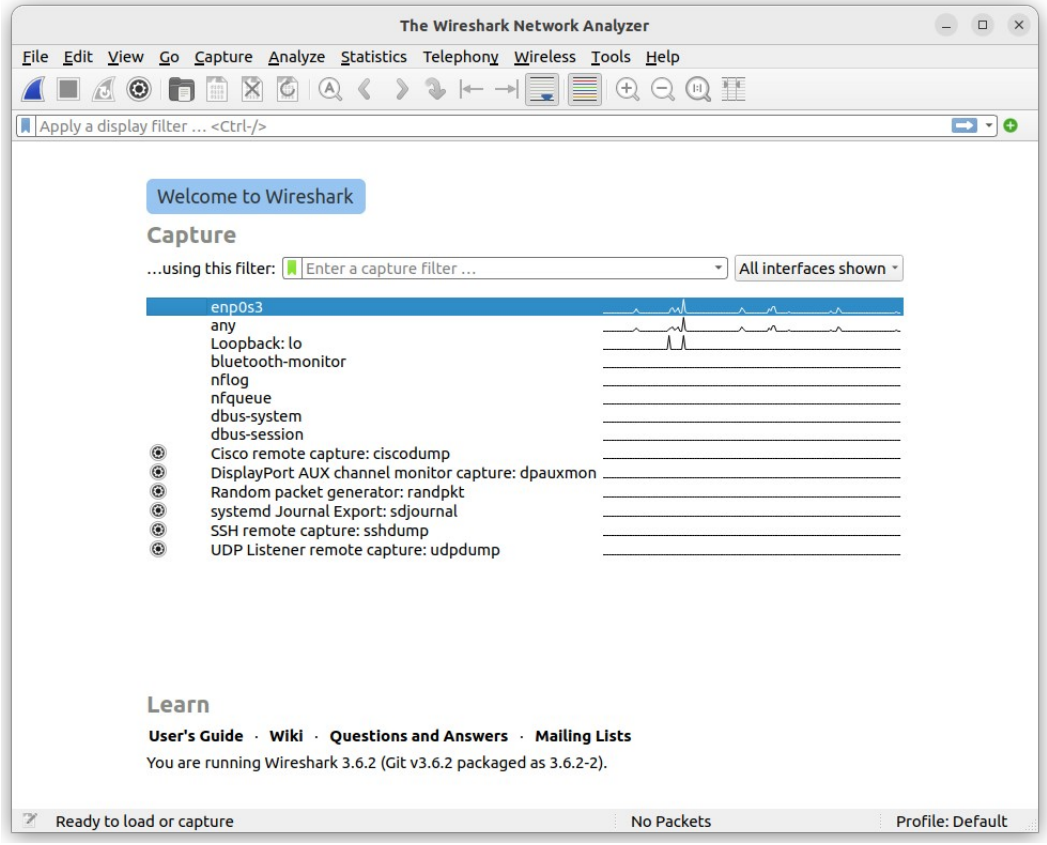
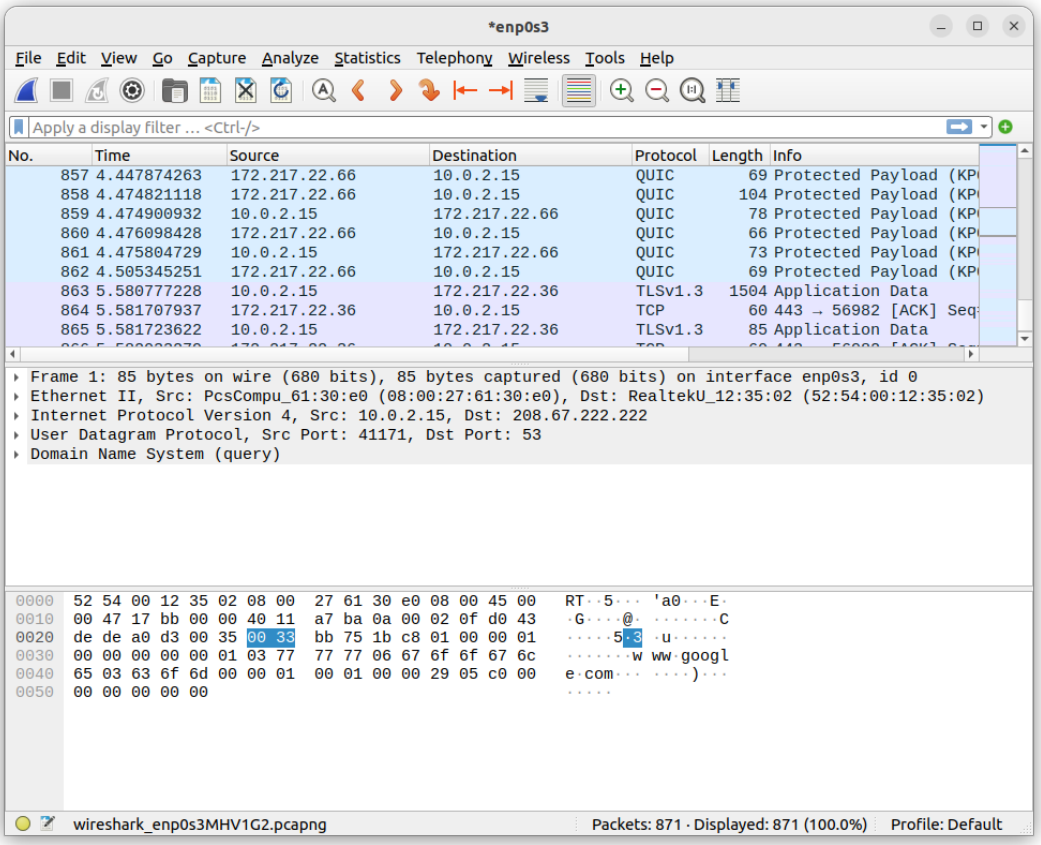
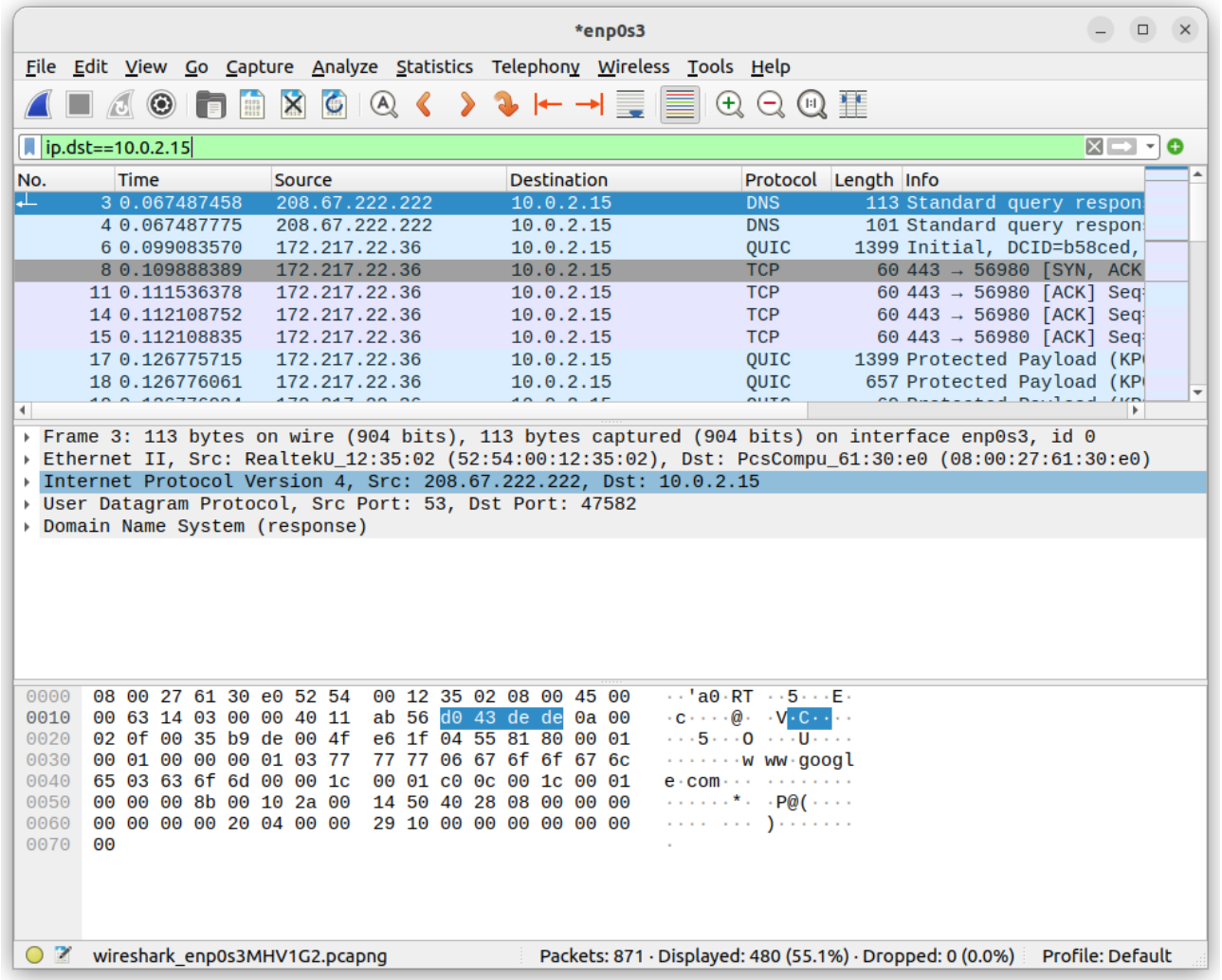


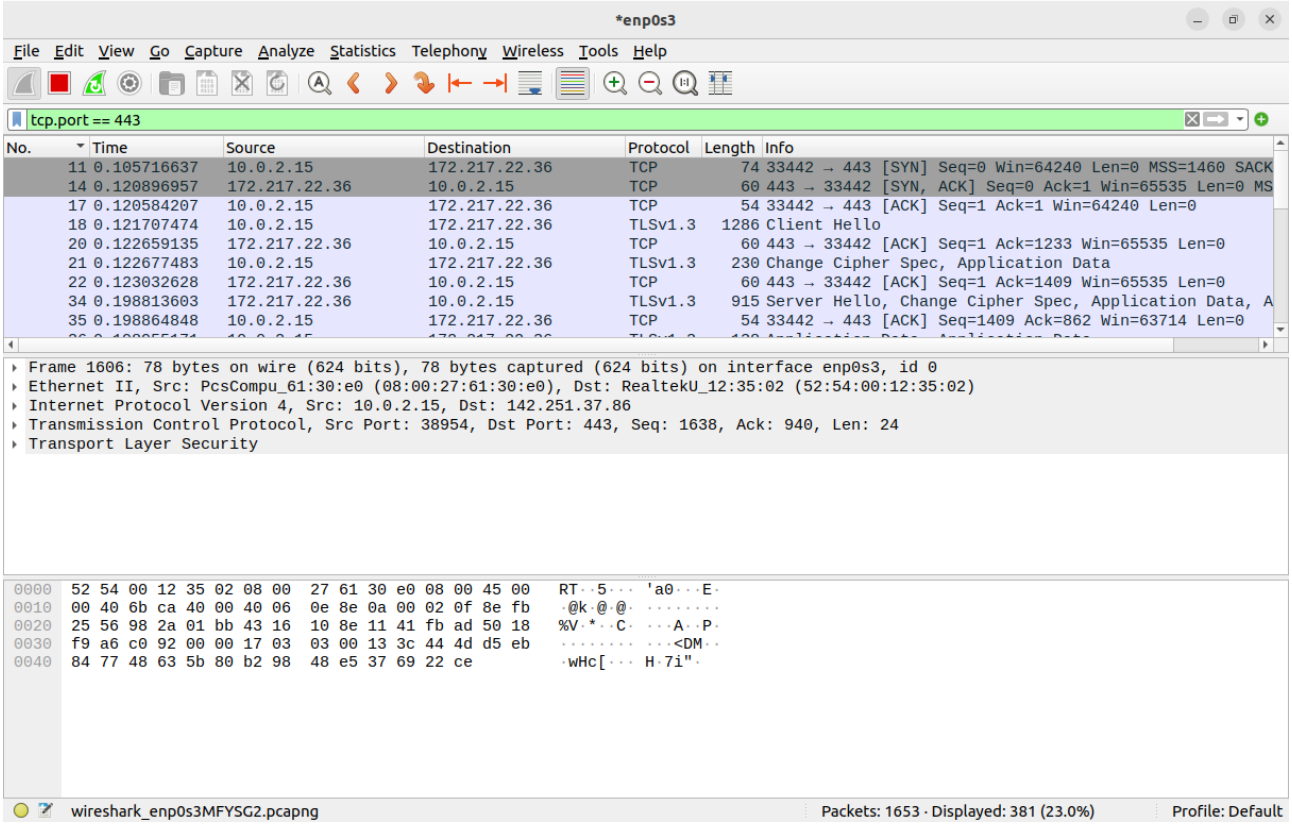
1. First window of Wireshark interent – enp0s3.



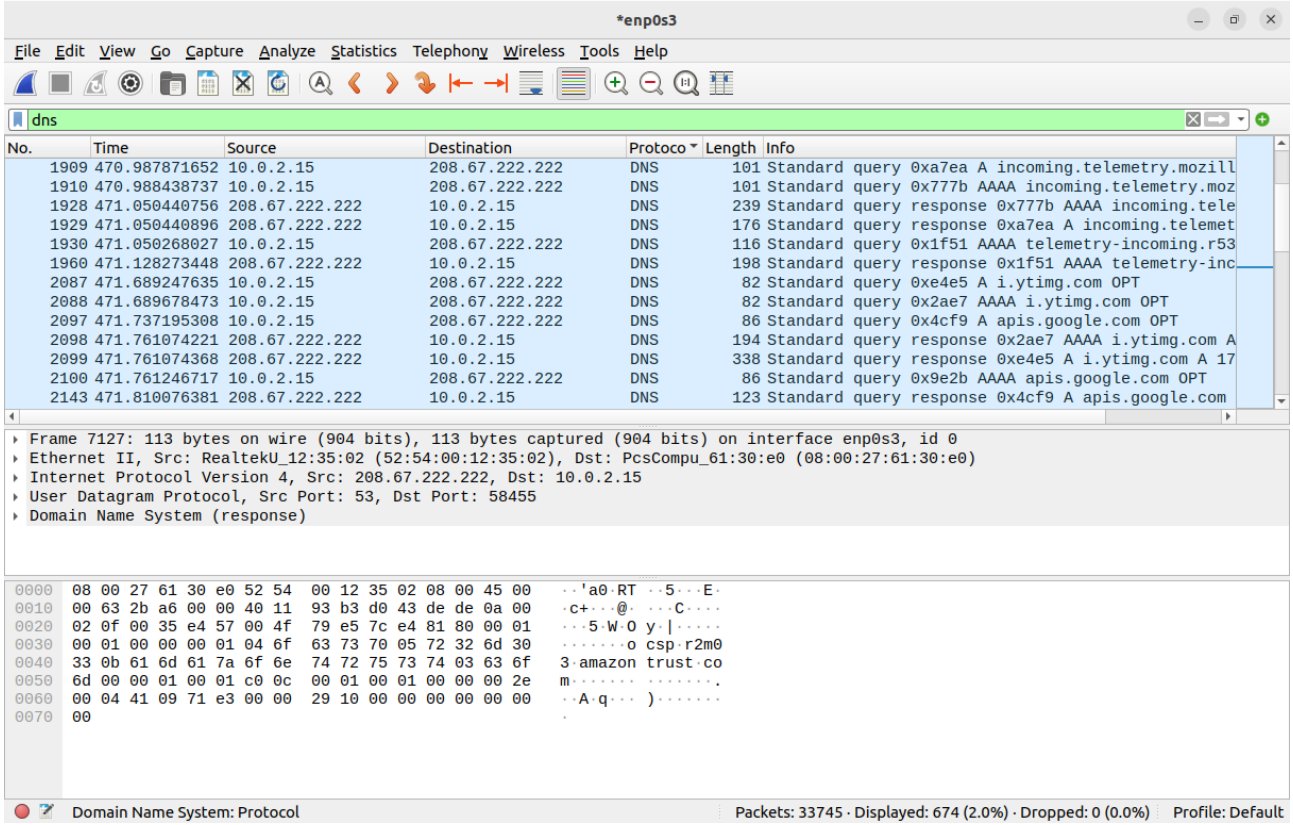
2. Packets catching on.



2.a. sorting results based on chosen ip == 10.0.2.15



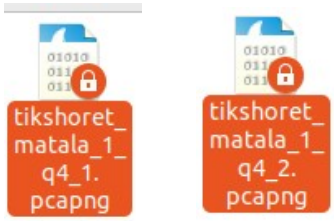
2.b. sorting by source port 443, the protocol that uses it is TCP and TLSv1.3.



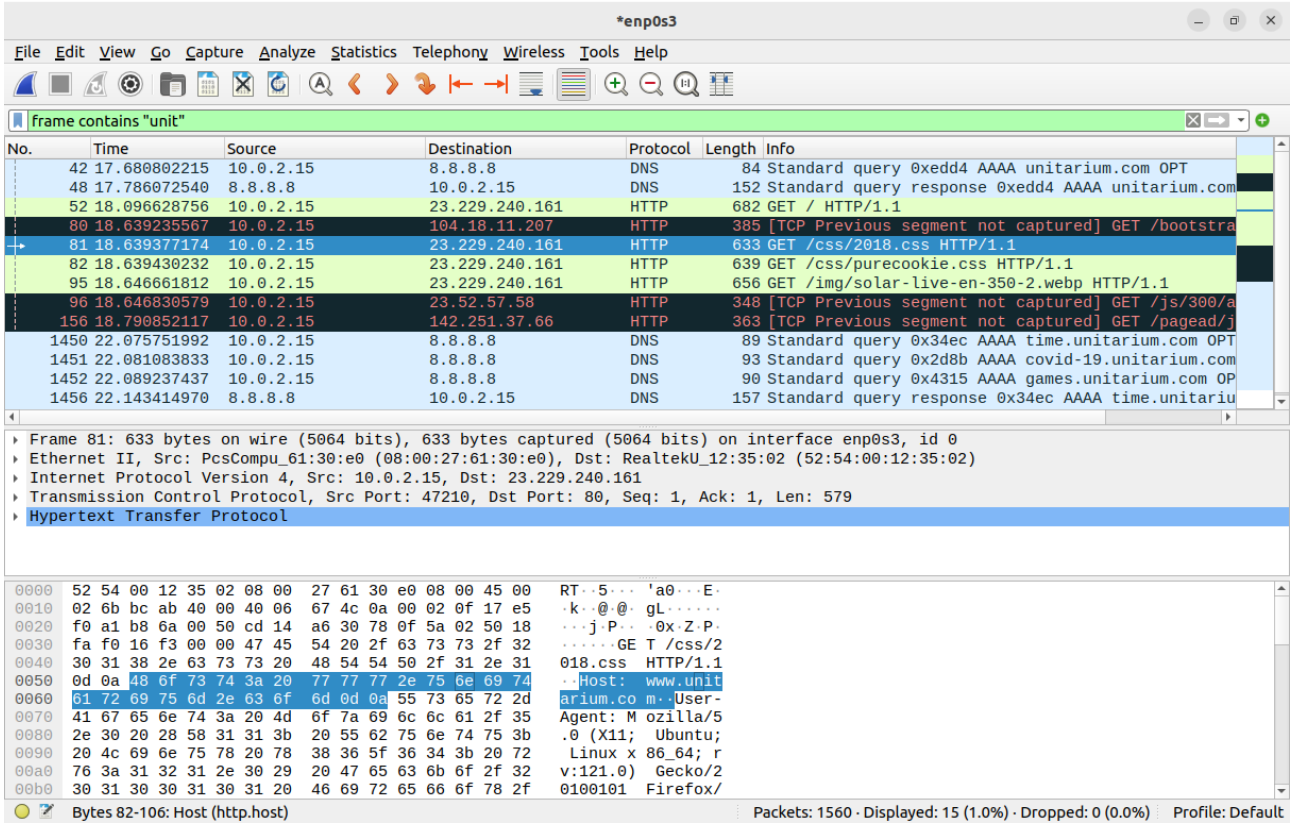
2.c. sorting by a specific protocol – DNS.

3. The caught packet's file from wireshark was saved in "pcapng" format.

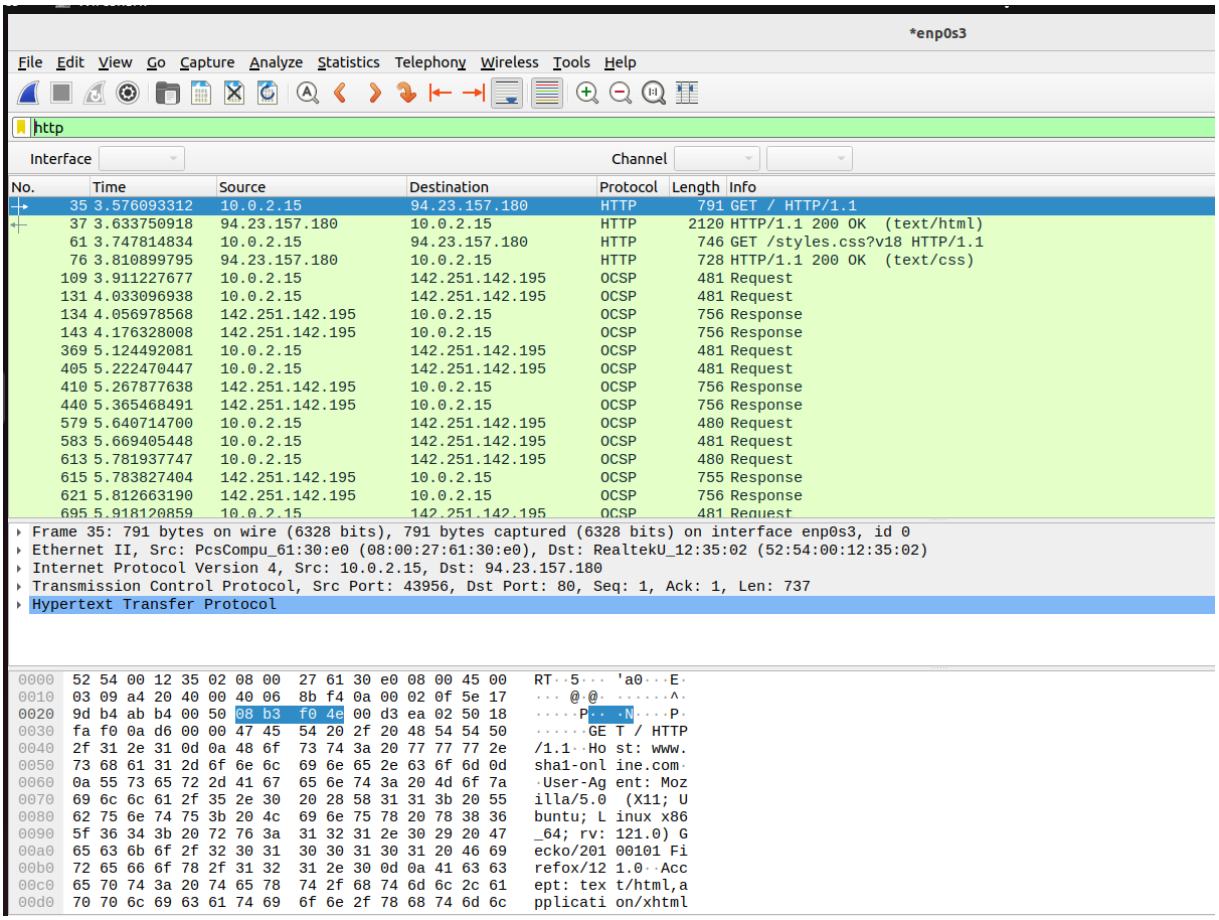
4. Saved two different packets using "pcapng" format.



5. Promiscuous mode is a setting in wireshark that can be turn on, which will make the network card catch, duplicate and save any frames that are transmitted through it, not only the ones that are destinated for it.



6. Filtering by " frame contains ‘unit’ " leaves only cought packets containing the sequence "unit" in their information.



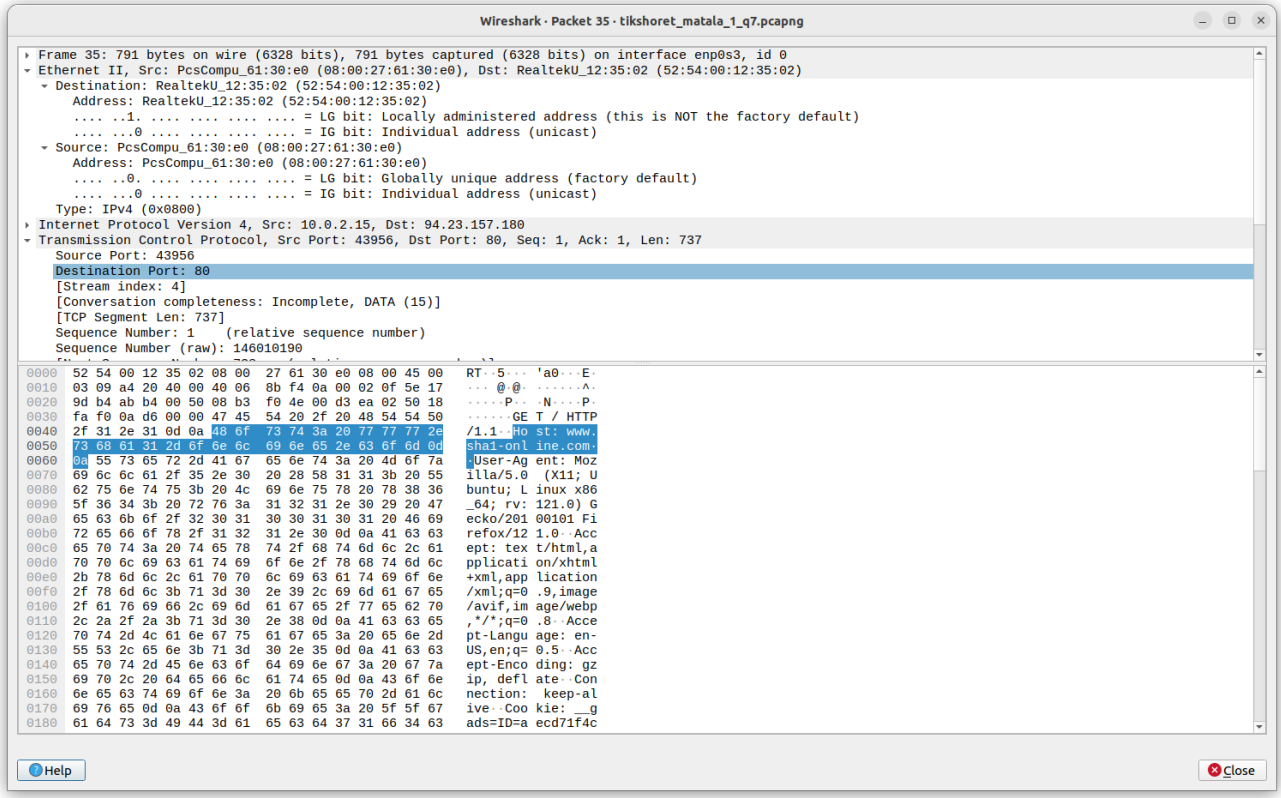
http://www.sha1-online.com

7. In the screenshot – first packet is the request one, second packet = response packet. Understood by the fact that these packets had the site's address in their description so thta these packets refer to the requested website. First packet here is the request one based on the "GET" keyword in the info – a hypertext transfer protocol command to recieve data from the requested http server. Therefore the second line describes the response (first packet's dest address is the src adress here)– containing text/html response as written in the packet's info.

8. (first two answers are based on the same screenshot as question no. 7)

a. It took approximatly 0.57 seconds between the request and the response.

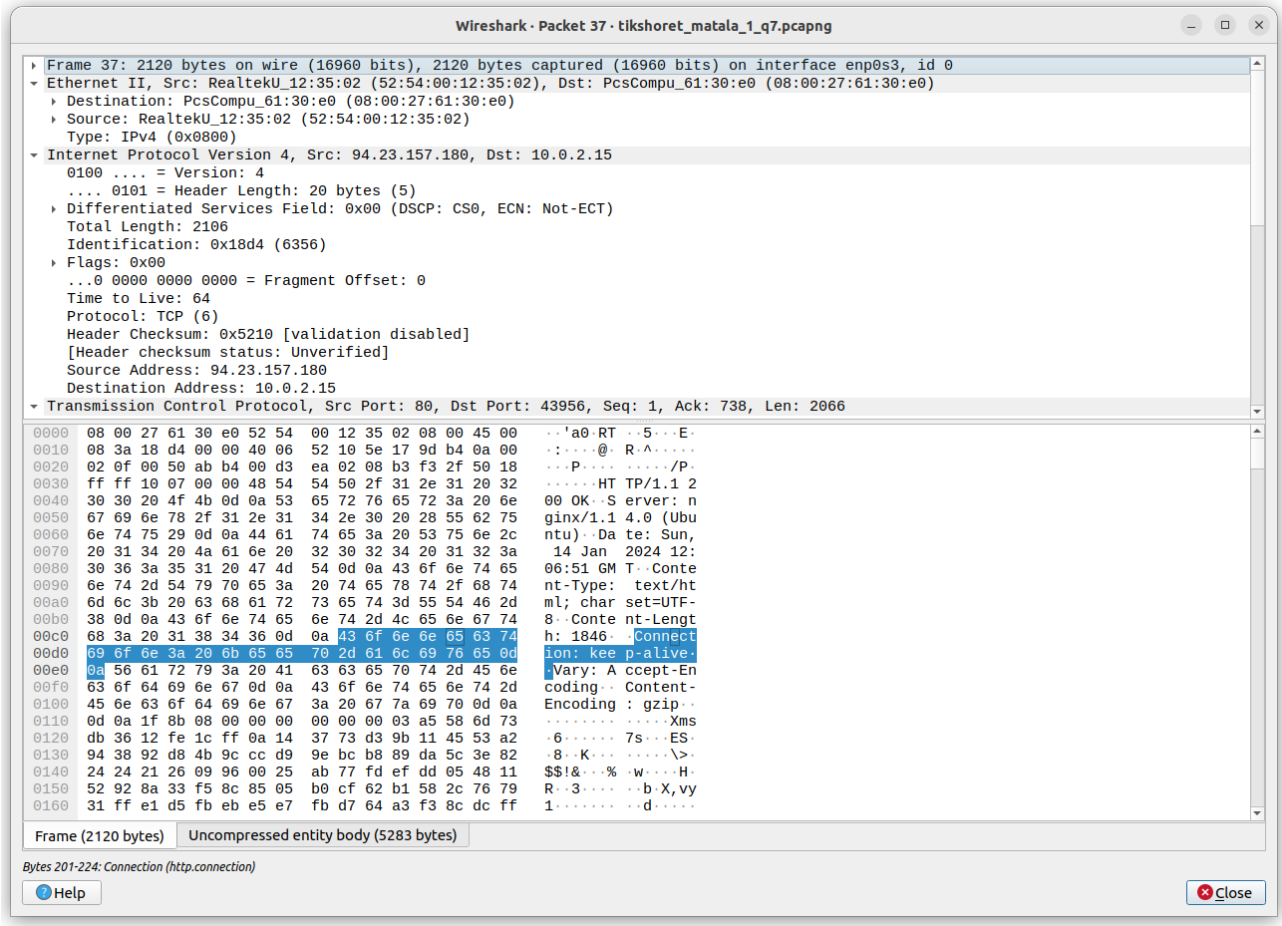
b. Http version was 1.1. (written in the info).



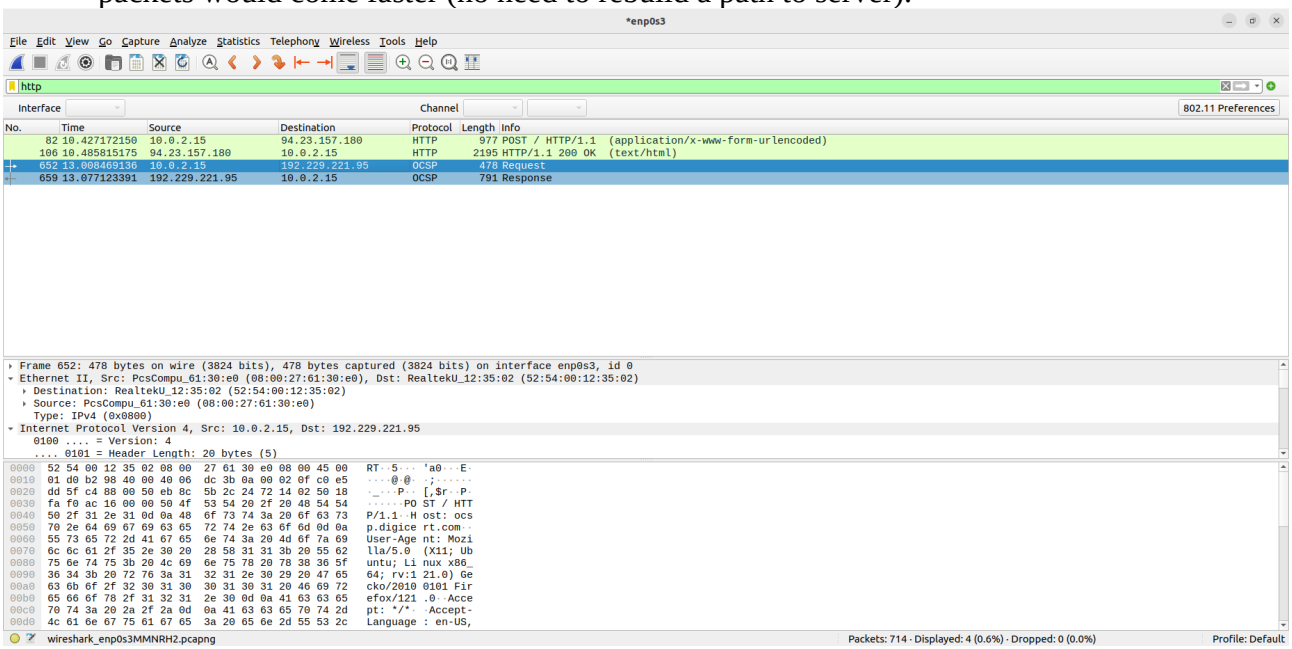
c. Source details: ip: 10.0.2.15. PscCompu_61:30:e0 (mac adress ending), MAC address: 08:00:27:61:30:e0.

d. The response frame is the "screenshoted" recieved frame no. 35.

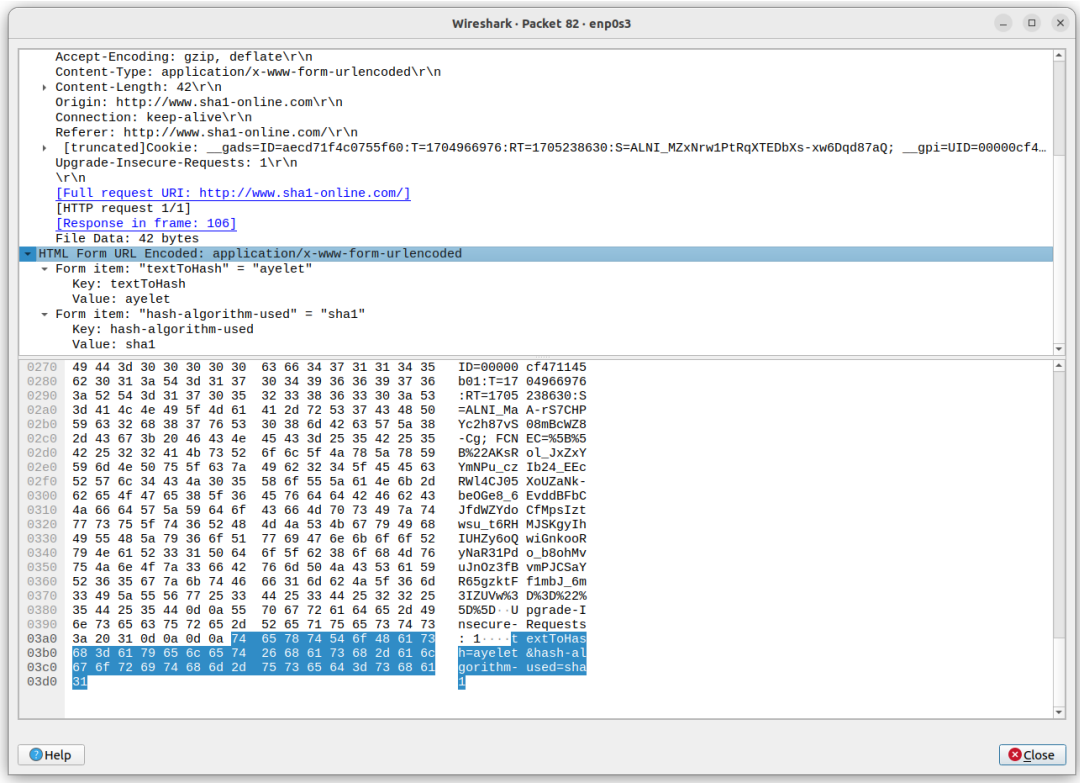
e. The destination port of the request packet is: 80.



9. a. The response code's status was 200 ok. (meaning it was procceeded correctly).
b. The response was recieved from a nginx server, ip address: 94.23.157.180.
c. It took two TCP frames to deliver the full response.
d. The connection type was "Keep-alive", which based on the details seems to mean that the connection to the server is maintained active so that the next requests or other recieved packets would come faster (no need to rebuild a path to server).



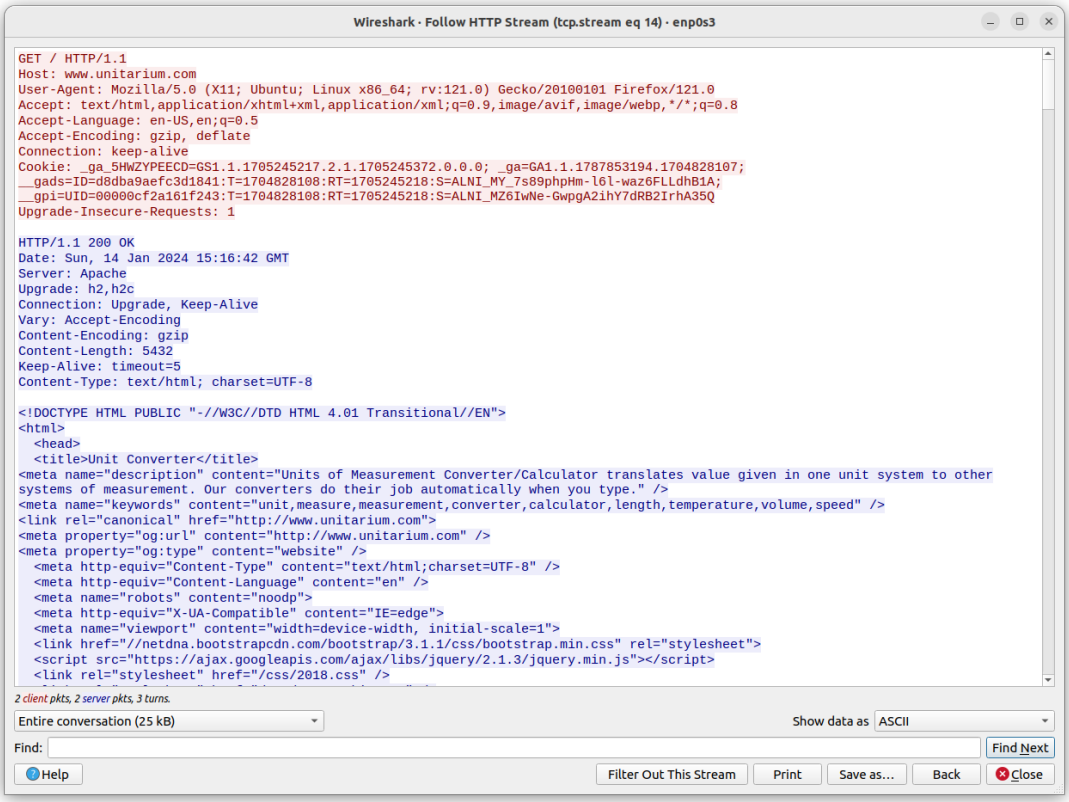
10. a. The calculations where performed via a distant server (if it would have been performed in the browser we wouldn't have seen any activity in wireshark + the request packet is destined to a different ip address).



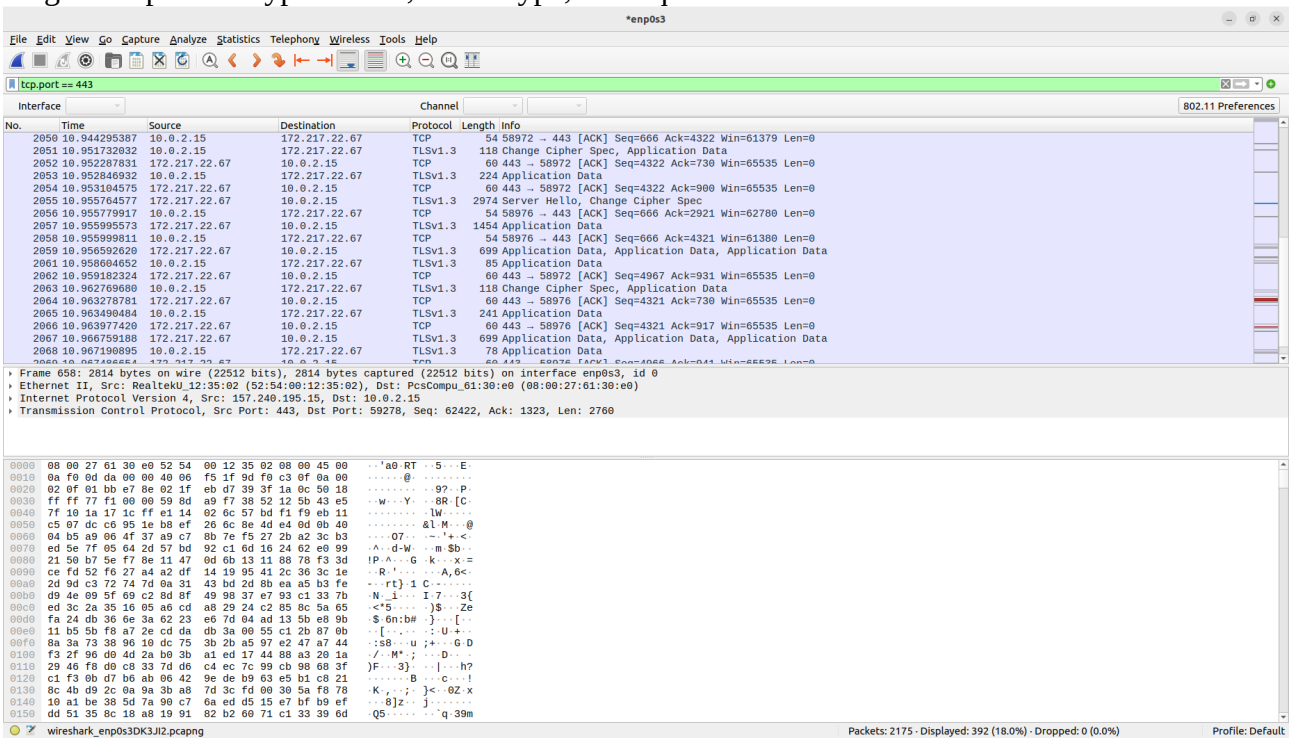
b. Data passed in the request: except for the regular information the packet also contains information about the calculation we are asking to perform – hash encoding the string "ayelet", while using hash algorithm "sha1".

c. Decided on http and not client sided calculating solution because the clint might not have the needed functions or abilities for the calculations.

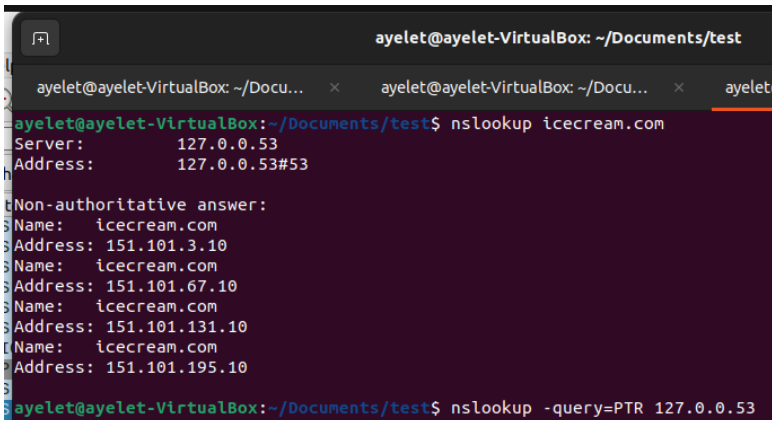
d. Possible risk that is caused by making the calculations on a distant server : delay in response, being dependent on the network connection, and tht the information is being exposed to client then.



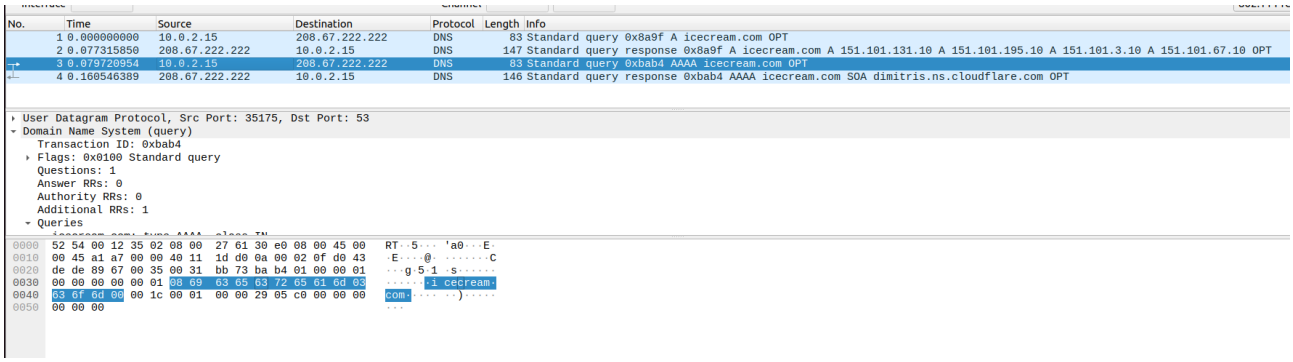
11. http://unitarium.com . a. As written at the bottom left corner of the screenshot there were 2 packets sent from client, and two sent from the server.
What came back in each packet from the server: The first server's packet contained text/html the second one contained text/css. Also contained http vesion, time stemp, connection status and how long to keep alive. Type of data, server type, the requested HTML file.



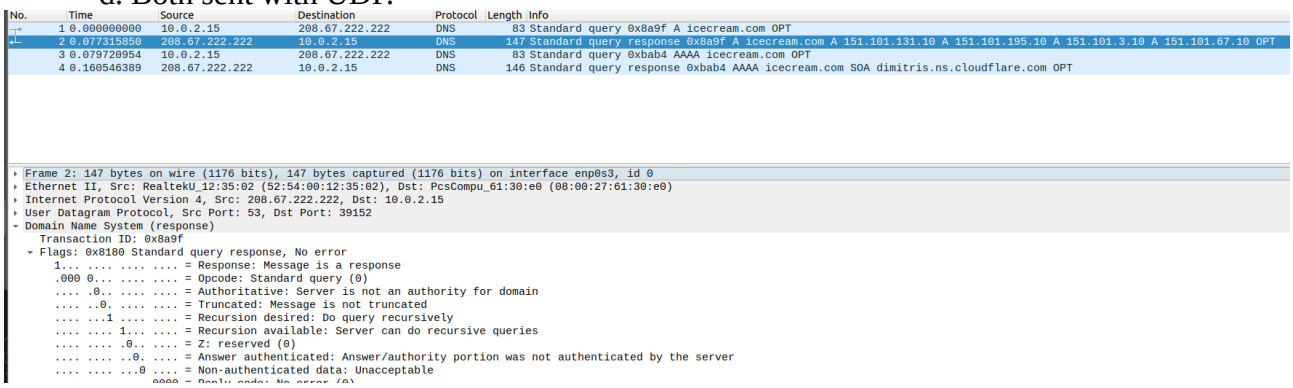
12. while requesting an http site, we've recieved http, tcp, and tlsv1.3 frames, an additional information used for encrtion and decription of http packets.



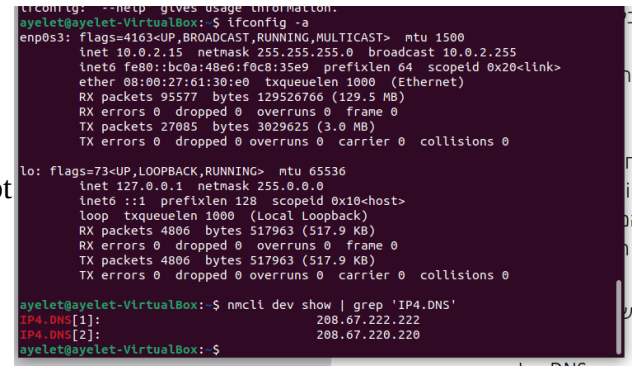
13. a. <u>The name of the answering server:</u> 127.0.0.53, a localhost.
<u>ip of domain:</u> has a 4 adresses, 151.101.131.10, 151.101.195.10, 151.101.3.10, 151.101.67.10
The server is non-authoritative.



14. a. I see to requests that regard this site icecream.com.
b. One request is of type A, one of type AAAA, first for ipv4, second for ipv6.
second request returned some server information.
c. First's request: src port: 39152 dest port: 53.
Second request's: src port: 35175 dest port: 53.
d. Both sent with UDP.



e. Were done using recursion.
f. for each request only one response.
g. A- ipv4, AAAA-ipv6.



15. a. Request sent to ip: 208.67.222.222
b. Yes, adresses are the same – in screenshot – 208.67.222.222
16. No ipv6 adress.

17. As shown in screenshot in wireshark dns is now 8.8.8.8.

Info	Length	Protocol	Destination	Source	Time	No.
Standard query 0xfa35 A play.google.com	75	DNS	8.8.8.8	10.9.3.181	24.976110	32112
Standard query 0x539b HTTPS play.google.com	75	DNS	8.8.8.8	10.9.3.181	24.976479	32118
Standard query response 0xfa35 A play.google.com A 142.251.142.206	91	DNS	10.9.3.181	8.8.8.8	25.025315	32156
Standard query response 0x539b HTTPS play.google.com SOA ns1.google.com	125	DNS	10.9.3.181	8.8.8.8	25.043374	32188

```
Wireless LAN adapter   Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Wi-Fi 6 AX203
   Physical Address. . . . . . . . . : 10-F6-0A-EF-A5-6A
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::248a:8fc7:5401:7314%15(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.9.3.181(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Lease Obtained. . . . . . . . . . :  פברואר 04יום ראשון 2024 14:27:48
   Lease Expires . . . . . . . . . . :  פברואר 04יום ראשון 2024 19:05:58
   Default Gateway . . . . . . . . . : 10.9.15.254
   DHCP Server . . . . . . . . . . . : 172.16.0.235
   DHCPv6 IAID . . . . . . . . . . . : 152106506
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2C-5B-54-E4-00-00-10-02-65-F7
   DNS Servers . . . . . . . . . . . : 8.8.8.8
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

18. Probably most of the time the response will be heavier, because it contains all the answers to the request while the request transfers only what it needs answers on.

19. 1.

```
C:\Users\ayele>ping icecream.com

Pinging icecream.com [151.101.195.10] with 32 bytes of data:
Reply from 151.101.195.10: bytes=32 time=43ms TTL=57
Reply from 151.101.195.10: bytes=32 time=42ms TTL=57
Reply from 151.101.195.10: bytes=32 time=42ms TTL=57
Reply from 151.101.195.10: bytes=32 time=59ms TTL=57

Ping statistics for 151.101.195.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 42ms, Maximum = 59ms, Average = 46ms

C:\Users\ayele>ipconfig/displaydns

Windows IP Configuration

    icecream.com
    ----------------------------------------
    Record Name . . . . . : icecream.com
    Record Type . . . . . : 1
    Time To Live  . . . . : 268
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 151.101.195.10


    Record Name . . . . . : icecream.com
    Record Type . . . . . : 1
    Time To Live  . . . . : 268
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 151.101.131.10


    Record Name . . . . . : icecream.com
```

2.

```
C:\Users\ayele>ipconfig/flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Users\ayele>
```

3.

```
C:\Users\ayele>ping icecream.com

Pinging icecream.com [151.101.195.10] with 32 bytes of data:
Reply from 151.101.195.10: bytes=32 time=43ms TTL=57
Reply from 151.101.195.10: bytes=32 time=42ms TTL=57
Reply from 151.101.195.10: bytes=32 time=42ms TTL=57
Reply from 151.101.195.10: bytes=32 time=59ms TTL=57

Ping statistics for 151.101.195.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 42ms, Maximum = 59ms, Average = 46ms

C:\Users\ayele>ipconfig/displaydns

Windows IP Configuration

    icecream.com
    ----------------------------------------
    Record Name . . . . . : icecream.com
    Record Type . . . . . : 1
    Time To Live  . . . . : 268
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 151.101.195.10


    Record Name . . . . . : icecream.com
    Record Type . . . . . : 1
    Time To Live  . . . . : 268
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 151.101.131.10


    Record Name . . . . . : icecream.com
```

20. When a computer wants to browse to an https site, if it doesn’t know the ip of the domain it sends a dns query to it’s dns server to recieve the site’s ip adress. Then it sends the http request to it’s server, the server then returns (when needed after the travel to distant server that contains the information about the site) the site’s info.
If needed the information is splitted into two queries.
The packets contain different information bout the status of the request and the site, whether the transmition was full and successful, connection type, etc. The site uploads.