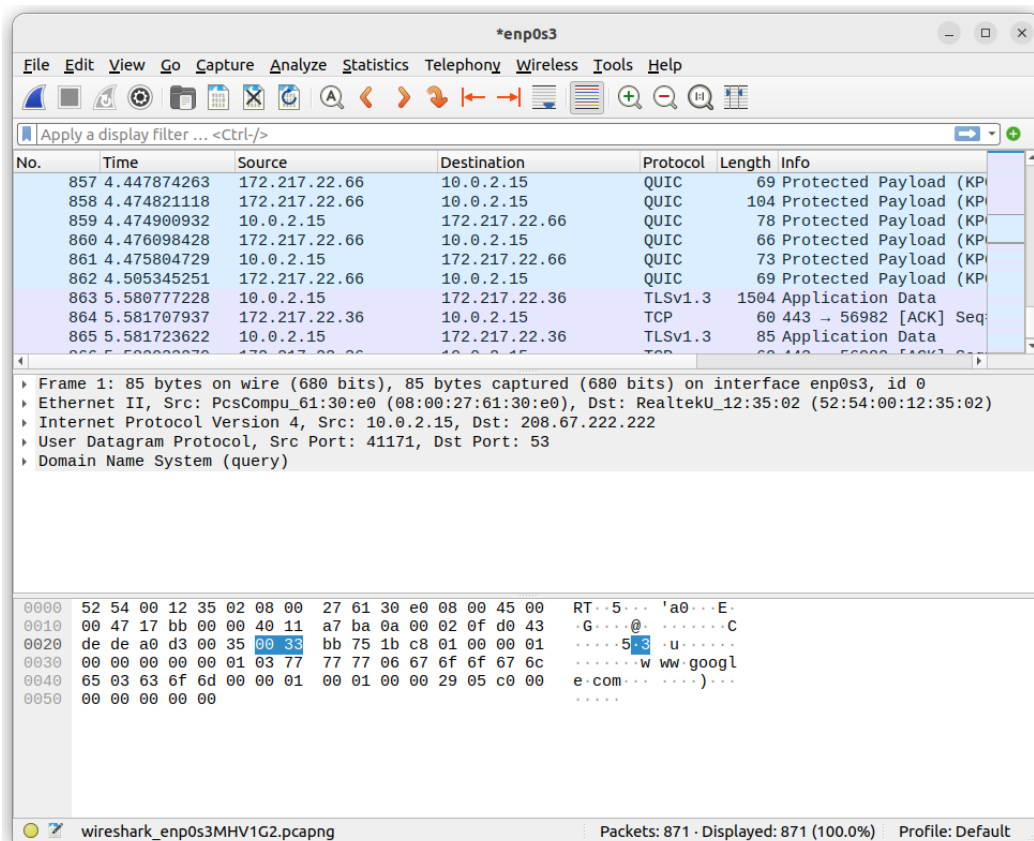


1. First window of Wireshark
 interent – enp0s3.



2. Packets catching on.

*enp0s3

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.dst==10.0.2.15

No.	Time	Source	Destination	Protocol	Length	Info
3	0.067487458	208.67.222.222	10.0.2.15	DNS	113	Standard query response
4	0.067487775	208.67.222.222	10.0.2.15	DNS	101	Standard query response
6	0.099083570	172.217.22.36	10.0.2.15	QUIC	1399	Initial, DCID=b58ced,
8	0.109888389	172.217.22.36	10.0.2.15	TCP	60	443 → 56980 [SYN, ACK]
11	0.111536378	172.217.22.36	10.0.2.15	TCP	60	443 → 56980 [ACK] Seq=
14	0.112108752	172.217.22.36	10.0.2.15	TCP	60	443 → 56980 [ACK] Seq=
15	0.112108835	172.217.22.36	10.0.2.15	TCP	60	443 → 56980 [ACK] Seq=
17	0.126775715	172.217.22.36	10.0.2.15	QUIC	1399	Protected Payload (KPI
18	0.126776061	172.217.22.36	10.0.2.15	QUIC	657	Protected Payload (KPI

Frame 3: 113 bytes on wire (904 bits), 113 bytes captured (904 bits) on interface enp0s3, id 0
 Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_61:30:e0 (08:00:27:61:30:e0)
 Internet Protocol Version 4, Src: 208.67.222.222, Dst: 10.0.2.15
 User Datagram Protocol, Src Port: 53, Dst Port: 47582
 Domain Name System (response)

```

0000  08 00 27 61 30 e0 52 54 00 12 35 02 08 00 45 00  ..'a0-RT ..5...E.
0010  00 63 14 03 00 00 40 11 ab 56 d0 43 de de 0a 00  .c...@. .V.C...
0020  02 0f 00 35 b9 de 00 4f e6 1f 04 55 81 80 00 01  ..5...0 ...U...
0030  00 01 00 00 00 01 03 77 77 77 06 67 6f 6f 67 6c  ....w ww.googl
0040  65 03 63 6f 6d 00 00 1c 00 01 c0 0c 00 1c 00 01  e.com...
0050  00 00 00 8b 00 10 2a 00 14 50 40 28 08 00 00 00  .....* .P@(...
0060  00 00 00 00 20 04 00 00 29 10 00 00 00 00 00 00  ..... ).....
0070  00
  
```

wireshark_enp0s3MHV1G2.pcapng Packets: 871 · Displayed: 480 (55.1%) · Dropped: 0 (0.0%) Profile: Default

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

*enp0s3

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.port == 443

No.	Time	Source	Destination	Protocol	Length	Info
11	0.105716637	10.0.2.15	172.217.22.36	TCP	74	33442 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK
14	0.120896957	172.217.22.36	10.0.2.15	TCP	60	443 → 33442 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MS
17	0.120584207	10.0.2.15	172.217.22.36	TCP	54	33442 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
18	0.121707474	10.0.2.15	172.217.22.36	TLSv1.3	1286	Client Hello
20	0.122659135	172.217.22.36	10.0.2.15	TCP	60	443 → 33442 [ACK] Seq=1 Ack=1233 Win=65535 Len=0
21	0.122677483	10.0.2.15	172.217.22.36	TLSv1.3	230	Change Cipher Spec, Application Data
22	0.123032628	172.217.22.36	10.0.2.15	TCP	60	443 → 33442 [ACK] Seq=1 Ack=1409 Win=65535 Len=0
34	0.198813603	172.217.22.36	10.0.2.15	TLSv1.3	915	Server Hello, Change Cipher Spec, Application Data, A
35	0.198864848	10.0.2.15	172.217.22.36	TCP	54	33442 → 443 [ACK] Seq=1409 Ack=862 Win=63714 Len=0

Frame 1606: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface enp0s3, id 0
 Ethernet II, Src: PcsCompu_61:30:e0 (08:00:27:61:30:e0), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
 Internet Protocol Version 4, Src: 10.0.2.15, Dst: 142.251.37.86
 Transmission Control Protocol, Src Port: 38954, Dst Port: 443, Seq: 1638, Ack: 940, Len: 24
 Transport Layer Security

```

0000  52 54 00 12 35 02 08 00 27 61 30 e0 08 00 45 00  RT..5... 'a0...E.
0010  00 40 6b ca 40 00 40 06 0e 8e 0a 00 02 0f 8e fb  .@k.@. ....
0020  25 56 98 2a 01 bb 43 16 10 8e 11 41 fb ad 50 18  %V.*...C...A..P.
0030  f9 a6 c0 92 00 00 17 03 03 00 13 3c 44 d5 eb    ....<DM...
0040  84 77 48 63 5b 80 b2 98 48 e5 37 69 22 ce      .wHc[... H-7i"
  
```

wireshark_enp0s3MFYSG2.pcapng Packets: 1653 · Displayed: 381 (23.0%) Profile: Default

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

Wireshark capture of DNS traffic on interface enp0s3. The packet list shows multiple DNS queries and responses. The packet details pane shows the structure of a DNS response packet. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
1909	470.987871652	10.0.2.15	208.67.222.222	DNS	101	Standard query 0xa7ea A incoming.telemetry.mozill
1910	470.988438737	10.0.2.15	208.67.222.222	DNS	101	Standard query 0x777b AAAA incoming.telemetry.moz
1928	471.050440756	208.67.222.222	10.0.2.15	DNS	239	Standard query response 0x777b AAAA incoming.tele
1929	471.050440896	208.67.222.222	10.0.2.15	DNS	176	Standard query response 0xa7ea A incoming.telemet
1930	471.050268027	10.0.2.15	208.67.222.222	DNS	116	Standard query 0x1f51 AAAA telemetry-incoming.r53
1960	471.128273448	208.67.222.222	10.0.2.15	DNS	198	Standard query response 0x1f51 AAAA telemetry-inc
2087	471.689247635	10.0.2.15	208.67.222.222	DNS	82	Standard query 0xe4e5 A i.ytimg.com OPT
2088	471.689678473	10.0.2.15	208.67.222.222	DNS	82	Standard query 0x2ae7 AAAA i.ytimg.com OPT
2097	471.737195308	10.0.2.15	208.67.222.222	DNS	86	Standard query 0x4cf9 A apis.google.com OPT
2098	471.761074221	208.67.222.222	10.0.2.15	DNS	194	Standard query response 0x2ae7 AAAA i.ytimg.com A
2099	471.761074368	208.67.222.222	10.0.2.15	DNS	338	Standard query response 0xe4e5 A i.ytimg.com A 17
2100	471.761246717	10.0.2.15	208.67.222.222	DNS	86	Standard query 0x9e2b AAAA apis.google.com OPT
2143	471.810076381	208.67.222.222	10.0.2.15	DNS	123	Standard query response 0x4cf9 A apis.google.com

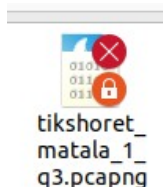
Frame 7127: 113 bytes on wire (904 bits), 113 bytes captured (904 bits) on interface enp0s3, id 0
Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_61:30:e0 (08:00:27:61:30:e0)
Internet Protocol Version 4, Src: 208.67.222.222, Dst: 10.0.2.15
User Datagram Protocol, Src Port: 53, Dst Port: 58455
Domain Name System (response)

0000 08 00 27 61 30 e0 52 54 00 12 35 02 08 00 45 00 ..a0-RT..5...E-
0010 00 63 2b a6 00 00 40 11 93 b3 d0 43 de de 0a 00 -c+...@...C....
0020 02 0f 00 35 e4 57 00 4f 79 e5 7c e4 81 80 00 01 ...5-W-o y|.....
0030 00 01 00 00 00 01 04 6f 63 73 70 05 72 32 6d 30o csp-r2m0
0040 33 0b 61 6d 61 7a 6f 6e 74 72 75 73 74 03 63 6f 3-amazon trust.co
0050 6d 00 00 01 00 01 c0 0c 00 01 00 01 00 00 00 2e m.....
0060 00 04 41 09 71 e3 00 00 29 10 00 00 00 00 00 00 ..A-q...).....
0070 00

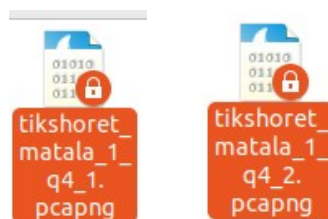
Domain Name System: Protocol Packets: 33745 · Displayed: 674 (2.0%) · Dropped: 0 (0.0%) Profile: Default

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 destined for it.

*enp0s3

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

frame contains "unit"

No.	Time	Source	Destination	Protocol	Length	Info
42	17.680802215	10.0.2.15	8.8.8.8	DNS	84	Standard query 0xedd4 AAAA unitarium.com OPT
48	17.786072540	8.8.8.8	10.0.2.15	DNS	152	Standard query response 0xedd4 AAAA unitarium.com
52	18.096628756	10.0.2.15	23.229.240.161	HTTP	682	GET / HTTP/1.1
80	18.639235567	10.0.2.15	104.18.11.207	HTTP	385	[TCP Previous segment not captured] GET /bootstrap
81	18.639377174	10.0.2.15	23.229.240.161	HTTP	633	GET /css/2018.css HTTP/1.1
82	18.639430232	10.0.2.15	23.229.240.161	HTTP	639	GET /css/purecookie.css HTTP/1.1
95	18.646661812	10.0.2.15	23.229.240.161	HTTP	656	GET /img/solar-live-en-350-2.webp HTTP/1.1
96	18.646830579	10.0.2.15	23.52.57.58	HTTP	348	[TCP Previous segment not captured] GET /js/300/a
156	18.790852117	10.0.2.15	142.251.37.66	HTTP	363	[TCP Previous segment not captured] GET /pagead/j
1450	22.075751992	10.0.2.15	8.8.8.8	DNS	89	Standard query 0x34ec AAAA time.unitarium.com OPT
1451	22.081083833	10.0.2.15	8.8.8.8	DNS	93	Standard query 0x2d8b AAAA covid-19.unitarium.com
1452	22.089237437	10.0.2.15	8.8.8.8	DNS	90	Standard query 0x4315 AAAA games.unitarium.com OP
1456	22.143414970	8.8.8.8	10.0.2.15	DNS	157	Standard query response 0x34ec AAAA time.unitariu

Frame 81: 633 bytes on wire (5064 bits), 633 bytes captured (5064 bits) on interface enp0s3, id 0
 Ethernet II, Src: PcsCompu_61:30:e0 (08:00:27:61:30:e0), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
 Internet Protocol Version 4, Src: 10.0.2.15, Dst: 23.229.240.161
 Transmission Control Protocol, Src Port: 47210, Dst Port: 80, Seq: 1, Ack: 1, Len: 579
 Hypertext Transfer Protocol

```

0000  52 54 00 12 35 02 08 00 27 61 30 e0 08 00 45 00  RT..5... 'a0...E
0010  02 6b bc ab 40 00 40 06 67 4c 0a 00 02 0f 17 e5  .k..@.. gL.....
0020  f0 a1 b8 6a 00 50 cd 14 a6 30 78 0f 5a 02 50 18  ...j..P.. 0x.Z.P
0030  fa f0 16 f3 00 00 47 45 54 20 2f 63 73 73 2f 32  ....GE T /css/2
0040  30 31 38 2e 63 73 73 20 48 54 54 50 2f 31 2e 31  018.css HTTP/1.1
0050  0d 0a 48 6f 73 74 3a 20 77 77 77 2e 75 6e 69 74  ..Host: www.unit
0060  61 72 69 75 6d 2e 63 6f 6d 0d 0a 55 73 65 72 2d  arium.co m..User-
0070  41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35  Agent: Mozilla/5
0080  2e 30 20 28 58 31 31 3b 20 55 62 75 6e 74 75 3b  .0 (X11; Ubuntu;
0090  20 4c 69 6e 75 78 20 78 38 36 5f 36 34 3b 20 72  Linux x86_64; r
00a0  76 3a 31 32 31 2e 30 29 20 47 65 63 6b 6f 2f 32  v:121.0) Gecko/2
00b0  30 31 30 30 31 30 31 20 46 69 72 65 66 6f 78 2f  0100101 Firefox/
  
```

Bytes 82-106: Host (http.host) Packets: 1560 · Displayed: 15 (1.0%) · Dropped: 0 (0.0%) Profile: Default

6. Filtering by " frame contains 'unit' " leaves only caught packets containing the sequence "unit" in their information.

*enp0s3

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

Interface Channel

No.	Time	Source	Destination	Protocol	Length	Info
35	3.576093312	10.0.2.15	94.23.157.180	HTTP	791	GET / HTTP/1.1
37	3.633750918	94.23.157.180	10.0.2.15	HTTP	2120	HTTP/1.1 200 OK (text/html)
61	3.747814834	10.0.2.15	94.23.157.180	HTTP	746	GET /styles.css?v18 HTTP/1.1
76	3.810899795	94.23.157.180	10.0.2.15	HTTP	728	HTTP/1.1 200 OK (text/css)
109	3.911227677	10.0.2.15	142.251.142.195	OCSP	481	Request
131	4.033096938	10.0.2.15	142.251.142.195	OCSP	481	Request
134	4.056978568	142.251.142.195	10.0.2.15	OCSP	756	Response
143	4.176328008	142.251.142.195	10.0.2.15	OCSP	756	Response
369	5.124492081	10.0.2.15	142.251.142.195	OCSP	481	Request
405	5.222470447	10.0.2.15	142.251.142.195	OCSP	481	Request
410	5.267877638	142.251.142.195	10.0.2.15	OCSP	756	Response
440	5.365468491	142.251.142.195	10.0.2.15	OCSP	756	Response
579	5.640714709	10.0.2.15	142.251.142.195	OCSP	480	Request
583	5.669405448	10.0.2.15	142.251.142.195	OCSP	481	Request
613	5.781937747	10.0.2.15	142.251.142.195	OCSP	480	Request
615	5.783827404	142.251.142.195	10.0.2.15	OCSP	755	Response
621	5.812663190	142.251.142.195	10.0.2.15	OCSP	756	Response
695	5.918120859	10.0.2.15	142.251.142.195	OCSP	481	Request

Frame 35: 791 bytes on wire (6328 bits), 791 bytes captured (6328 bits) on interface enp0s3, id 0
 Ethernet II, Src: PcsCompu_61:30:e0 (08:00:27:61:30:e0), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
 Internet Protocol Version 4, Src: 10.0.2.15, Dst: 94.23.157.180
 Transmission Control Protocol, Src Port: 43956, Dst Port: 80, Seq: 1, Ack: 1, Len: 737
 Hypertext Transfer Protocol

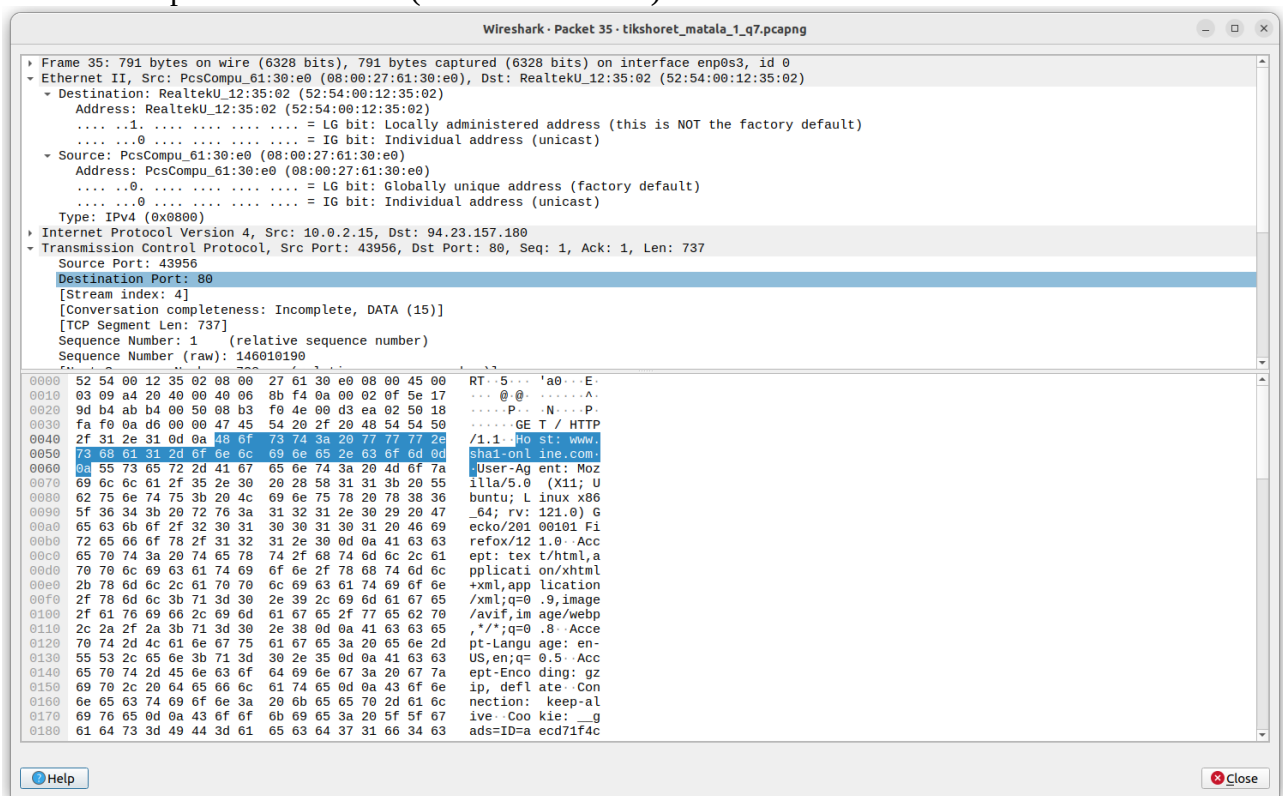
```

0000  52 54 00 12 35 02 08 00 27 61 30 e0 08 00 45 00  RT..5... 'a0...E
0010  03 09 a4 20 40 00 40 06 8b f4 0a 00 02 0f 5e 17  .@..@.....^
0020  9d b4 ab b4 00 50 08 b3 f0 4e 00 d3 ea 02 50 18  ....P...N...P
0030  fa f0 0a 0d 00 00 47 45 54 20 2f 20 48 54 54 50  ....GE T / HTTP
0040  2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77 77 2e  /1.1..Ho st: ww.
0050  73 68 61 31 2d 6f 6e 6c 69 6e 65 2e 63 6f 6d 0d  sha1-onl ine.com
0060  0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a  .User-Ag ent: Moz
0070  69 6c 6c 61 2f 35 2e 30 20 28 58 31 31 3b 20 55  illa/5.0 (X11; U
0080  62 75 6e 74 75 3b 20 4c 69 6e 75 78 20 78 38 36  buntu; L inux x86
0090  5f 36 34 3b 20 72 76 3a 31 32 31 2e 30 29 20 47  _64; rv: 121.0) G
00a0  65 63 6b 6f 2f 32 30 31 30 30 31 30 31 20 46 69  ecko/201 00101 Fi
00b0  72 65 66 6f 78 2f 31 32 31 2e 30 0d 0a 41 63 63  refox/12 1.0..Acc
00c0  65 70 74 3a 20 74 65 78 74 2f 68 74 6d 6c 2c 61  ept: tex t/html,a
00d0  70 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d 6c  pplicati on/xhtml
  
```

<http://www.sha1-online.com>

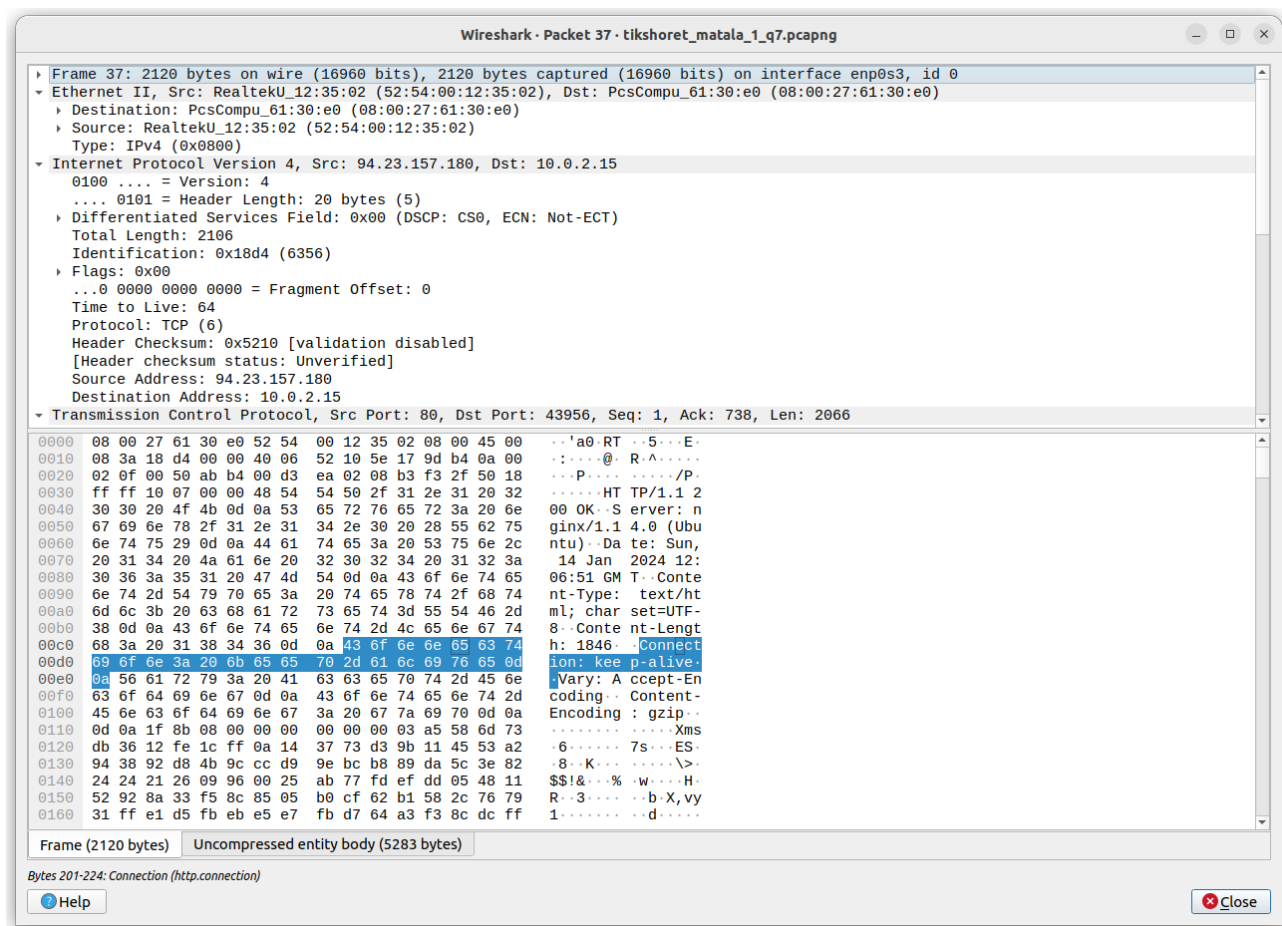
7. In the screenshot – first packet is the request one, second packet = response packet. Understood by the fact that these packets had the site's address in their description so that these packets refer to the requested website. First packet here is the request one based on the "GET" keyword in the info – a hypertext transfer protocol command to receive data from the requested http server. Therefore the second line describes the response (first packet's dest address is the src address 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)
- It took approximately 0.57 seconds between the request and the response.
 - Http version was 1.1. (written in the info).

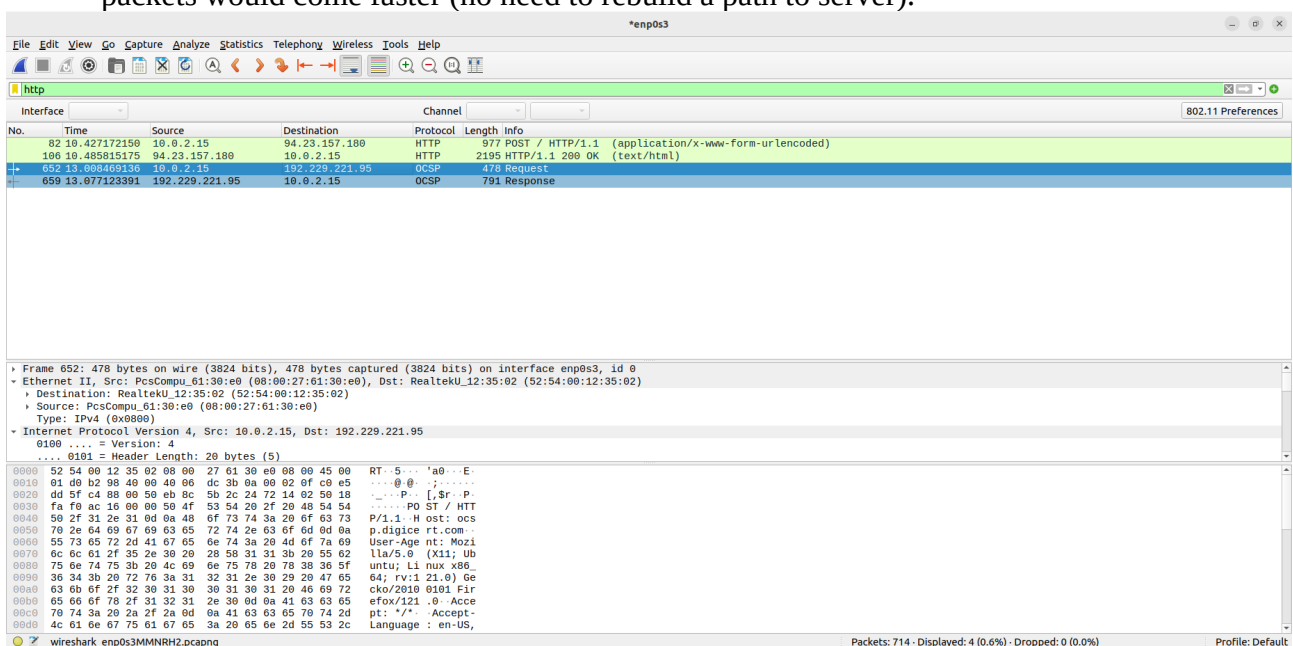


c. Source details: ip: 10.0.2.15. PscCompu_61:30:e0 (mac adress ending), MAC address: 08:00:27:61:30:e0.

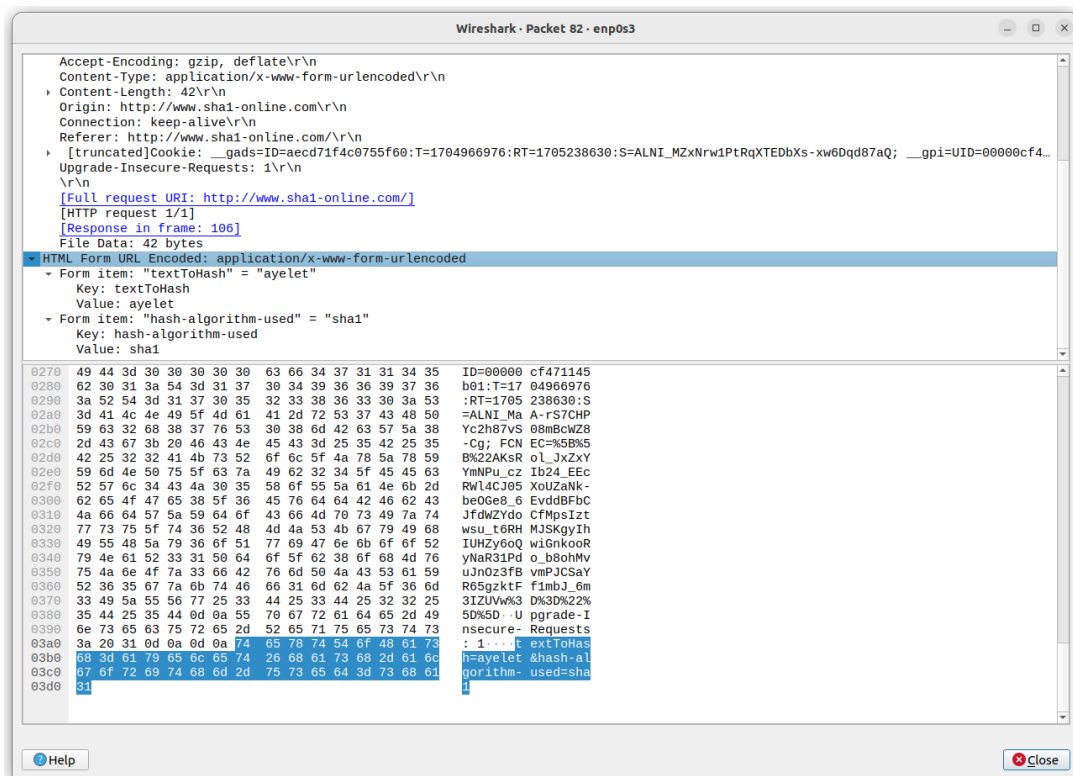
- The response frame is the "screenshoted" recieved frame no. 35.
- The destination port of the request packet is: 80.



9.
 - a. The response code's status was 200 ok. (meaning it was proceeded 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).



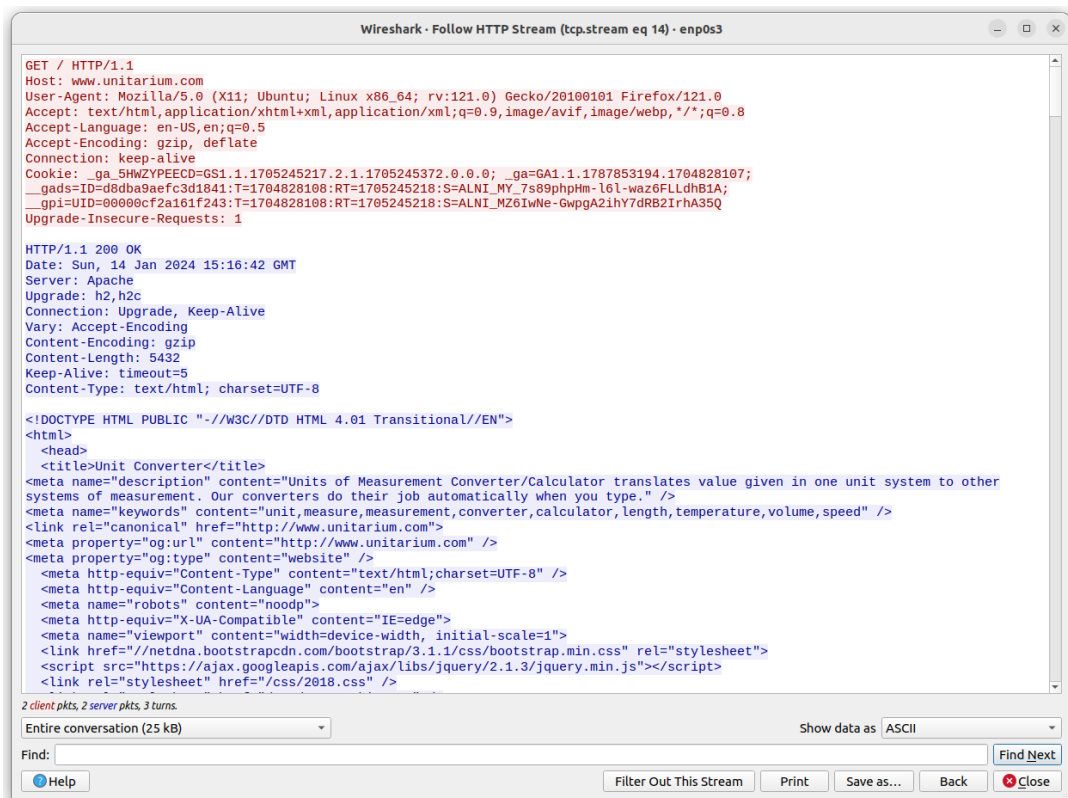
10.
 - a. The calculations where performed via a distant server (if it would have been performed in the browser we wouldn't have seen any activity in wireshark + the request packet is destined to a different ip address).



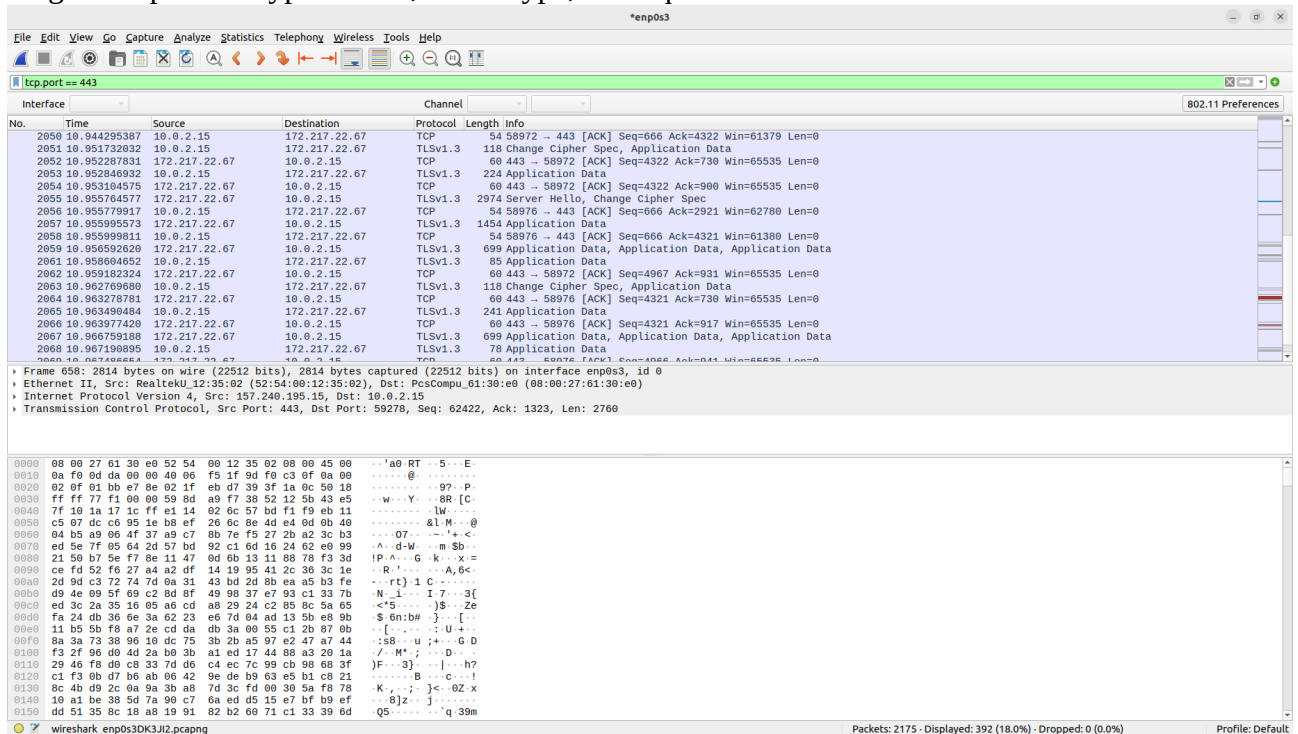
b. Data passed in the request: except for the regular information the packet also contains information about the calculation we are asking to perform – hash encoding the string "ayelet", while using hash algorithm "sha1".

c. Decided on http and not client sided calculating solution because the client 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 that 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 version, time stamp, 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 tls1.3 frames, an additional information used for encrntion and decryption of http packets.


```

ayelet@ayelet-VirtualBox: ~/Documents/test
ayelet@ayelet-VirtualBox: ~/Documents/test$ nslookup icecream.com
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
Name:   icecream.com
Address: 151.101.3.10
Name:   icecream.com
Address: 151.101.67.10
Name:   icecream.com
Address: 151.101.131.10
Name:   icecream.com
Address: 151.101.195.10
ayelet@ayelet-VirtualBox: ~/Documents/test$ nslookup -query=PTR 127.0.0.53

```

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

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.15	208.67.222.222	DNS	83	Standard query 0x8a9f A icecream.com OPT
2	0.077315850	208.67.222.222	10.0.2.15	DNS	147	Standard query response 0x8a9f A icecream.com A 151.101.131.10 A 151.101.195.10 A 151.101.3.10 A 151.101.67.10 OPT
3	0.079720954	10.0.2.15	208.67.222.222	DNS	83	Standard query 0xbab4 AAAA icecream.com OPT
4	0.160546389	208.67.222.222	10.0.2.15	DNS	146	Standard query response 0xbab4 AAAA icecream.com SOA dimitris.ns.cloudflare.com OPT


```

User Datagram Protocol, Src Port: 35175, Dst Port: 53
Domain Name System (query)
Transaction ID: 0xbab4
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 1
Queries
  0x8a9f A icecream.com
  0xbab4 AAAA icecream.com

```

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.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.15	208.67.222.222	DNS	83	Standard query 0x8a9f A icecream.com OPT
2	0.077315850	208.67.222.222	10.0.2.15	DNS	147	Standard query response 0x8a9f A icecream.com A 151.101.131.10 A 151.101.195.10 A 151.101.3.10 A 151.101.67.10 OPT
3	0.079720954	10.0.2.15	208.67.222.222	DNS	83	Standard query 0xbab4 AAAA icecream.com OPT
4	0.160546389	208.67.222.222	10.0.2.15	DNS	146	Standard query response 0xbab4 AAAA icecream.com SOA dimitris.ns.cloudflare.com OPT


```

Frame 2: 147 bytes on wire (1176 bits), 147 bytes captured (1176 bits) on interface enp0s3, id 0
Ethernet II, Src: RealtekU12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_61:30:e0 (08:00:27:61:30:e0)
Internet Protocol Version 4, Src: 208.67.222.222, Dst: 10.0.2.15
User Datagram Protocol, Src Port: 53, Dst Port: 39152
Domain Name System (response)
Transaction ID: 0x8a9f
Flags: 0x8180 Standard query response, No error
1... .. = Response: Message is a response
.000 0... .. = Opcode: Standard query (0)
... .. = Authoritative: Server is not an authority for domain
... .. = Truncated: Message is not truncated
... .. = Recursion desired: Do query recursively
... .. = Recursion available: Server can do recursive queries
... .. = Z: reserved (0)
... .. = Answer authenticated: Answer/authority portion was not authenticated by the server
... .. = Non-authenticated data: Unacceptable

```

- 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, addresses are the same – in screenshot – 208.67.222.222
16. No ipv6 adress.

```

ifconfig: --help gives usage information.
ayelet@ayelet-VirtualBox: $ ifconfig -a
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
    inet6 fe80::bc0a:48e6:f0c8:35e9 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:61:30:e0 txqueuelen 1000 (Ethernet)
    RX packets 95577 bytes 129526766 (129.5 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 27085 bytes 3029625 (3.0 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 4806 bytes 517963 (517.9 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4806 bytes 517963 (517.9 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

ayelet@ayelet-VirtualBox: $ nmap -sT 208.67.222.222
Nmap scan report for 208.67.222.222
Host is up (0.0000s latency).

```

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 2024 14:27:48
Lease Expires . . . . . : פברואר 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 transmittion was full and successful, connection type, etc. The site uploads.