, since Wireshark tracing began. To display the**

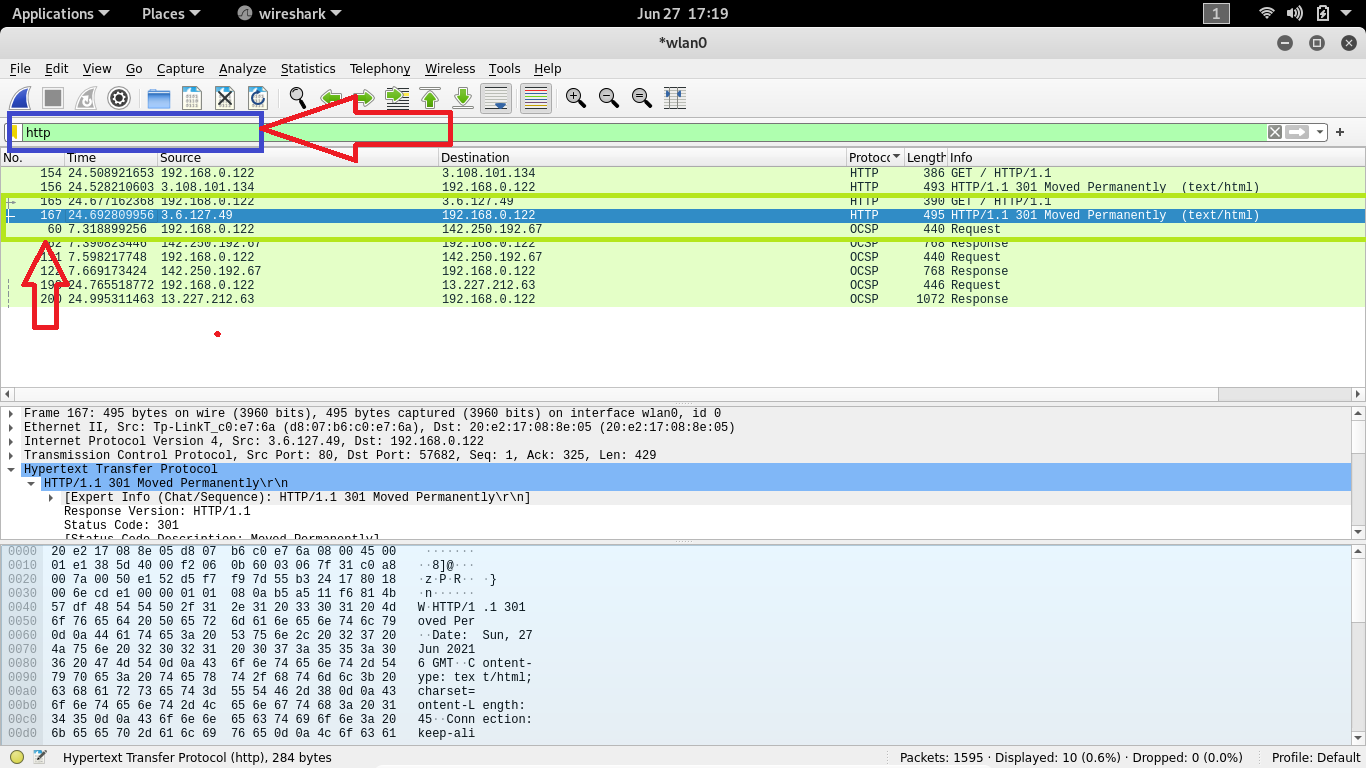
**Time field in time-of-day format, select the Wireshark View pull down menu, then select**

**Time Display Format, then select Time-of-day. For now you don’t need to understand**

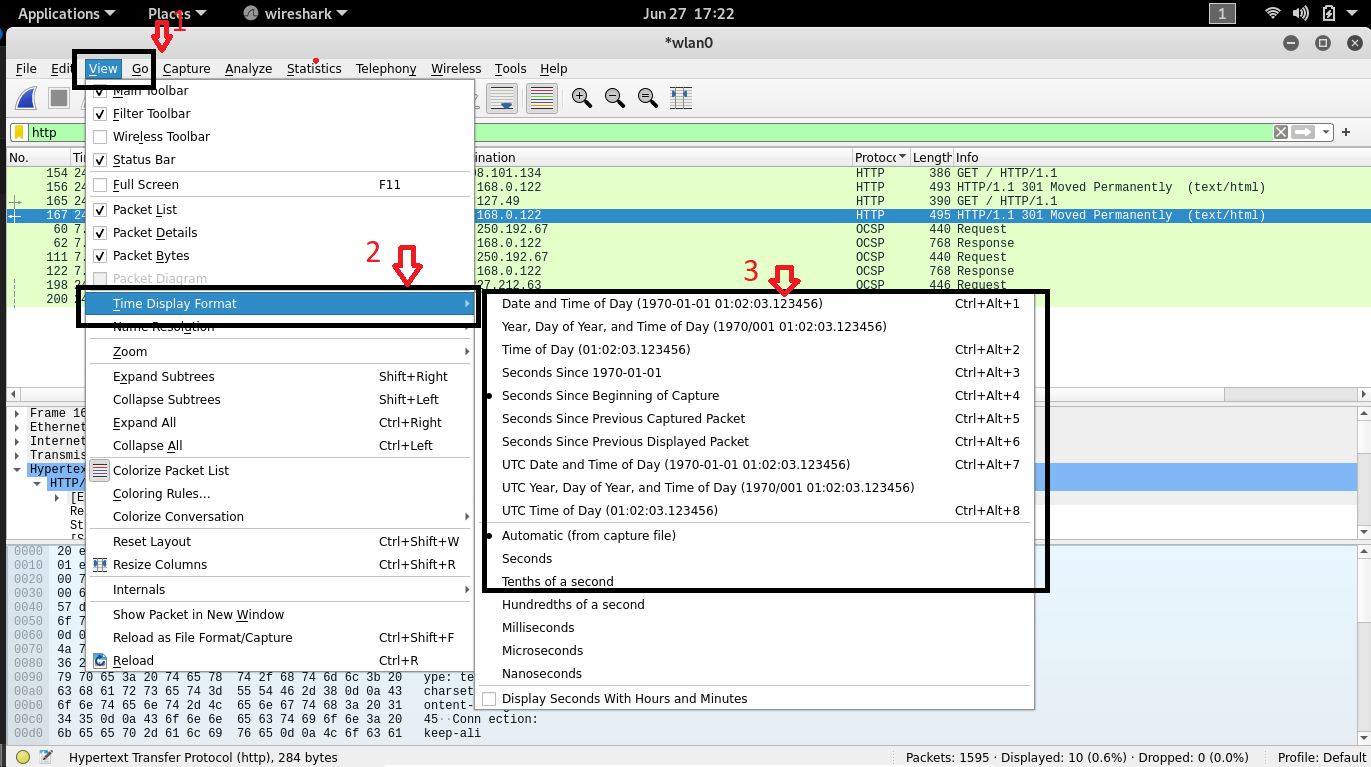
**HTTP GET and OK, but reading the textbook may be helpful if you are curious on how**

**they work.).**

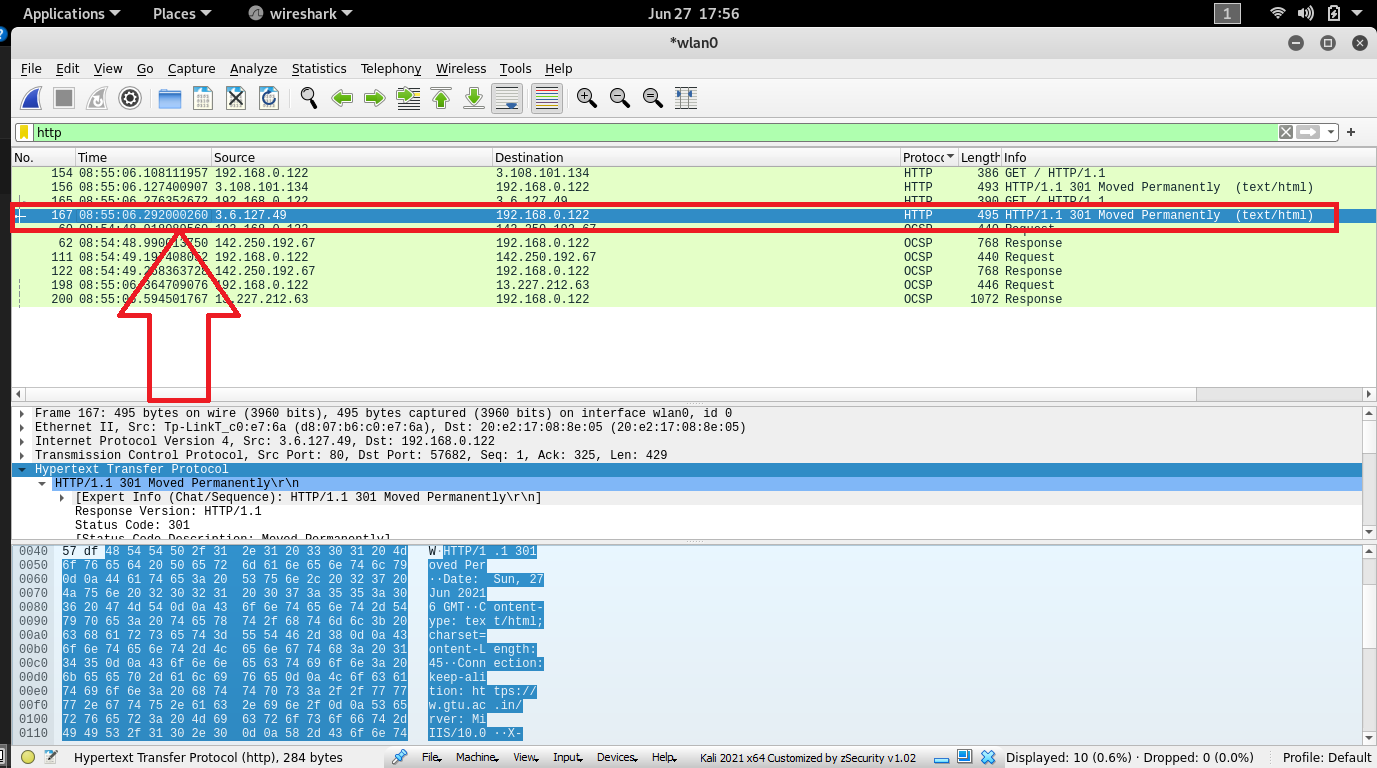
ANS 🡪 Reply was received in 0.015647588

****

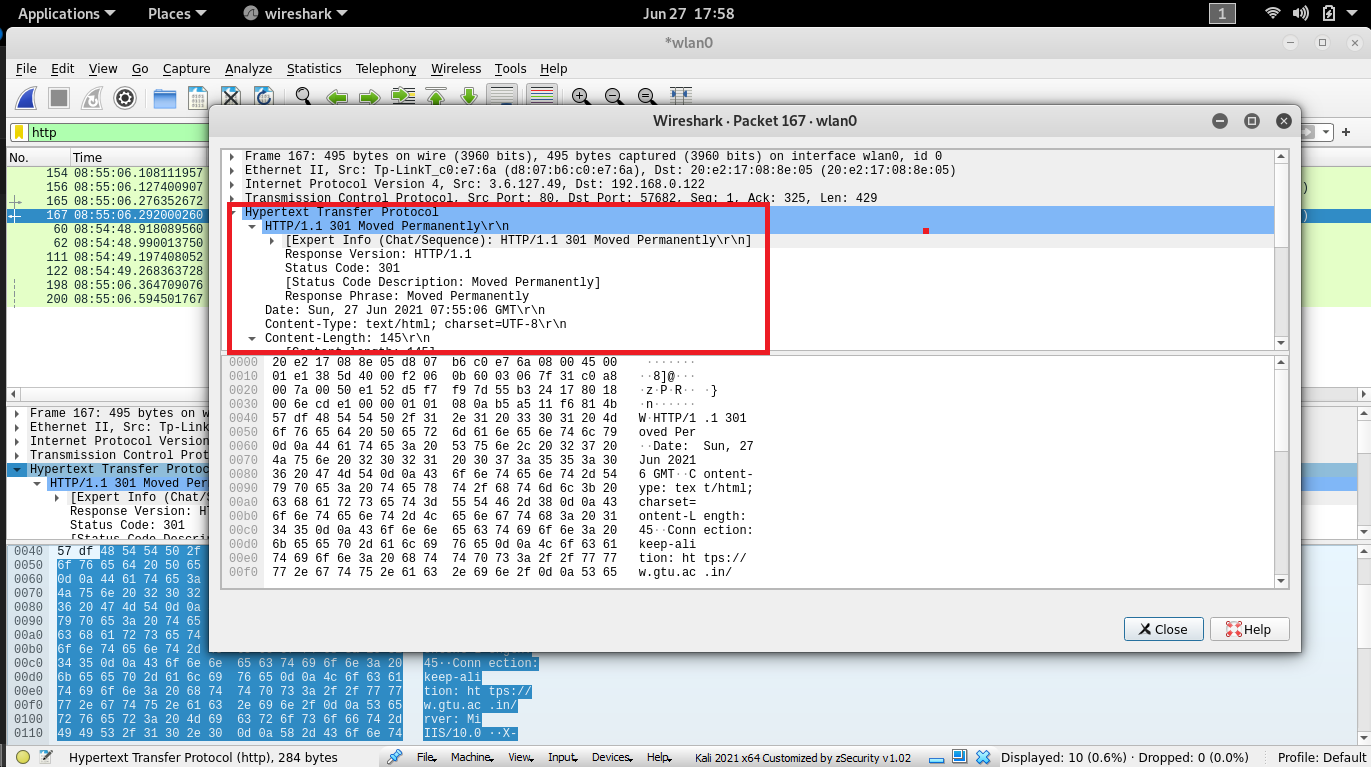
Search http in Apply as Display filter option



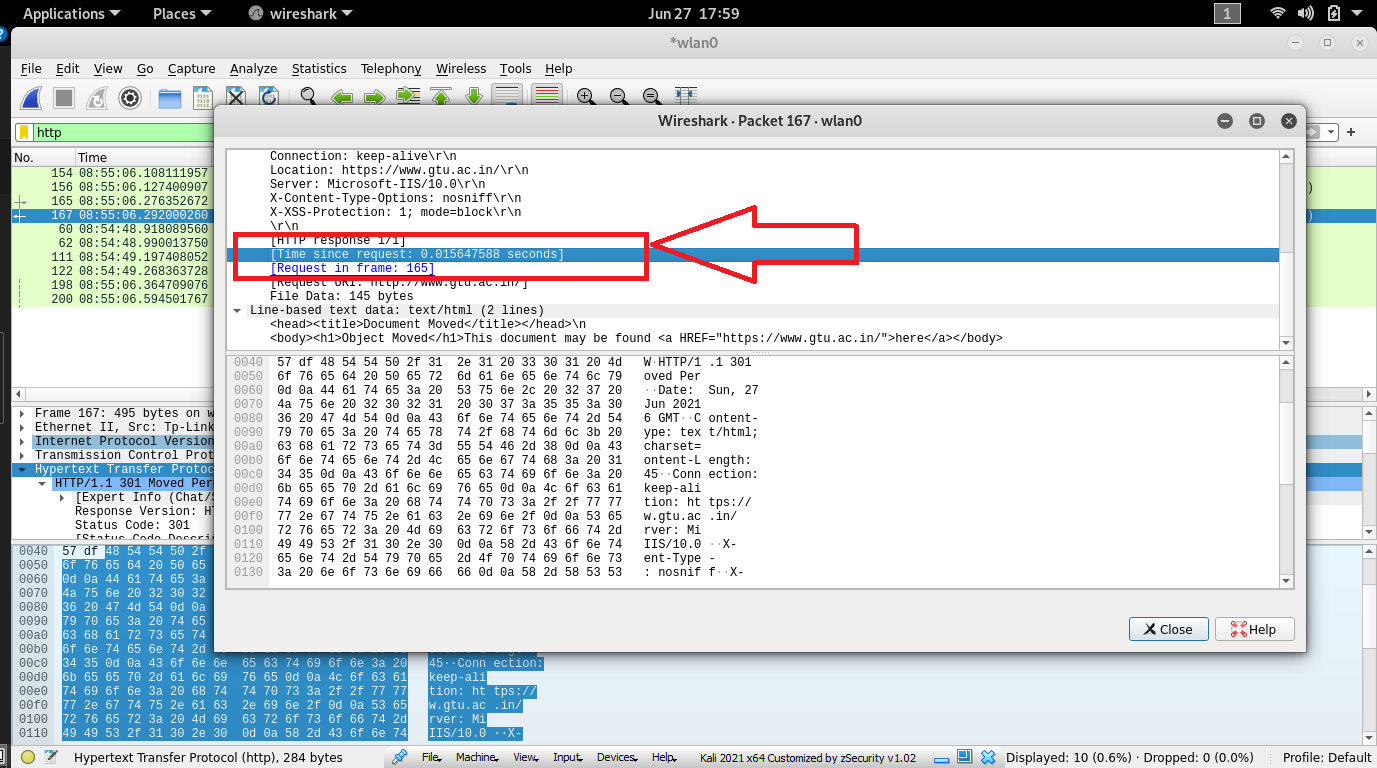
Then after choose Time of Day Option



Now Double click on Highlighted line



Might your Interface look like this one

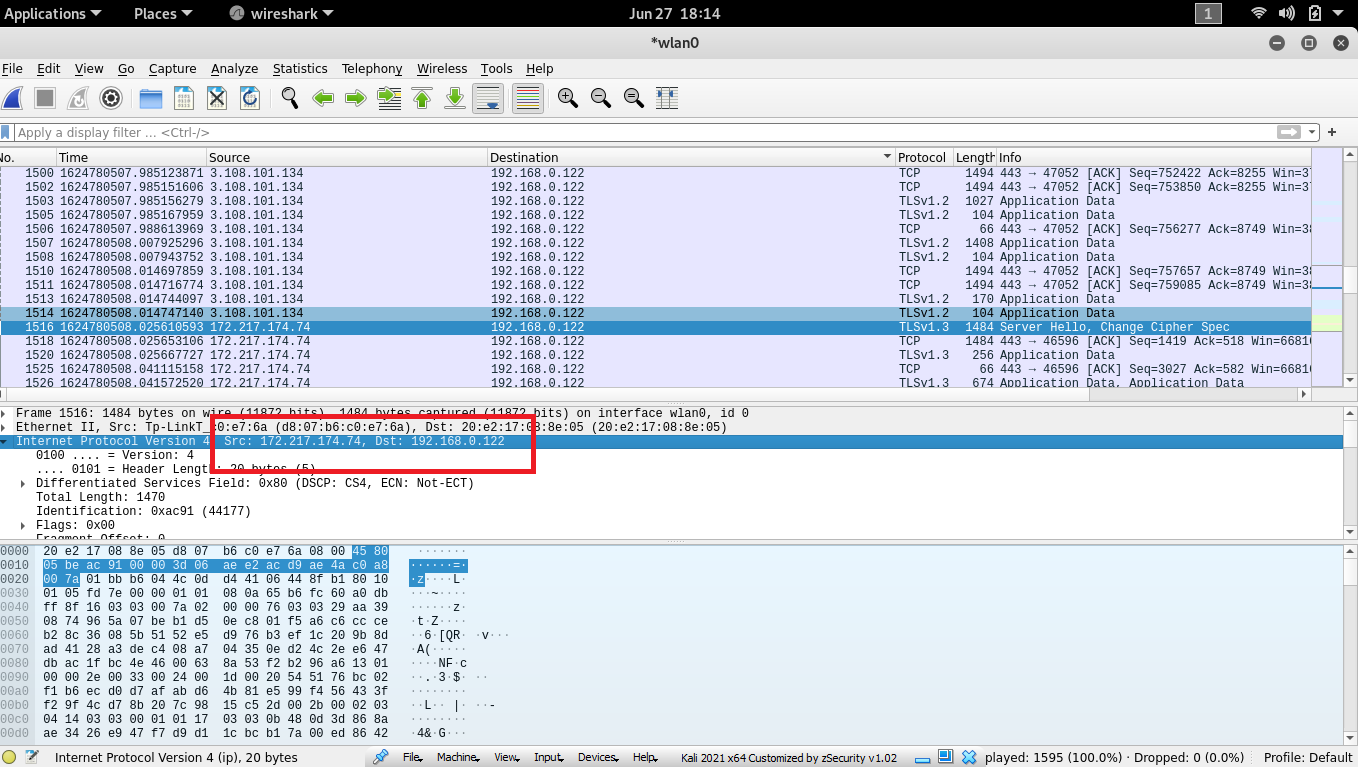


Find This line You will get your answer

**3. What is the Internet address of the www.google.com? What is the Internet address**

**of your computer? Include a screenshot and describe where you got the data to answer**

**this question.**

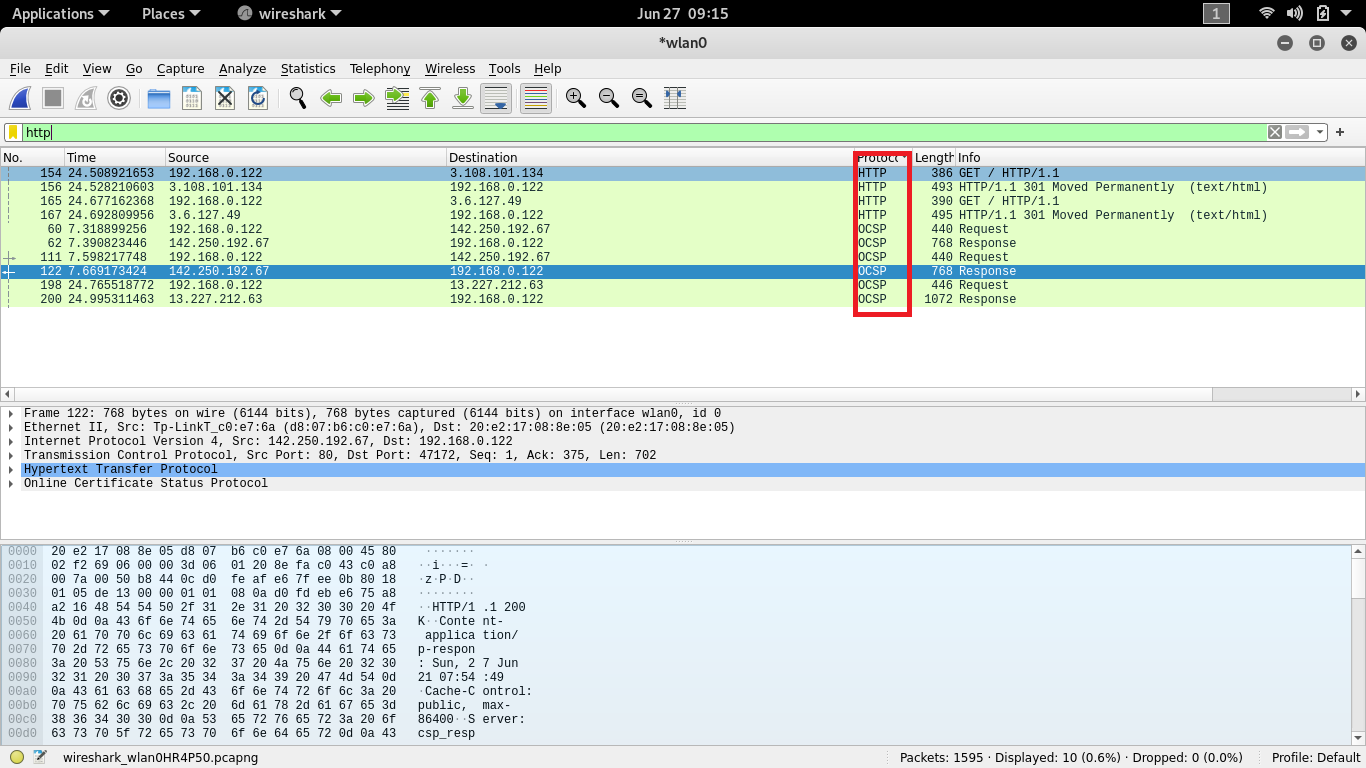


[www.google.com](http://www.google.com) 🡪 172.217.174.74

MY IP 🡪 192.168.0.122

**4. Provide a screenshot showing http protocol only with Wireshark running on your**

**computer.**

****

**5. How many packets did you capture (total of all protocols, not just HTTP)? Now,**

**use display filters to determine how many packets contain your ip address (hint: Use**

**ip.addr instead of the clumsy ip.src or ip.dst format). What is this filter you used? Now,**

**reverse the filter to determine how many packets don’t contain your ip address. See any**

**problems here? If not, you've already figured out the point of this question, so explain how**

**you did so. If so, how can this problem be fixed? What are the appropriate display filters**

**to use? How does Wireshark warn you of such a problem?**

**ANS 🡪**

**6. Use your newly acquired Wireshark skills to capture the process when your**

**browser loads the front page of INI's website (i.e. http://www.ini.cmu.edu). How many**

**packets did you capture? Were all of them HTTP? How many HTTP requests did you**

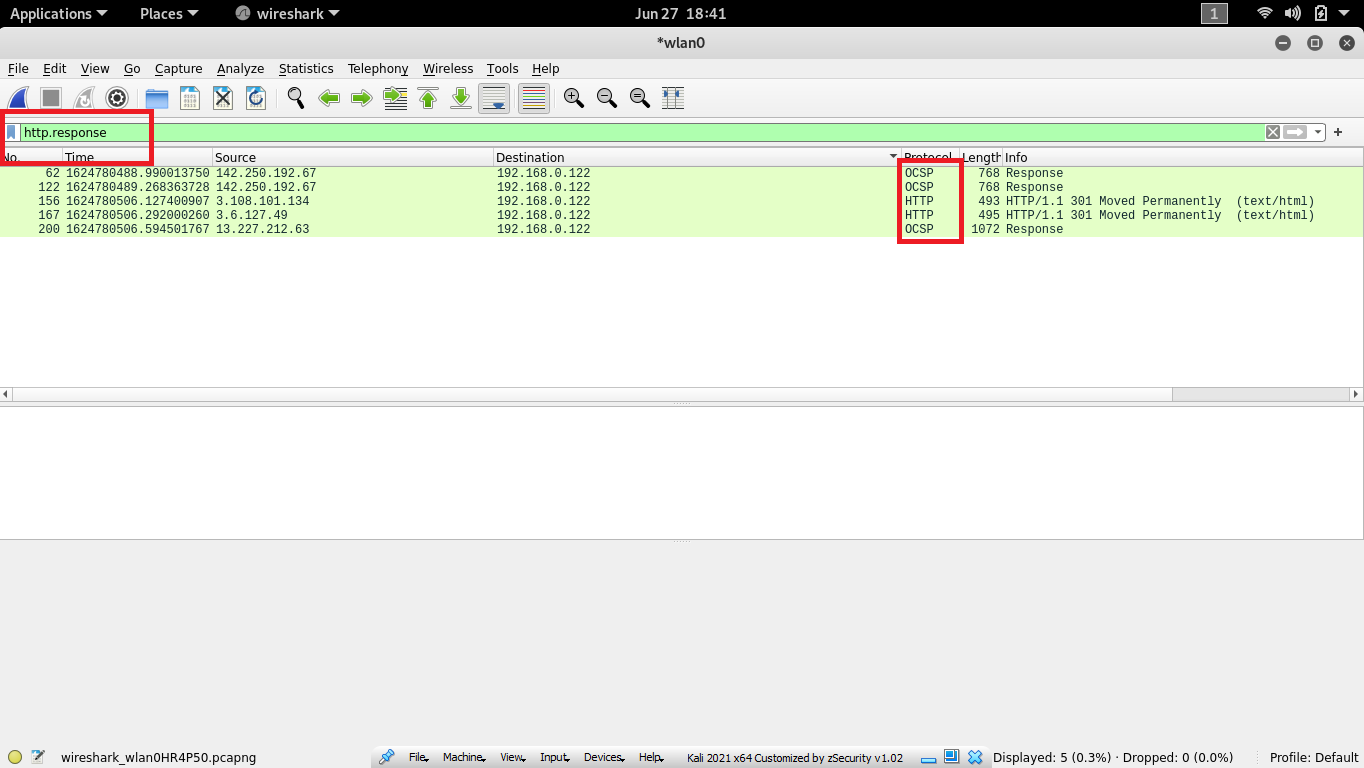
**make? Were all the replies "200 OK"? Did you find anything else interesting? Please**

**ensure you have examined this packet capture in detail, using appropriate Wireshark**

**functionality. Please include screen captures where you think they are necessary.**

Package Captured🡪****

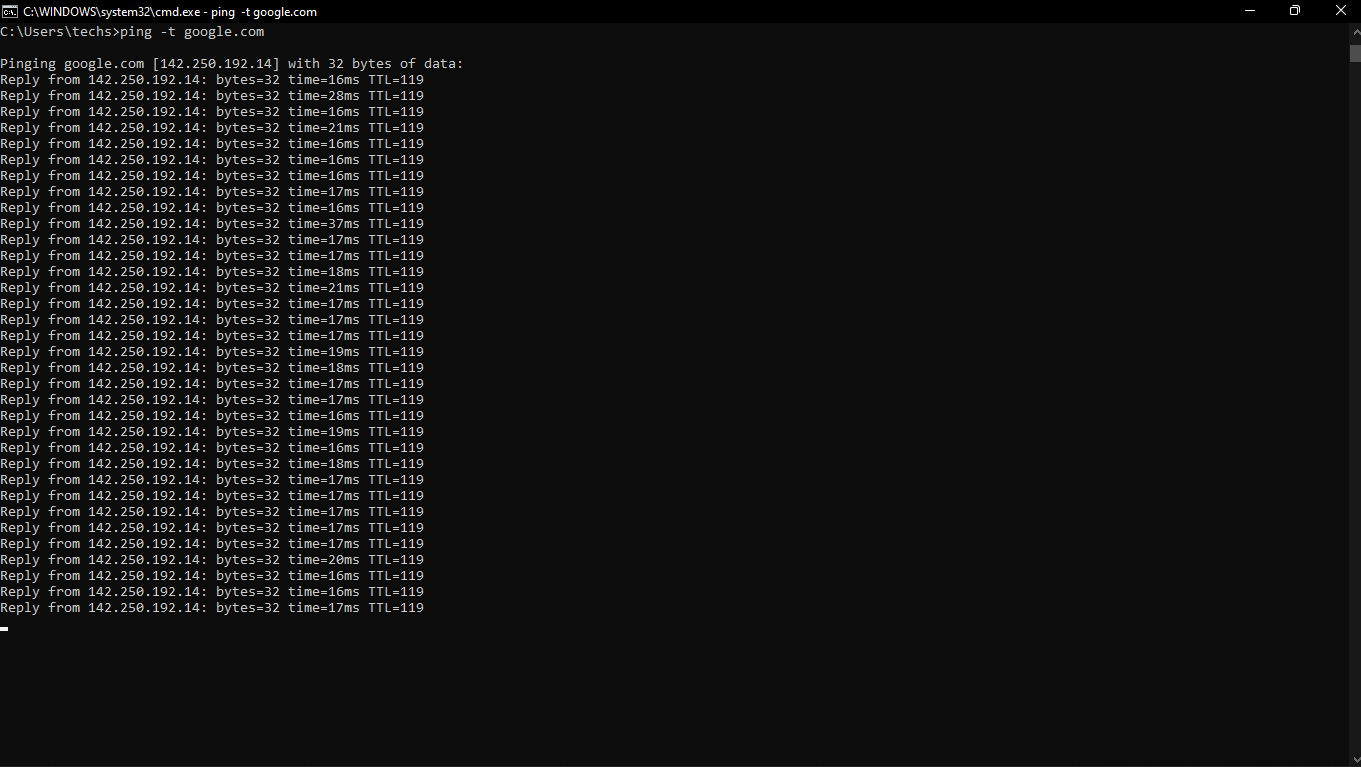
* No, All Packages were not http.
* 10 http request Were made

****

**USE ipconfig/all**

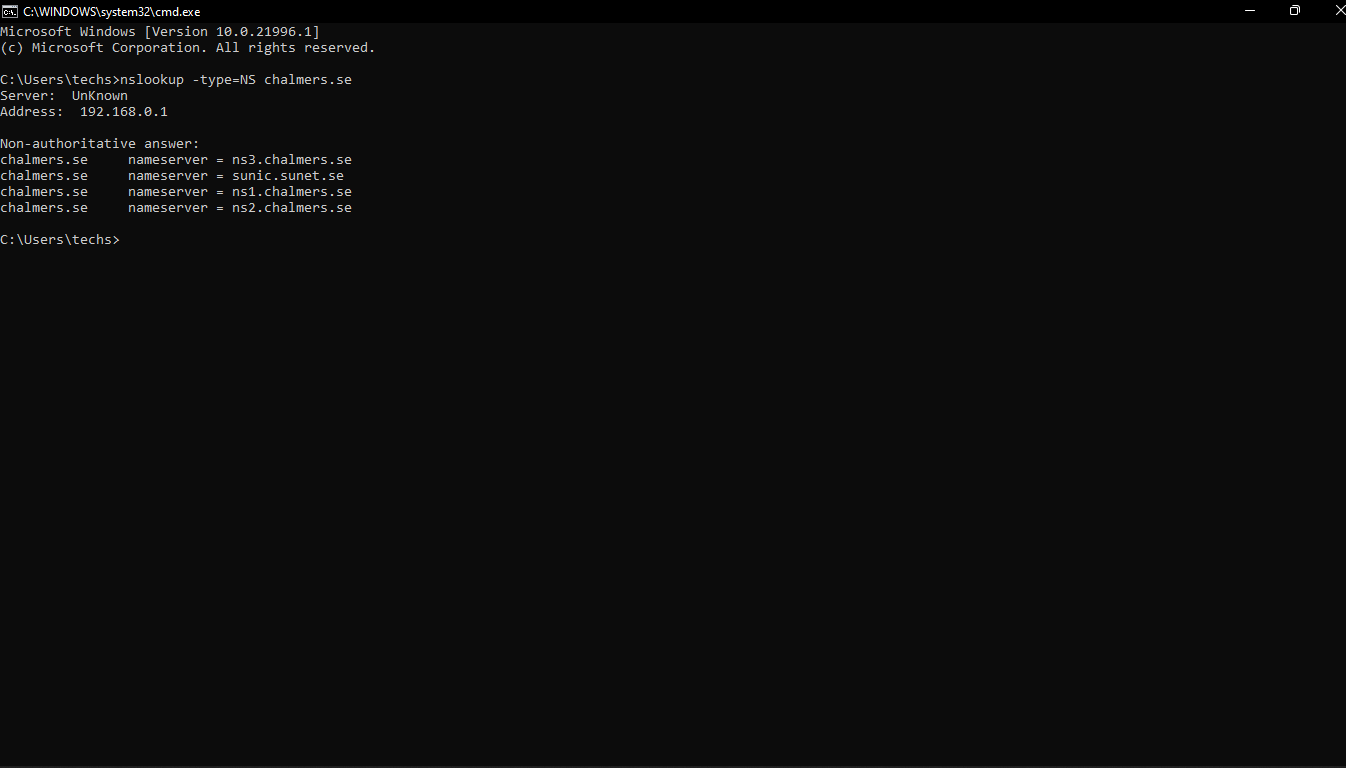


**Use ping –t google.com to get IP address**

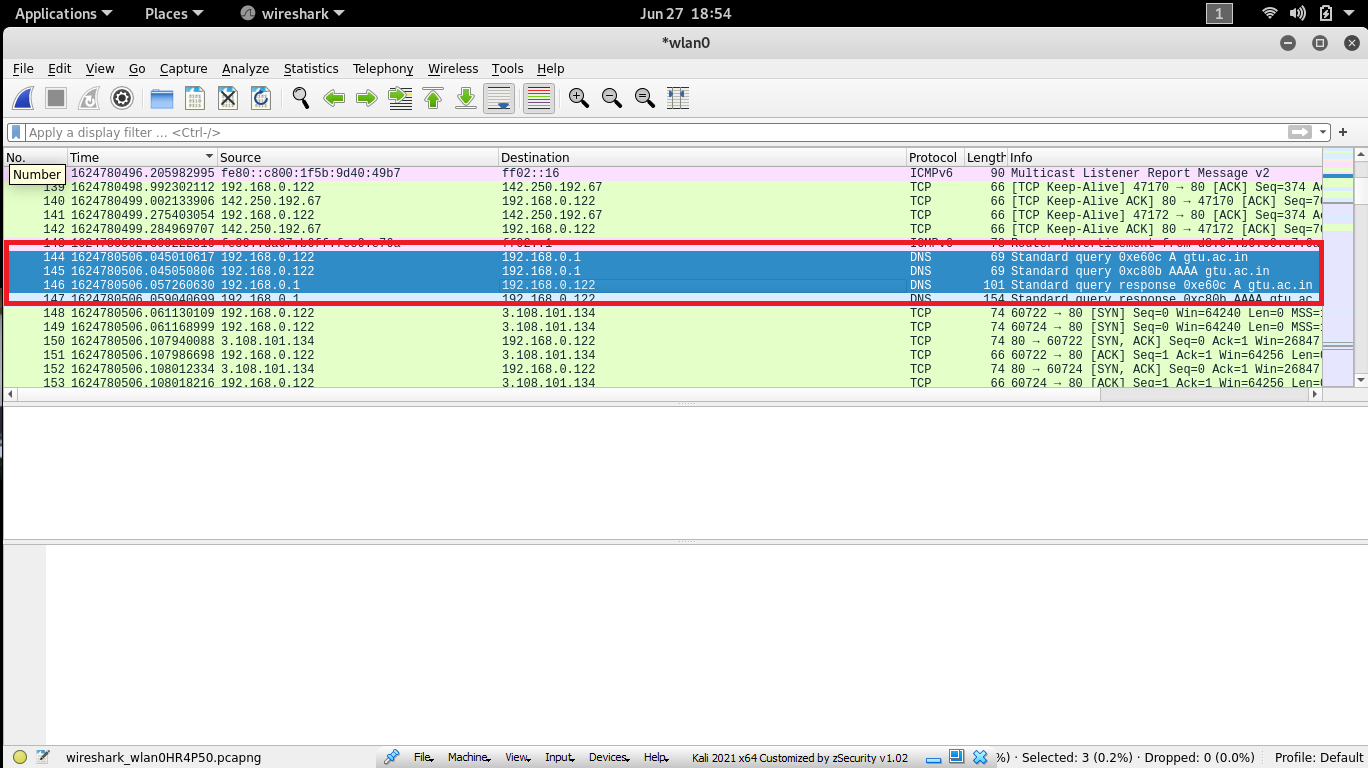
****

**Use nslookup www.google.com**

**nslookup –type=NS chalmers.se**

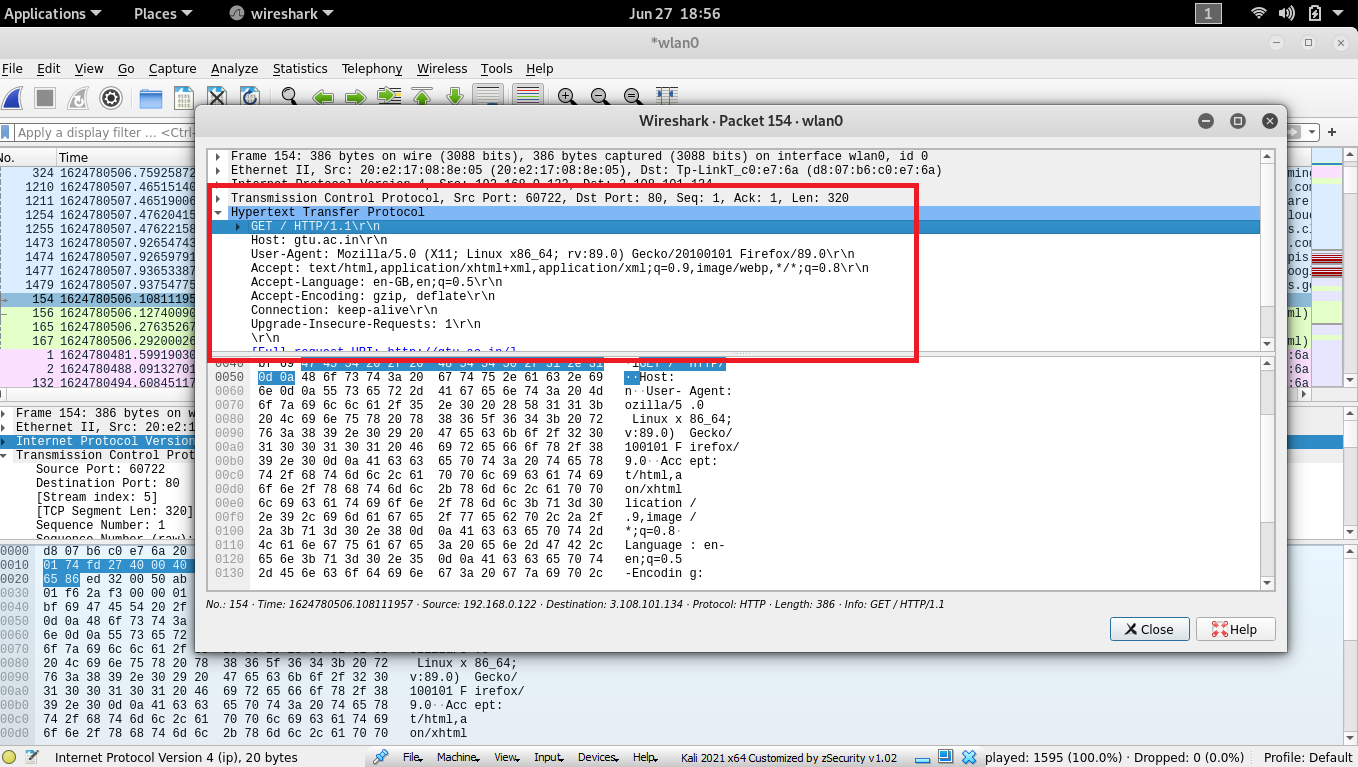
****

**7. What is the IP address of your computer? Of the gtu.ac.in server?**

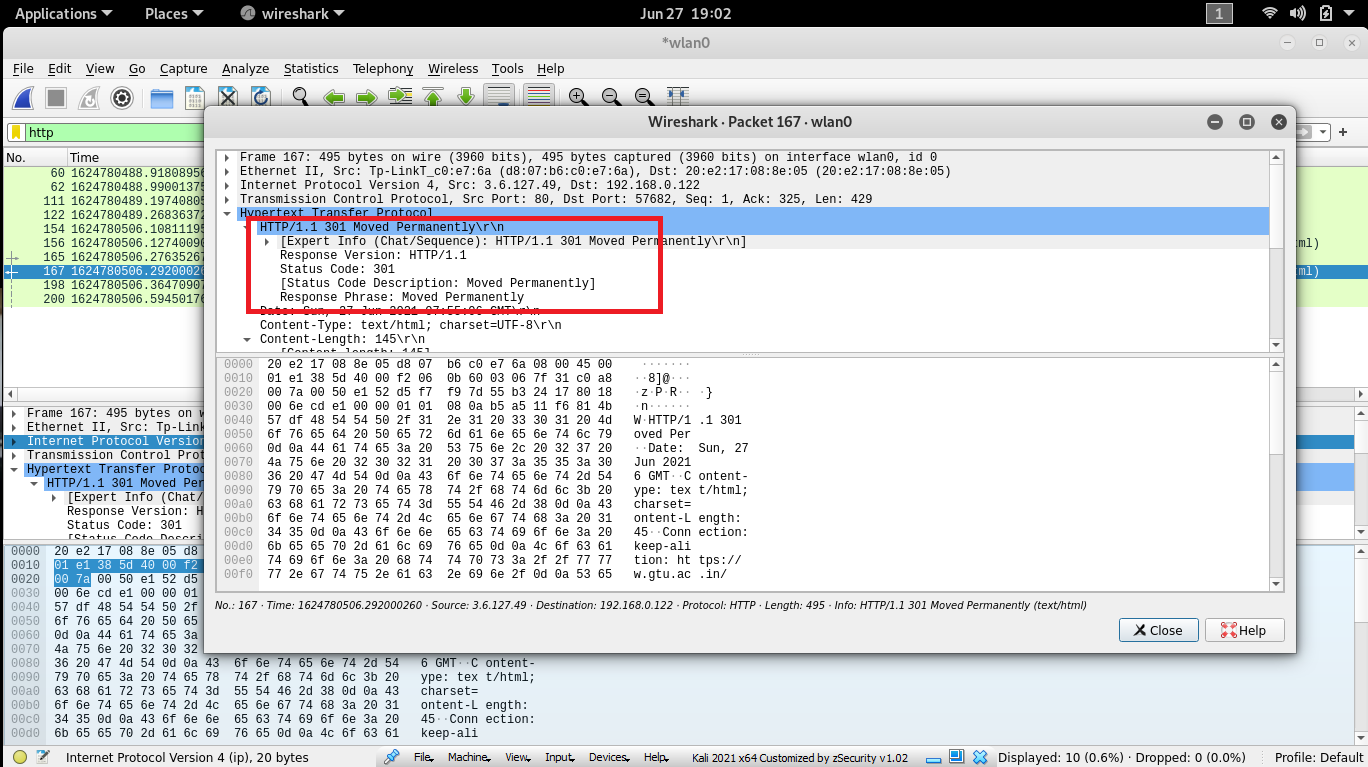
****

**8. What HTTP version is your browser running? What version of HTTP is the server**

**running?**

****

**9. What is the status code and phrase returned from the server to your browser?**

****

**10. What languages does your browser indicate to the server that it can accept? Which**

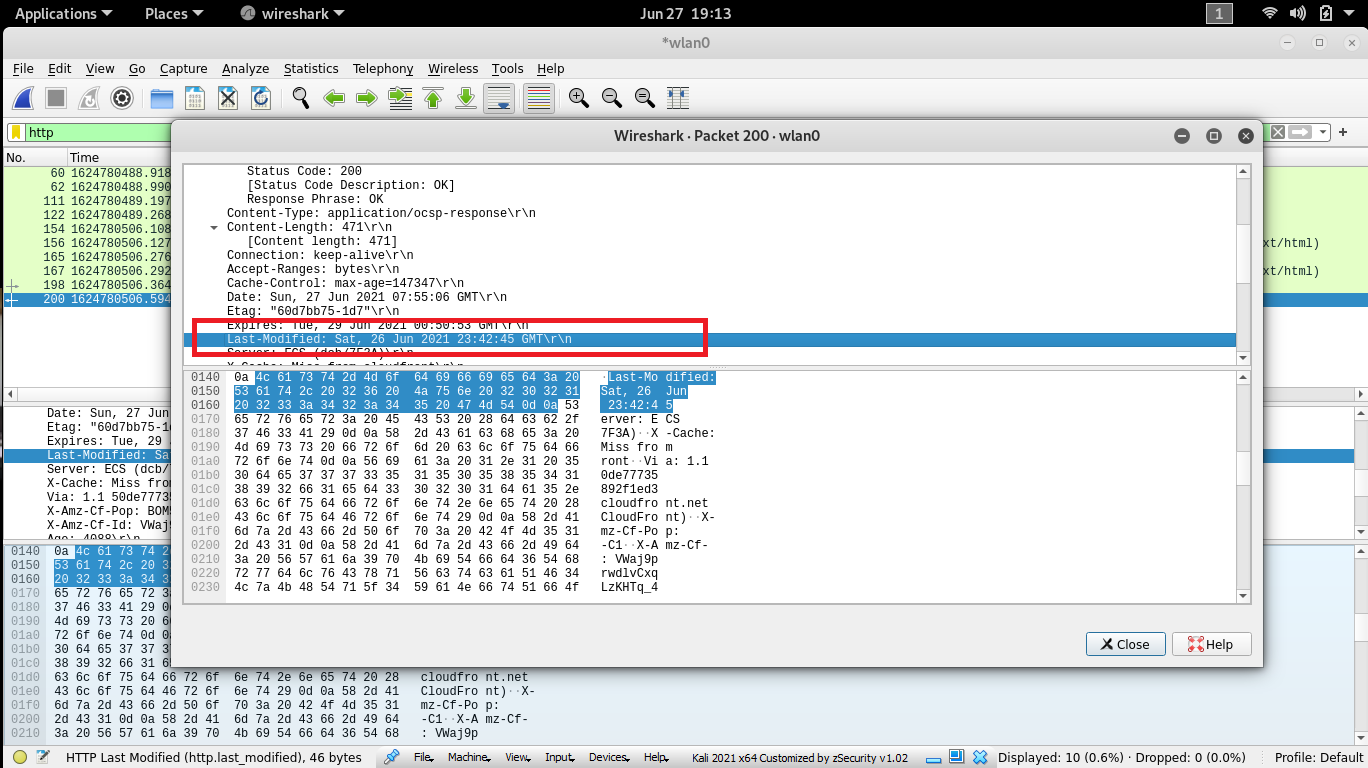
**header line is used to indicate this information?**

****

According t the picture above, en=GB ot en means United Kingdom English

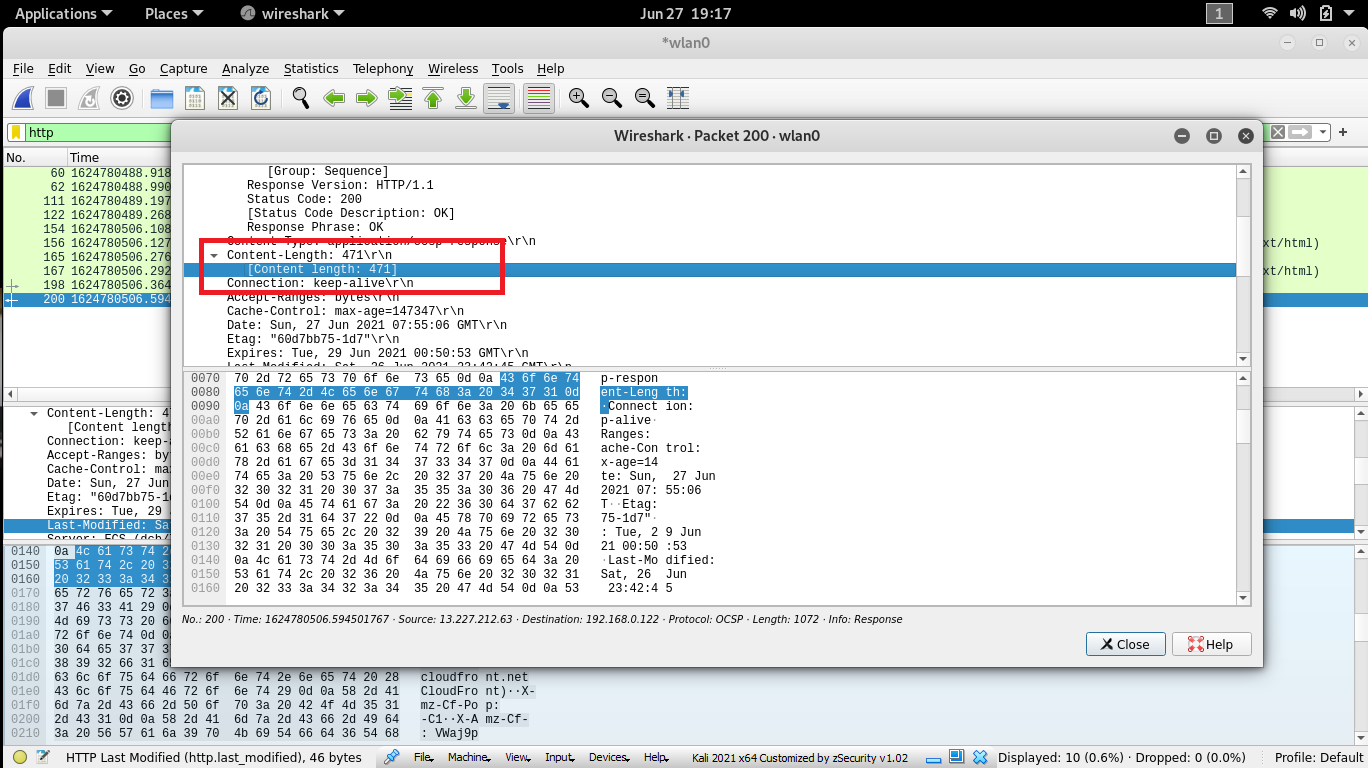
**11. When was the HTML-file, that you have retrieved, last modified at the server? Which**

**header line is used to indicate this information?**

****

**12. How many bytes of content (size of file) are returned to your browser? Which header**

**line is used to indicate this information?**

****

**HTTP Conditional GET/Response Interaction**

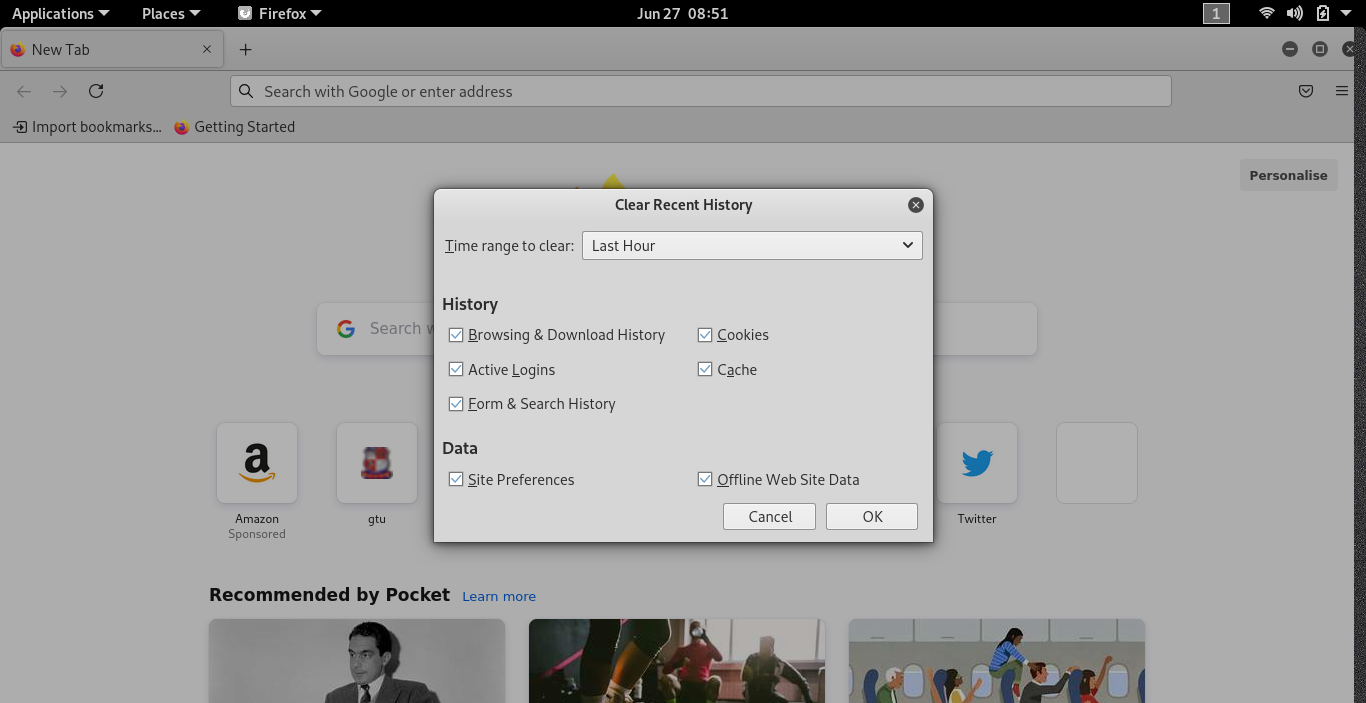
**13. We know that most web browsers perform object caching and thus perform the**

**conditional GET when retrieving HTTP objects. Before performing the steps below, make**

**sure that your browser’s cache is empty.**

**14. Start up your web browser, and make sure your browser’s cache is cleared.**

**Ans 🡪** as I told before press CTRL + SHIFT + DLT



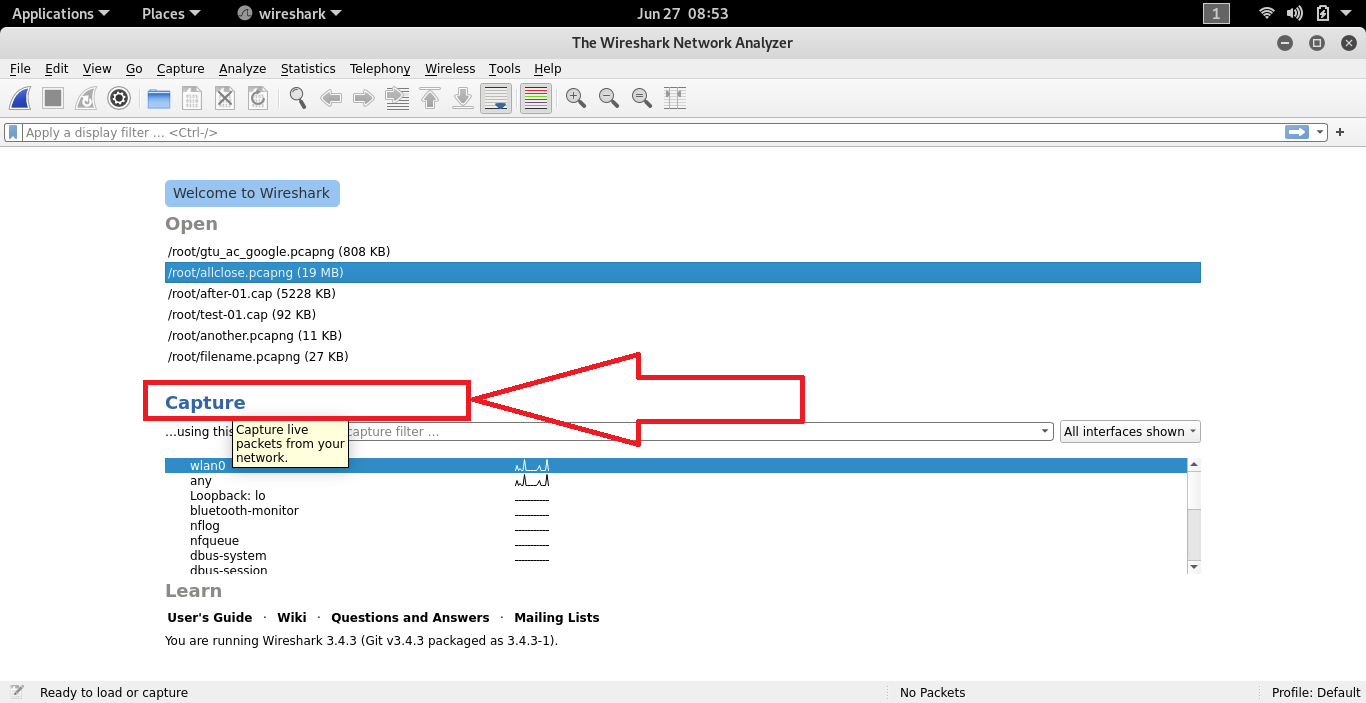
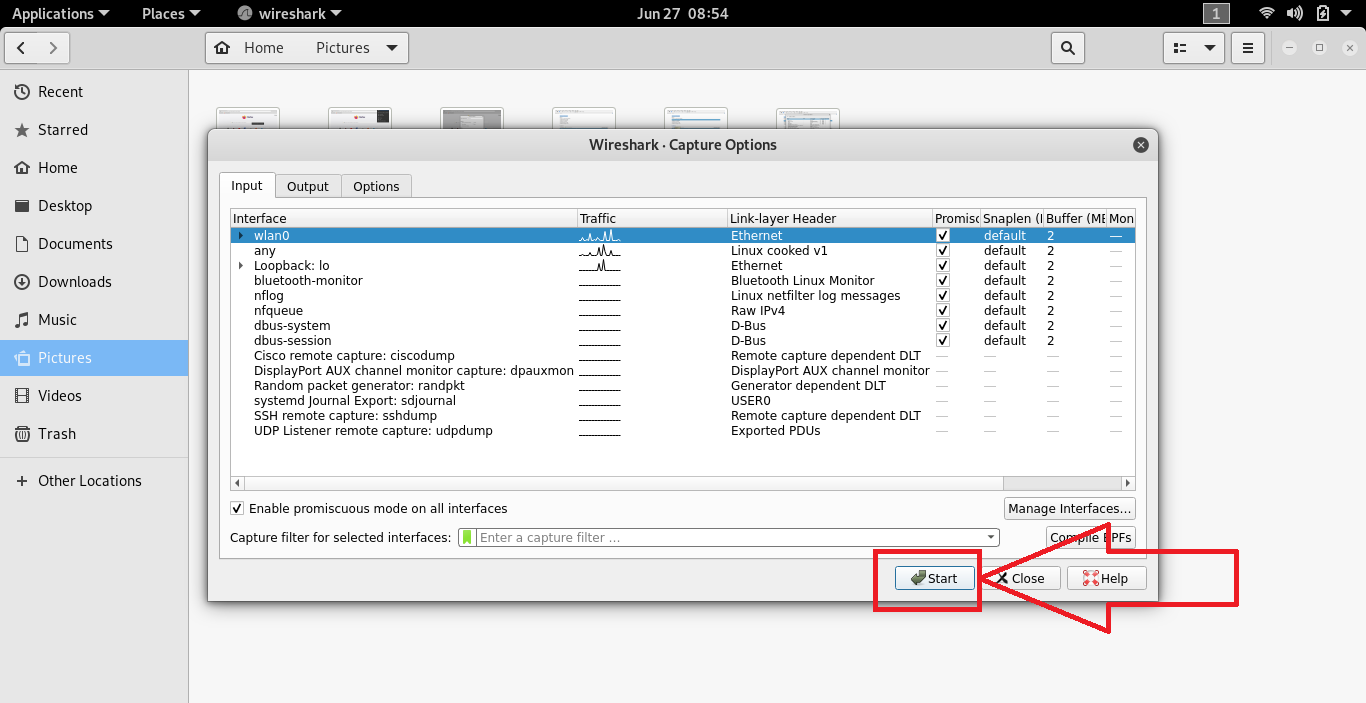
**15. Start up the Wireshark packet sniffer, and make sure that “http” is in the displayfilter,**

**so that only captured HTTP messages will be displayed in the packet-list pane.**

**16. Enter the following URL into your browser:**

[**http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html**](http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html)

**ans🡪 follow below steps**

1. Clear catch and cookie as per above image
2. 
3. 
4. 

Enter the [**http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html**](http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html) **inside browser and after 2 second press F5 simply refresh the page**

1. 
2. Stop the packet capture in wireshark

**Answer the following questions. Please explain how you can find the answers.**

**19. Inspect the contents of the first HTTP GET request from your browser to the server.**

**Is there an “IF-MODIFIED-SINCE” header line in the HTTP GET message? Why or why**

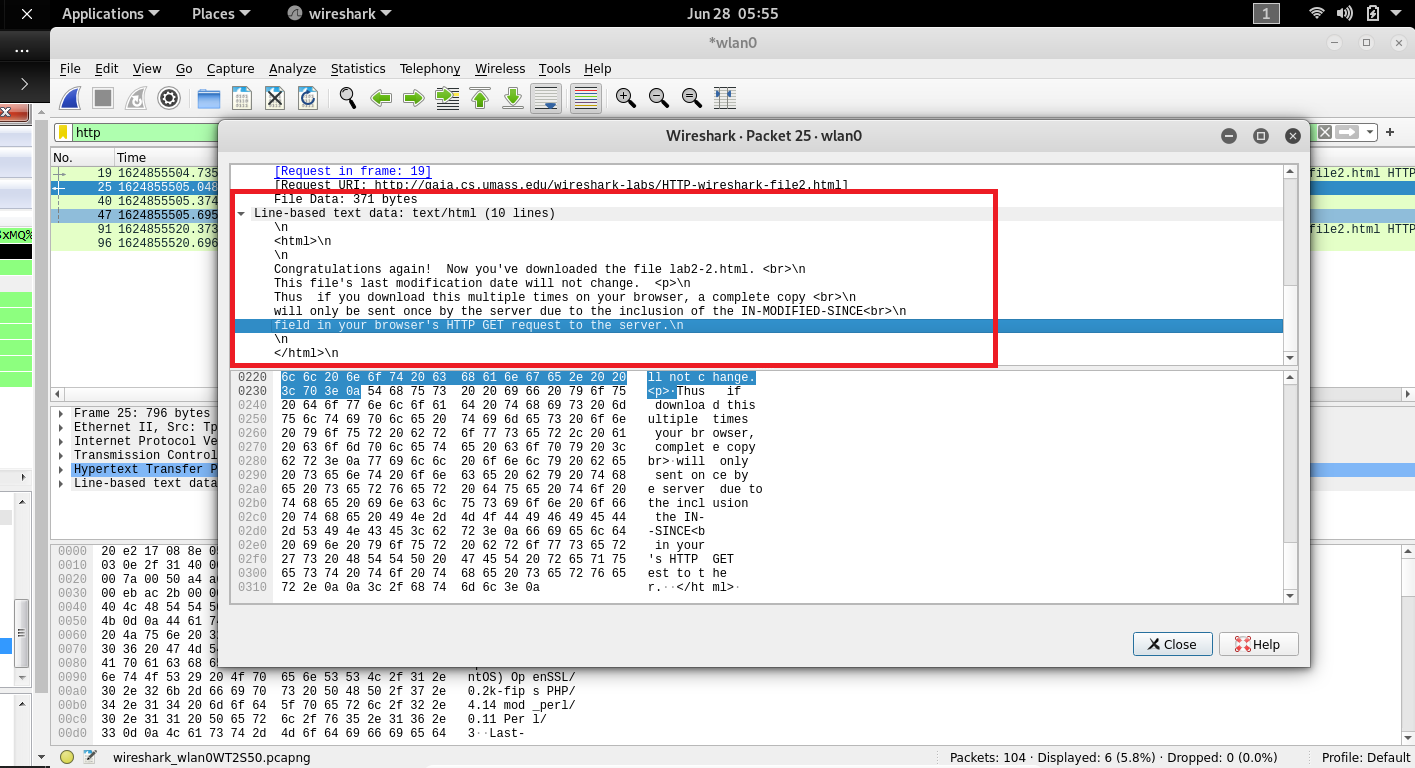
**not?**

Ans 🡪 No there is no IF-MODIFIED-SINCE line in the GET message.

**20. Inspect the contents of the server response. Has the server explicitly returned the**

**contents of the file? How can you tell?**

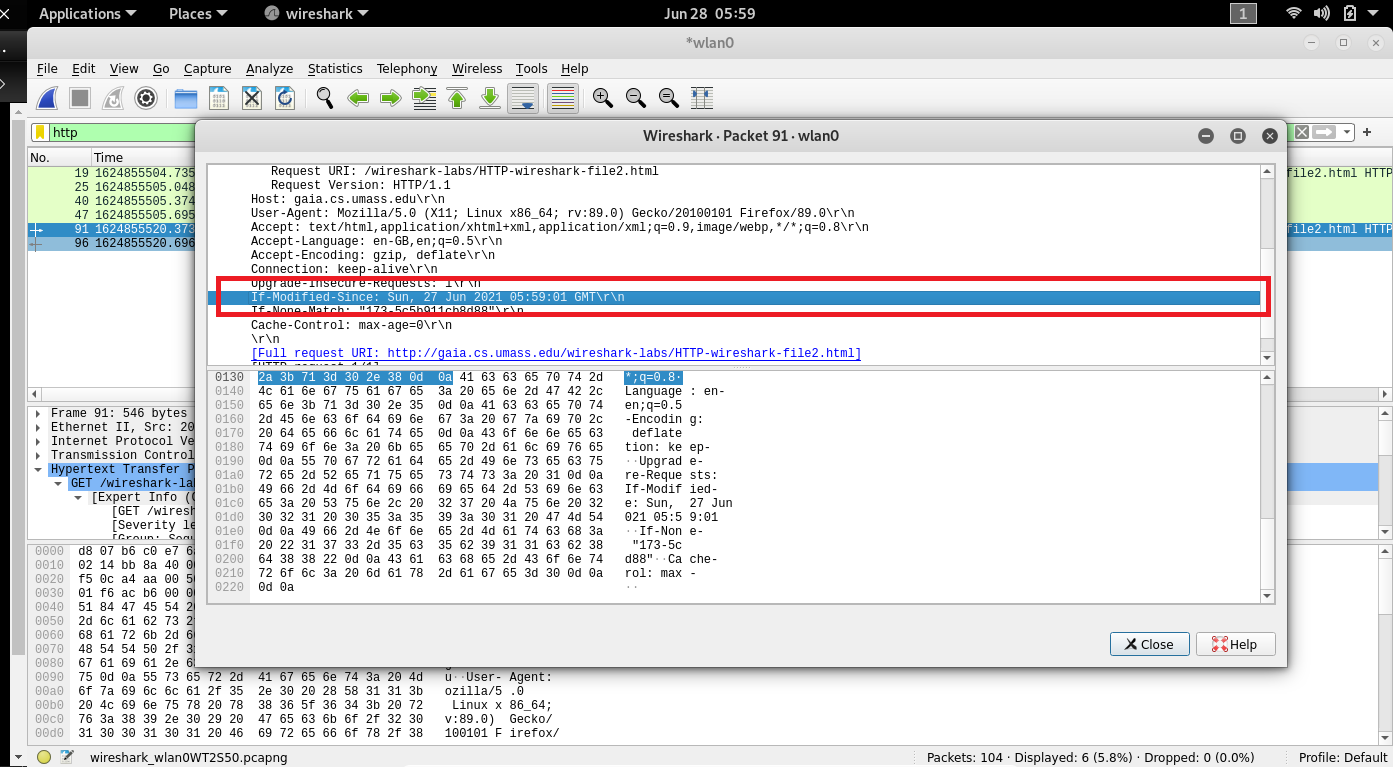
**ANS 🡪** The server did explicitly return the contents of the file. Wireshark includes a section titled “Line-Based Text Data” which shows what the server sent back to my browser which is specifically what the website showed when I brought it up on my browser.

****

**21. Now inspect the contents of the second HTTP GET request from your browser to the**

**server. Is there an “IF-MODIFIED-SINCE:” header line in the HTTP GET message? If so,**

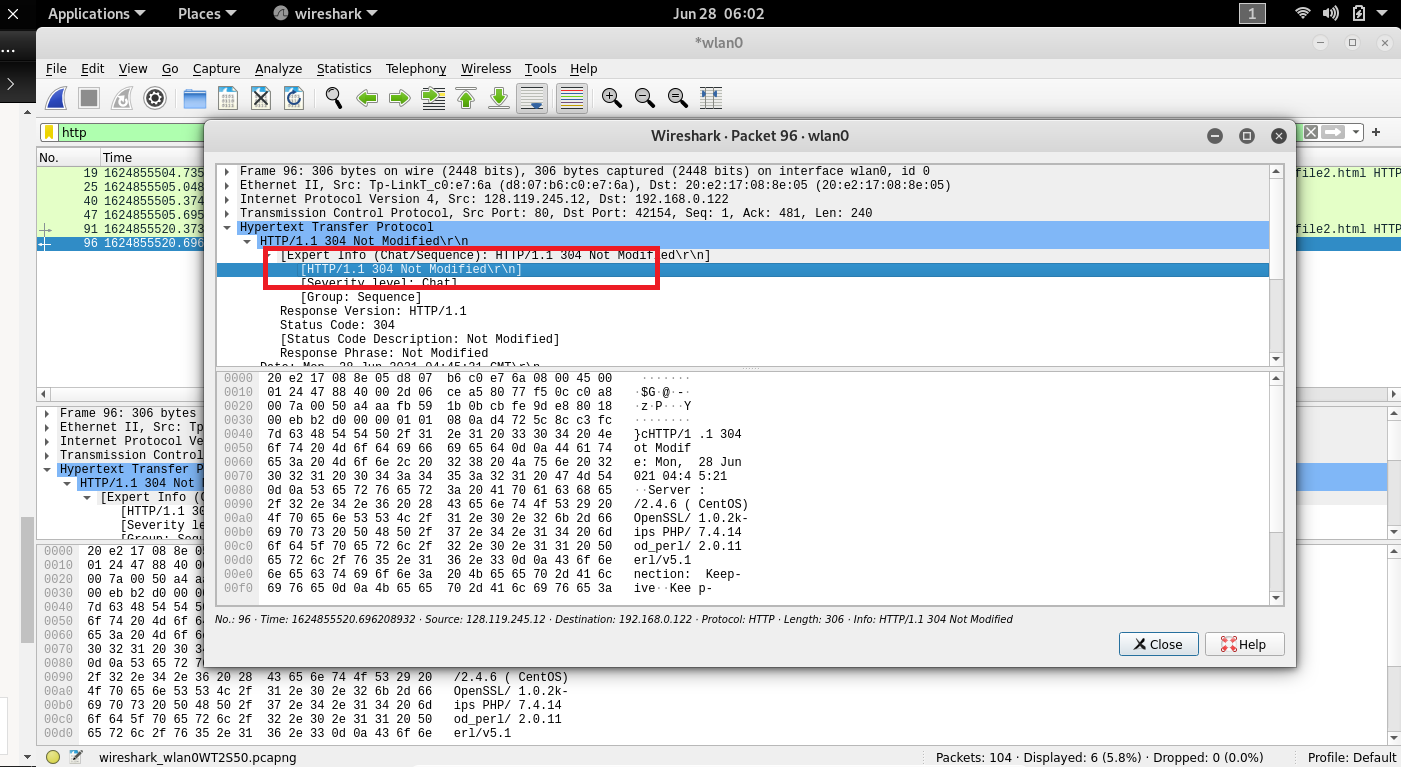
**what information follows the “IF-MODIFIED-SINCE:” header line?**

Ans 🡪 Yes in the second HTTP message an IF-MODIFIED-SINCE line is included. The information that follows is the date and time that I last accessed the webpage

**22. What is the HTTP status code and phrase returned from the server in response to**

**this second HTTP GET? Has the server explicitly returned the contents of the file? Explain.**

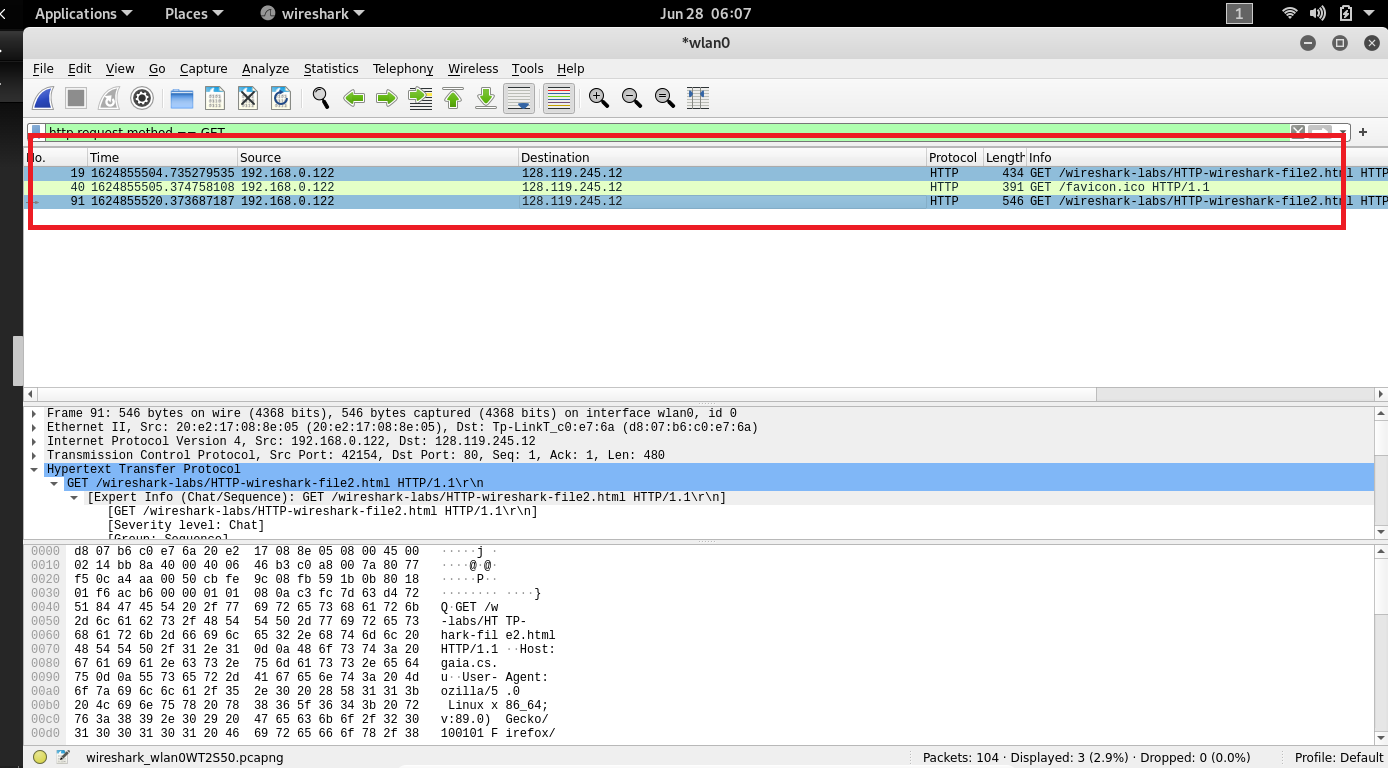
**ANS 🡪** The server did not return the contents of the file because the browser simply retrieved the contents from its cache. Had the file been modified since it was last accessed, it would have returned the contents of the file, instead it simply told my browser to retrieve the old file from its cached memory.

****

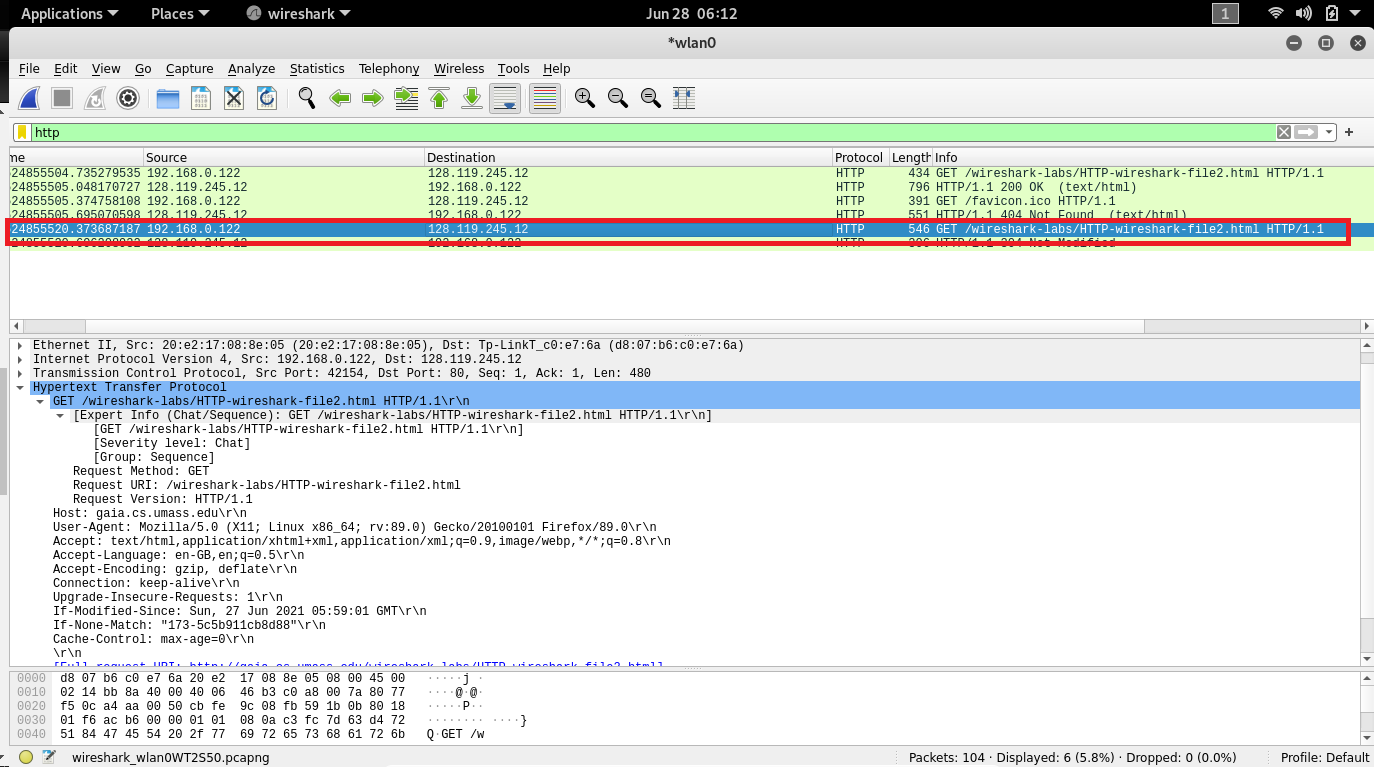
**23. How many HTTP GET request messages has your browser sent? Which packet in**

**the trace contains the request for the Bill of Rights?**

**Ans 🡪** my browser only sent 4 HTTP GET Request to the server.

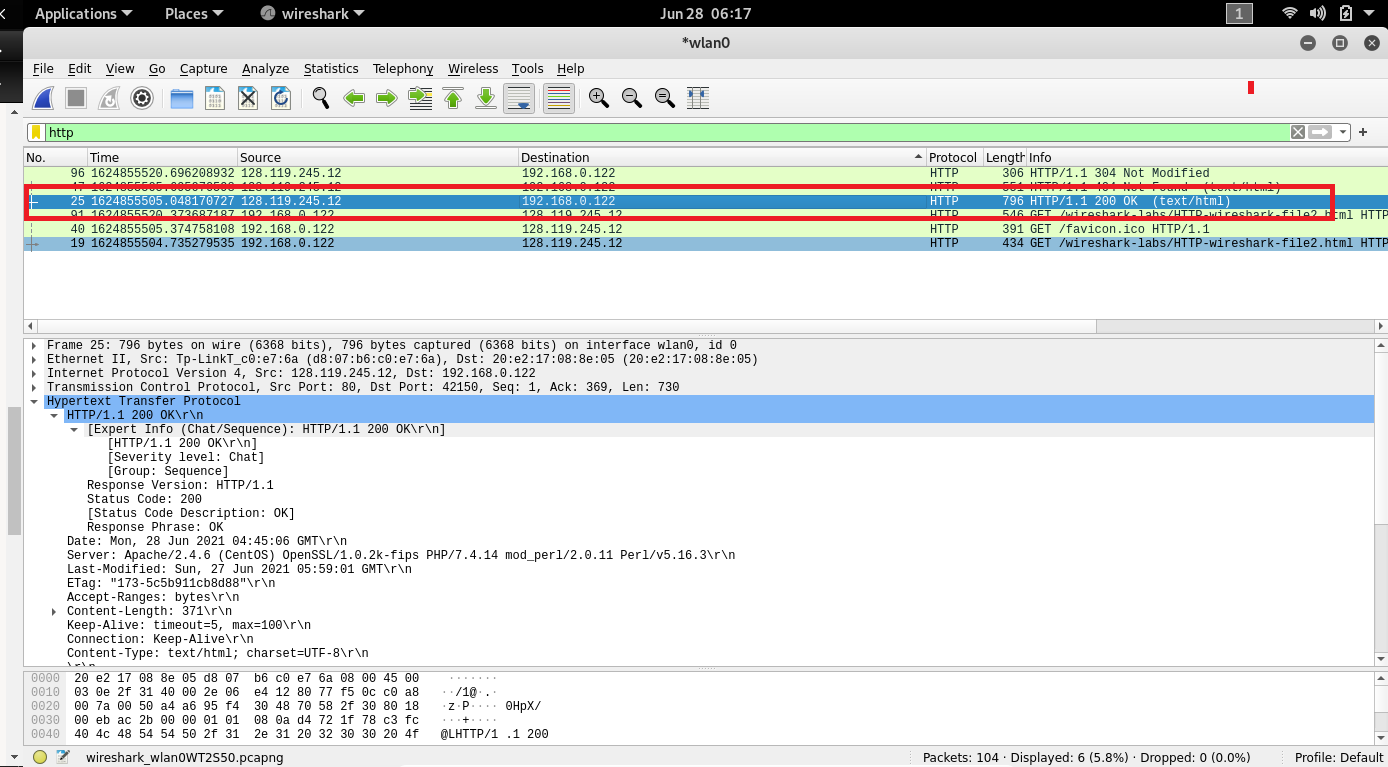
****

* The Packet that contained the GET message was packet number 40.

****

**24. Which packet in the trace contains the status code and phrase associated with the**

**response to the HTTP GET request? What is the status code and phrase in the response?**

**ANS🡪** The packet that contains the status code and phrase which the server sent in response to the GET message was packet number 241.****