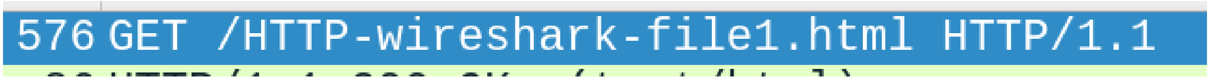
Lab 4 : Wireshark practice : Basic HTTP and DNS

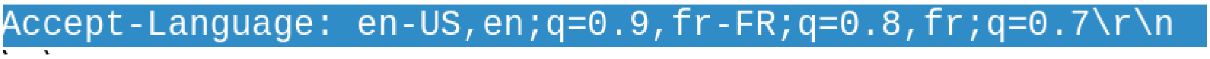
1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?

My browser is running in 1.1



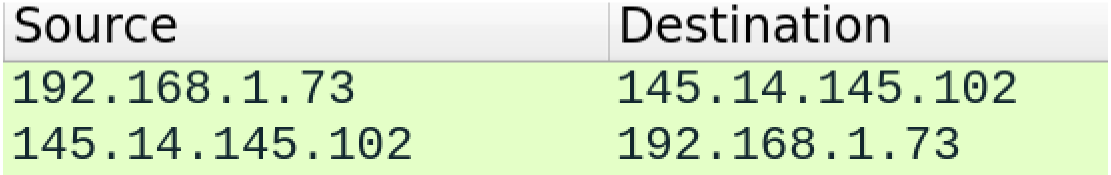
```
576 GET /HTTP-wireshark-file1.html HTTP/1.1
```

2. What languages (if any) does your browser indicate that it can accept to the server?



```
Accept-Language: en-US,en;q=0.9,fr-FR;q=0.8,fr;q=0.7\r\n
```

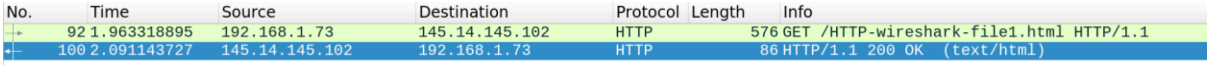
3. What is the IP address of your computer? Of the 000webhostapp.com server?



Source	Destination
192.168.1.73	145.14.145.102
145.14.145.102	192.168.1.73

My ip address is the first source and the second destination : 192.168.1.73
The 000webhostapp.com server ip address is 145.14.145.102.

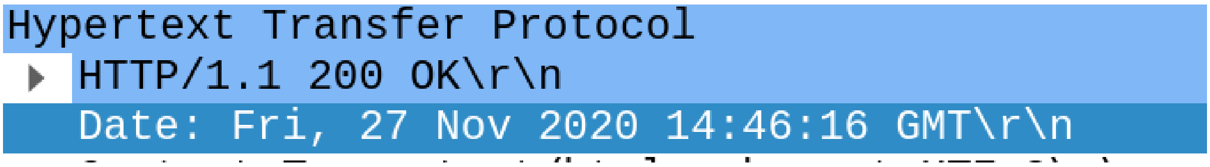
Q4) What is the status code returned from the server to your browser?



No.	Time	Source	Destination	Protocol	Length	Info
92	1.963318895	192.168.1.73	145.14.145.102	HTTP	576	GET /HTTP-wireshark-file1.html HTTP/1.1
100	2.091143727	145.14.145.102	192.168.1.73	HTTP	86	HTTP/1.1 200 OK (text/html)

The status code returned from the server to my browser is 200 that means OK.

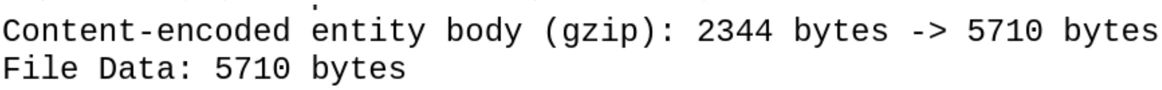
Q5) When (hour and date) was the HTML file that you are retrieving has been received?



```
Hypertext Transfer Protocol
  ▸ HTTP/1.1 200 OK\r\n
    Date: Fri, 27 Nov 2020 14:46:16 GMT\r\n
```

The HTML file was received on the friday 27 of november at 14;46:16.

Q6) How many bytes of content are being returned to your browser?



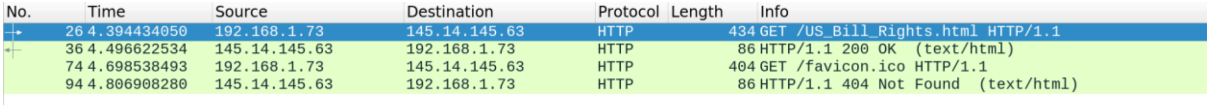
```
Content-encoded entity body (gzip): 2344 bytes -> 5710 bytes
File Data: 5710 bytes
```

There are 2344 bytes that are returned.

Q7) By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one.

No there is no headers within the data

Q8) How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the US Bill or Rights?



No.	Time	Source	Destination	Protocol	Length	Info
26	4.394434050	192.168.1.73	145.14.145.63	HTTP	434	GET /US_Bill_Rights.html HTTP/1.1
36	4.496622534	145.14.145.63	192.168.1.73	HTTP	86	HTTP/1.1 200 OK (text/html)
74	4.698538493	192.168.1.73	145.14.145.63	HTTP	404	GET /favicon.ico HTTP/1.1
94	4.806908280	145.14.145.63	192.168.1.73	HTTP	86	HTTP/1.1 404 Not Found (text/html)

I get 2 http get requests on wireshark.
The trace number for the US bill rights is 26.

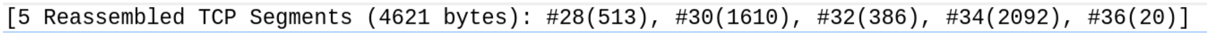
Q9) Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?

The packet number of the response is 36.

Q10) What is the status code and phrase in the response?

The status code is 200 and the response phase is OK.

Q11) How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?



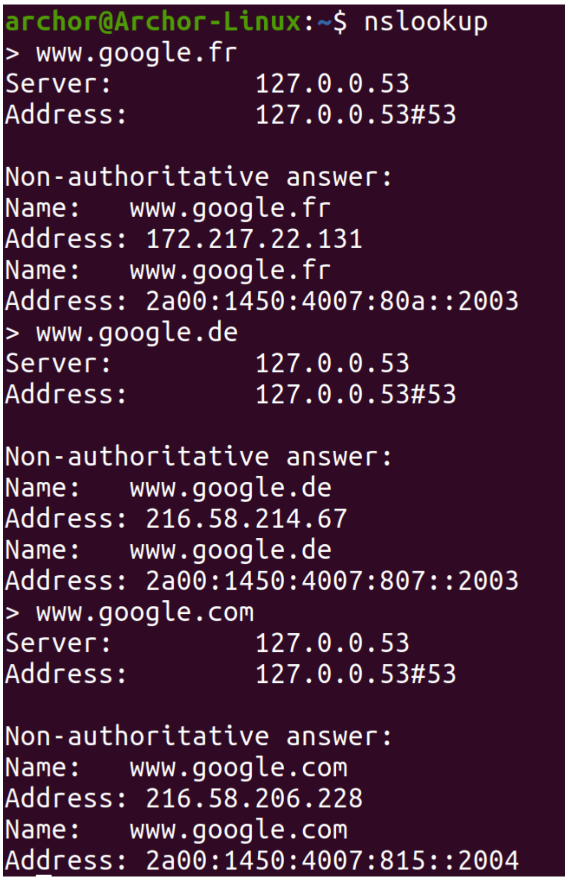
```
[5 Reassembled TCP Segments (4621 bytes): #28(513), #30(1610), #32(386), #34(2092), #36(20)]
```

There is 5 data containing TCP segments to carry the http response.

Q12) Explain briefly the second command line nslookup –type=NS ece.

It change the type of the information query to NS

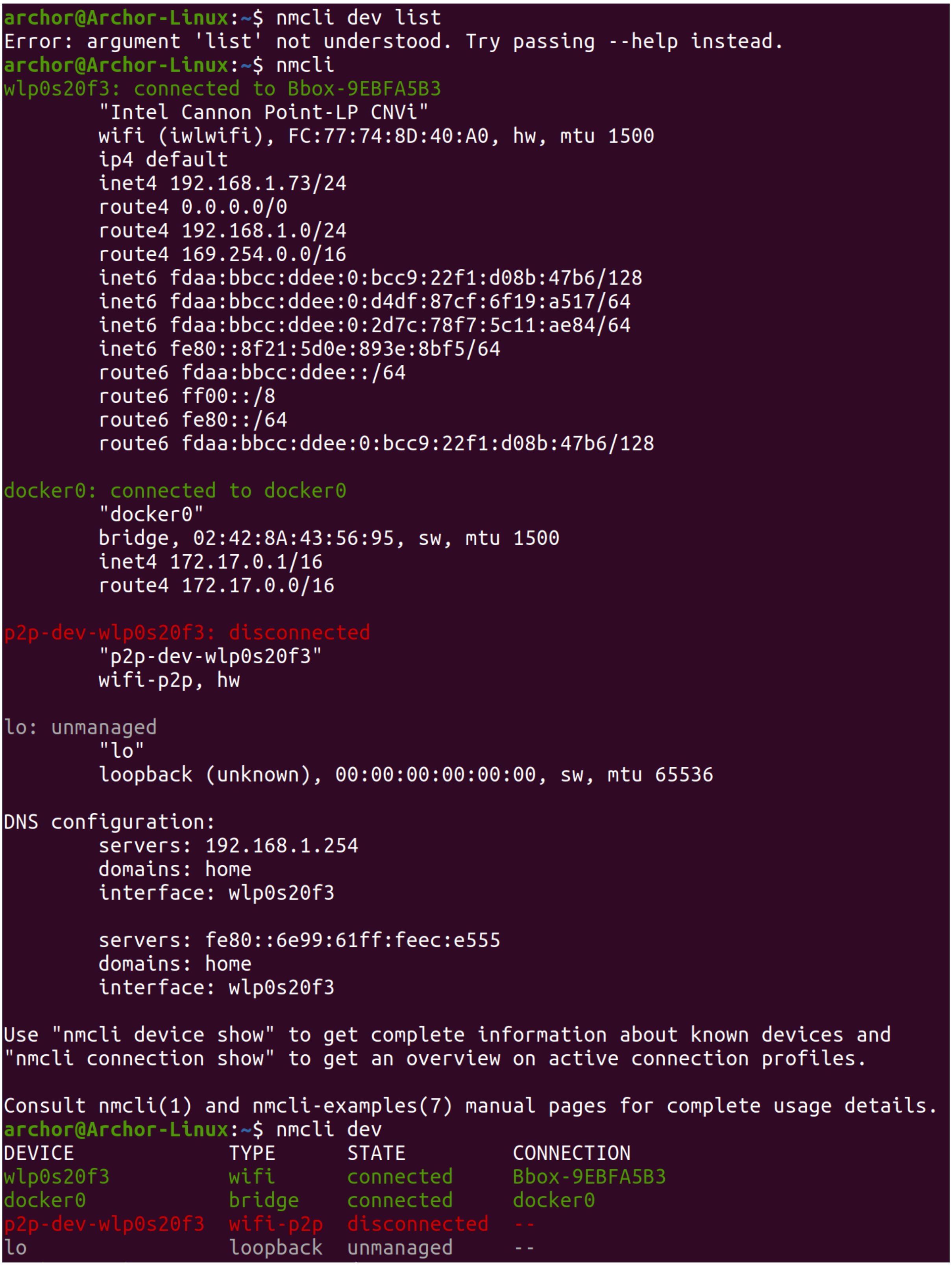
Q13) Run nslookup to obtain the IP address of google web server for .fr, .de and .com. Comment the obtained result ?



```
archor@Archor-Linux:~$ nslookup
> www.google.fr
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   www.google.fr
Address: 172.217.22.131
Name:   www.google.fr
Address: 2a00:1450:4007:80a::2003
> www.google.de
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   www.google.de
Address: 216.58.214.67
Name:   www.google.de
Address: 2a00:1450:4007:807::2003
> www.google.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   www.google.com
Address: 216.58.206.228
Name:   www.google.com
Address: 2a00:1450:4007:815::2004
```

We can see from the result that the IPV6 addresses are very similar.

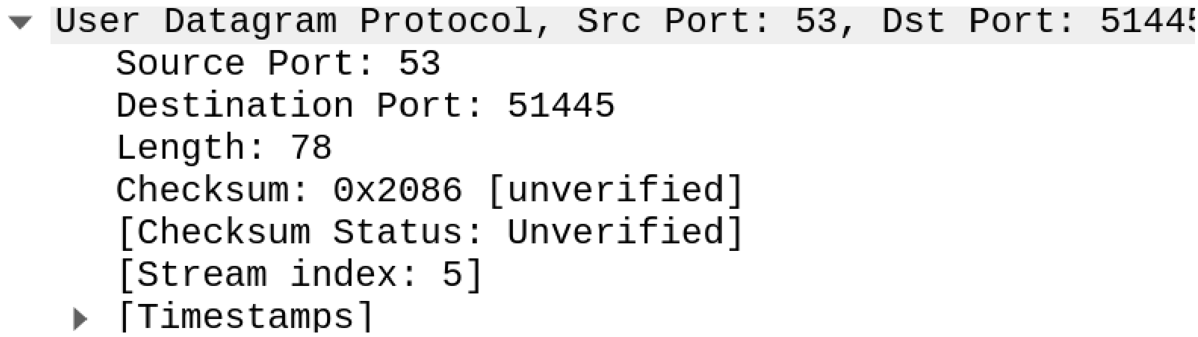
Q14) Use your “ipconfig/all” (windows) to get more information about your network. If you are on Linux you can use the command line “nmcli dev list”



```
archor@Archor-Linux:~$ nmcli dev list
Error: argument 'list' not understood. Try passing --help instead.
archor@Archor-Linux:~$ nmcli
wlp0s20f3: connected to Bbox-9EBFA5B3
        "Intel Cannon Point-LP CNVi"
        wifi (iwlwifi), FC:77:74:8D:40:A0, hw, mtu 1500
        ip4 default
        inet4 192.168.1.73/24
        route4 0.0.0.0/0
        route4 192.168.1.0/24
        route4 169.254.0.0/16
        inet6 fdaa:bbcc:ddee:0:bcc9:22f1:d08b:47b6/128
        inet6 fdaa:bbcc:ddee:0:d4df:87cf:6f19:a517/64
        inet6 fdaa:bbcc:ddee:0:2d7c:78f7:5c11:ae84/64
        inet6 fe80::8f21:5d0e:893e:8bf5/64
        route6 fdaa:bbcc:ddee::/64
        route6 ff00::/8
        route6 fe80::/64
        route6 fdaa:bbcc:ddee:0:bcc9:22f1:d08b:47b6/128

docker0: connected to docker0
        "docker0"
        bridge, 02:42:8A:43:56:95, sw, mtu 1500
        inet4 172.17.0.1/16
        route4 172.17.0.0/16

p2p-dev-wlp0s20f3: disconnected
        "p2p-dev-wlp0s20f3"
        wifi-p2p, hw

lo: unmanaged
        "lo"
        loopback (unknown), 00:00:00:00:00:00, sw, mtu 65536

DNS configuration:
        servers: 192.168.1.254
        domains: home
        interface: wlp0s20f3

        servers: fe80::6e99:61ff:feec:e555
        domains: home
        interface: wlp0s20f3

Use "nmcli device show" to get complete information about known devices and
"nmcli connection show" to get an overview on active connection profiles.

Consult nmcli(1) and nmcli-examples(7) manual pages for complete usage details.
archor@Archor-Linux:~$ nmcli dev
DEVICE             TYPE      STATE         CONNECTION
wlp0s20f3          wifi      connected     Bbox-9EBFA5B3
docker0            bridge    connected     docker0
p2p-dev-wlp0s20f3  wifi-p2p  disconnected  --
lo                 loopback  unmanaged     --
```

The command isn’t working on Linux. So I removed the parameters in order to make it work.

Q15) Locate the DNS query and response messages for www.ece.fr . To filter the query and response add in your filter the expression (dns.qry.name contains www.ece.fr). Are these messages sent over UDP or TCP?



```
▼ User Datagram Protocol, Src Port: 53, Dst Port: 51445
      Source Port: 53
      Destination Port: 51445
      Length: 78
      Checksum: 0x2086 [unverified]
      [Checksum Status: Unverified]
      [Stream index: 5]
   ▶ [Timestamps]
```

It use UDP.

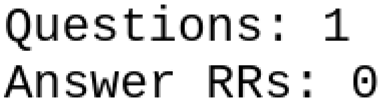
Q16) What is the destination port for the DNS query message? What is the source port of DNS response message?

The destination port is 53 and the source code for DNS response message is 53. As we can see in the previous screenshot

Q17) To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same? Use the result of ipconfig/all to answer.

It was sent to 192.168.1.254 which is my DNS ip adress. They are the same adresses.

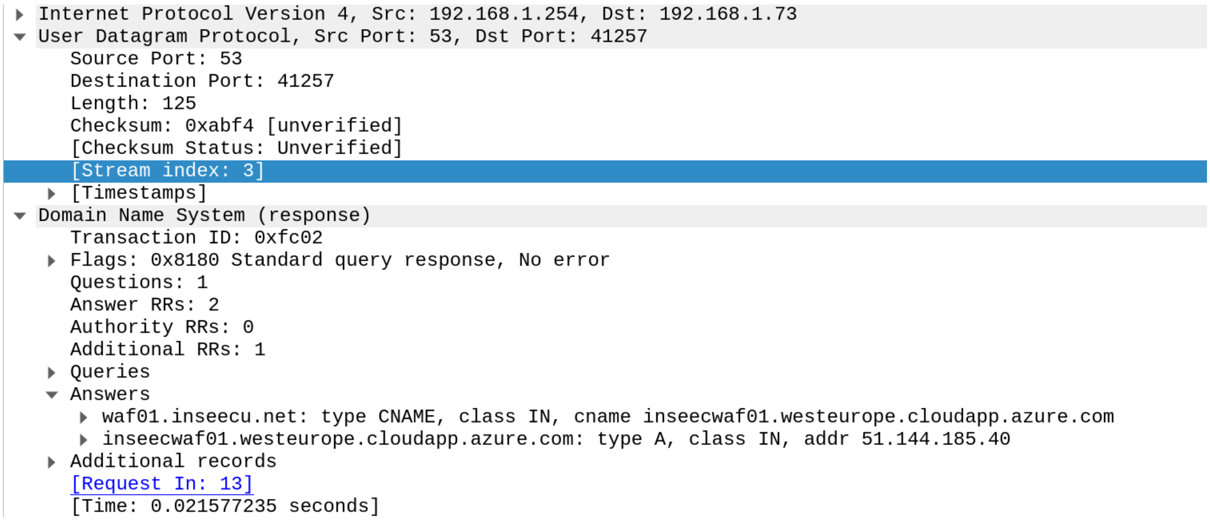
Q18) Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?



```
Questions: 1
Answer RRs: 0
```

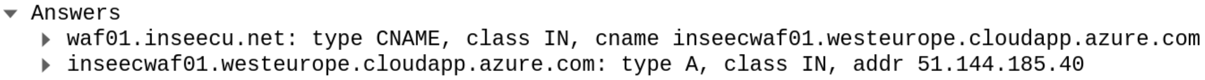
It’s a NS DNS type, it contain no answers.

Q19) Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?



```
▸ Internet Protocol Version 4, Src: 192.168.1.254, Dst: 192.168.1.73
▾ User Datagram Protocol, Src Port: 53, Dst Port: 41257
     Source Port: 53
     Destination Port: 41257
     Length: 125
     Checksum: 0xabf4 [unverified]
     [Checksum Status: Unverified]
     [Stream index: 3]
   ▸ [Timestamps]
▾ Domain Name System (response)
     Transaction ID: 0xfc02
   ▸ Flags: 0x8180 Standard query response, No error
     Questions: 1
     Answer RRs: 2
     Authority RRs: 0
     Additional RRs: 1
   ▸ Queries
   ▾ Answers
      ▸ waf01.inseecu.net: type CNAME, class IN, cname inseecwaf01.westeurope.cloudapp.azure.com
      ▸ inseecwaf01.westeurope.cloudapp.azure.com: type A, class IN, addr 51.144.185.40
   ▸ Additional records
     [Request In: 13]
     [Time: 0.021577235 seconds]
```

There are 2 answers and they contain :



```
▾ Answers
   ▸ waf01.inseecu.net: type CNAME, class IN, cname inseecwaf01.westeurope.cloudapp.azure.com
   ▸ inseecwaf01.westeurope.cloudapp.azure.com: type A, class IN, addr 51.144.185.40
```

Q20) Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message? Propose a filter expression to capture only SYN packets.

The destination IP adress of the SYN packet corresponds to the IP adress provided in the DNS response.

The filter expresion to capture SYN packets TCP.flag.syn == 1