Networking

TP – 4

Jacques Polart
Ing4 - SI

The basic HTTP GET/response interaction

Q1) Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?
1.1

Q2) What languages (if any) does your browser indicate that it can accept to the server?
HTTP

Q3) What is the IP address of your computer? Of the gaia.cs.umass.edu server?
Me : 128.119.245.12
Server : 10.9.19.190

Q4) What is the status code returned from the server to your browser?
200

Q5) When (hour and date) was the HTML file that you are retrieving has been received?
Date : Fri, 12 Nov 2021 12:36:34 GMT

Q6) How many bytes of content are being returned to your browser?
File Data: 4500 bytes

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

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?
2 GET request
packet number : 421

Q9) Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?
Packet number : 462

Q10) What is the status code and phrase in the response?
Status code : 200 Ok

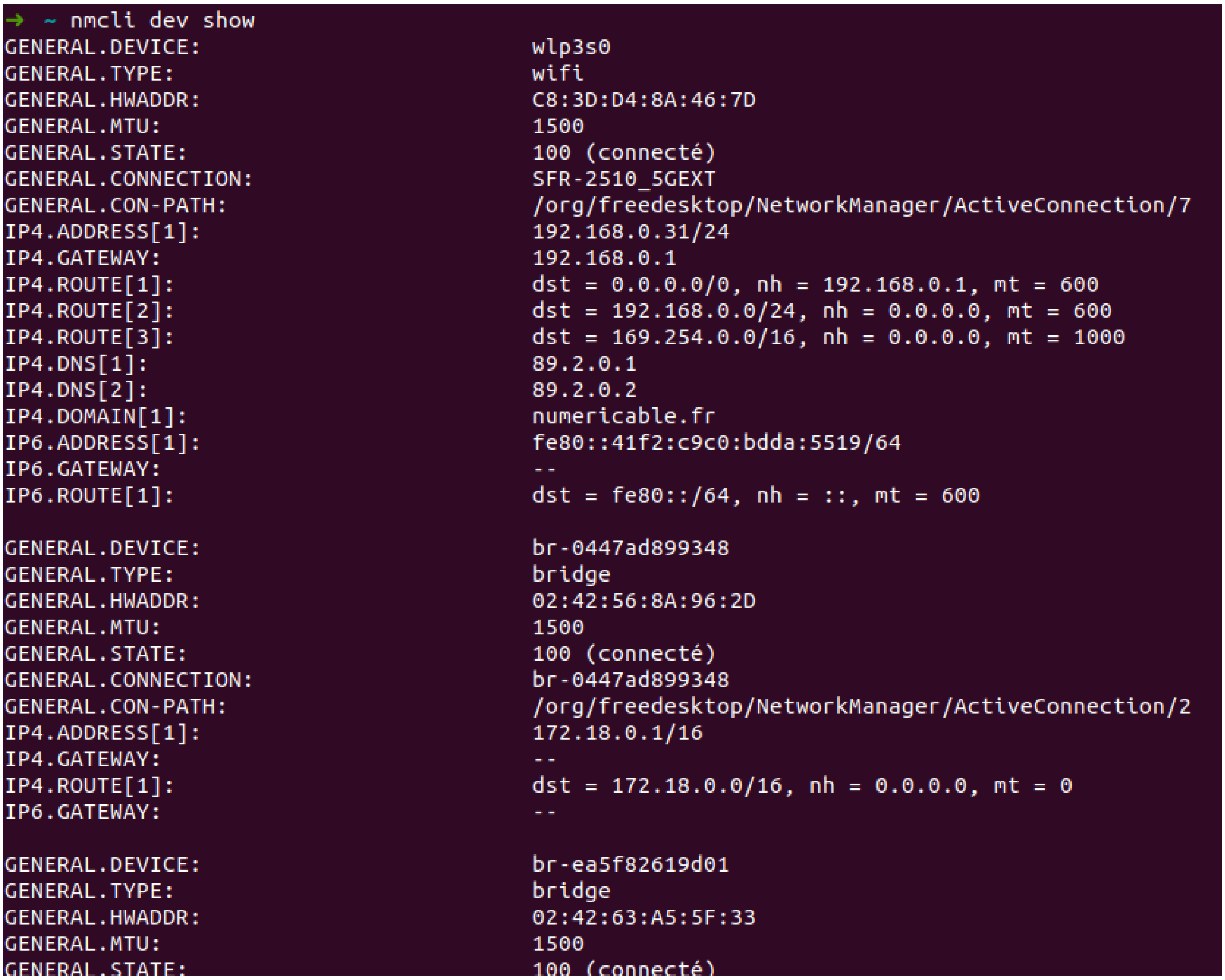
Q11) How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?
3 TCP segments

DNS

Q 12) Explain briefly the second command line nslookup –type=NS ece.fr
It is used to check the NS records of a domain. By checking the NS records, you can see which is the authoritative server for a specific domain.

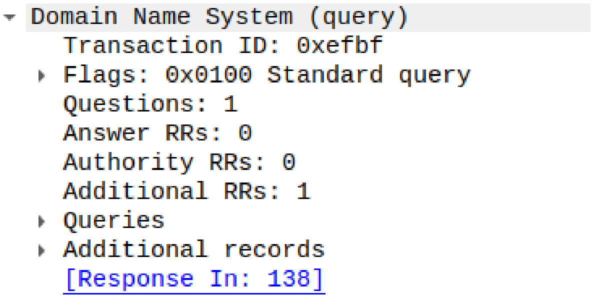
Q13) Run nslookup to obtain the IP address of google web server for .fr, .de and .com. Comment the obtained result.
All Ip address are differents

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"

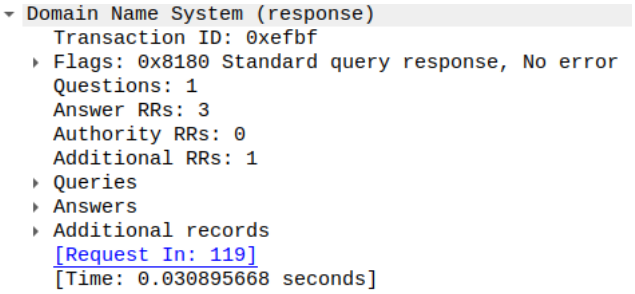


```
➜  ~ nmcli dev show
GENERAL.DEVICE:                         wlp3s0
GENERAL.TYPE:                           wifi
GENERAL.HWADDR:                         C8:3D:D4:8A:46:7D
GENERAL.MTU:                            1500
GENERAL.STATE:                          100 (connecté)
GENERAL.CONNECTION:                     SFR-2510_5GEXT
GENERAL.CON-PATH:                       /org/freedesktop/NetworkManager/ActiveConnection/7
IP4.ADDRESS[1]:                         192.168.0.31/24
IP4.GATEWAY:                            192.168.0.1
IP4.ROUTE[1]:                           dst = 0.0.0.0/0, nh = 192.168.0.1, mt = 600
IP4.ROUTE[2]:                           dst = 192.168.0.0/24, nh = 0.0.0.0, mt = 600
IP4.ROUTE[3]:                           dst = 169.254.0.0/16, nh = 0.0.0.0, mt = 1000
IP4.DNS[1]:                             89.2.0.1
IP4.DNS[2]:                             89.2.0.2
IP4.DOMAIN[1]:                          numericable.fr
IP6.ADDRESS[1]:                         fe80::41f2:c9c0:bdda:5519/64
IP6.GATEWAY:                            --
IP6.ROUTE[1]:                           dst = fe80::/64, nh = ::, mt = 600

GENERAL.DEVICE:                         br-0447ad899348
GENERAL.TYPE:                           bridge
GENERAL.HWADDR:                         02:42:56:8A:96:2D
GENERAL.MTU:                            1500
GENERAL.STATE:                          100 (connecté)
GENERAL.CONNECTION:                     br-0447ad899348
GENERAL.CON-PATH:                       /org/freedesktop/NetworkManager/ActiveConnection/2
IP4.ADDRESS[1]:                         172.18.0.1/16
IP4.GATEWAY:                            --
IP4.ROUTE[1]:                           dst = 172.18.0.0/16, nh = 0.0.0.0, mt = 0
IP6.GATEWAY:                            --

GENERAL.DEVICE:                         br-ea5f82619d01
GENERAL.TYPE:                           bridge
GENERAL.HWADDR:                         02:42:63:A5:5F:33
GENERAL.MTU:                            1500
GENERAL.STATE:                          100 (connecté)
```

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?

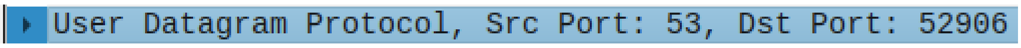


```
▾ Domain Name System (query)
    Transaction ID: 0xefbf
  ▸ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 1
  ▸ Queries
  ▸ Additional records
    [Response In: 138]
```



```
▾ Domain Name System (response)
    Transaction ID: 0xefbf
  ▸ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 1
  ▸ Queries
  ▸ Answers
  ▸ Additional records
    [Request In: 119]
    [Time: 0.030895668 seconds]
```

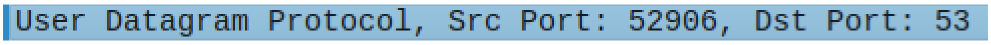
It is send by UDP



```
▸ User Datagram Protocol, Src Port: 53, Dst Port: 52906
```

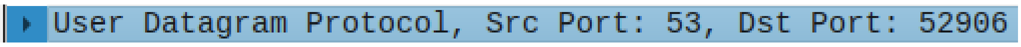
Q16) What is the destination port for the DNS query message? What is the source port of DNS response message?

The destiniation port of the query message is 53



```
User Datagram Protocol, Src Port: 52906, Dst Port: 53
```

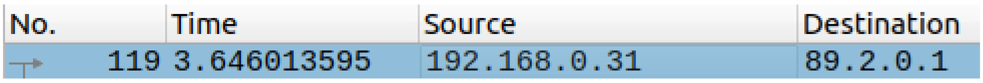
The source port of the responce message is 53



```
▸ User Datagram Protocol, Src Port: 53, Dst Port: 52906
```

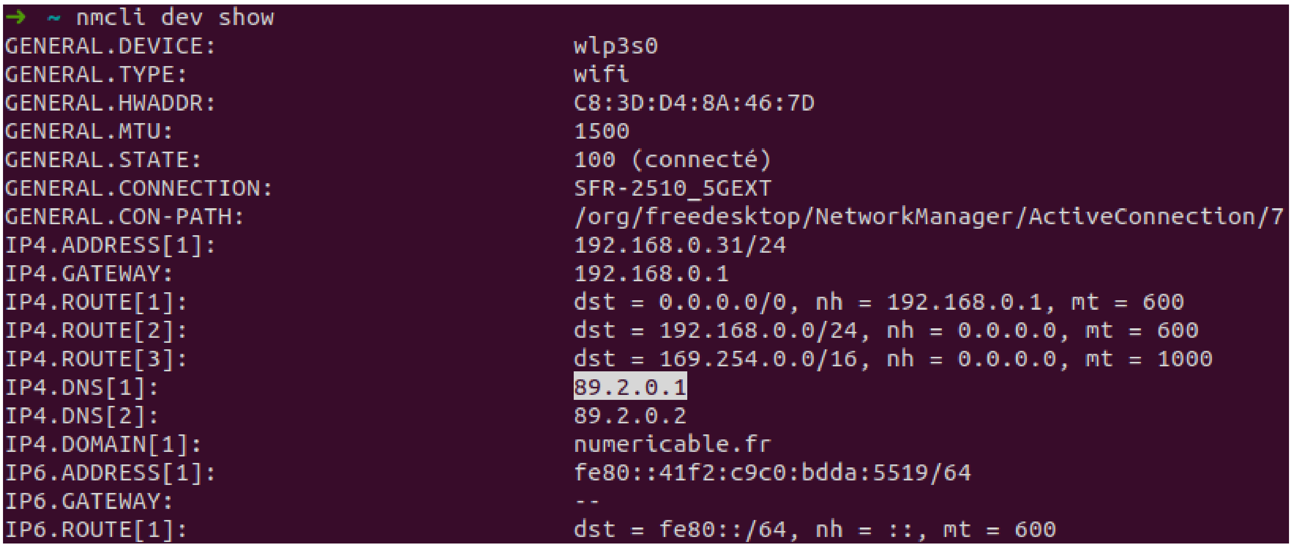
Q17) To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same? Use the result of ipconfig/all to answer.

Ip address in in the query message : 89.2.0.1



No.	Time	Source	Destination
119	3.646013595	192.168.0.31	89.2.0.1

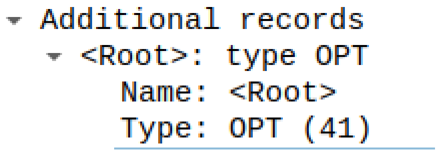
IP address of local DNS server : 89.2.0.1



```
➜ ~ nmcli dev show
GENERAL.DEVICE:                         wlp3s0
GENERAL.TYPE:                           wifi
GENERAL.HWADDR:                         C8:3D:D4:8A:46:7D
GENERAL.MTU:                            1500
GENERAL.STATE:                          100 (connecté)
GENERAL.CONNECTION:                     SFR-2510_5GEXT
GENERAL.CON-PATH:                       /org/freedesktop/NetworkManager/ActiveConnection/7
IP4.ADDRESS[1]:                         192.168.0.31/24
IP4.GATEWAY:                            192.168.0.1
IP4.ROUTE[1]:                           dst = 0.0.0.0/0, nh = 192.168.0.1, mt = 600
IP4.ROUTE[2]:                           dst = 192.168.0.0/24, nh = 0.0.0.0, mt = 600
IP4.ROUTE[3]:                           dst = 169.254.0.0/16, nh = 0.0.0.0, mt = 1000
IP4.DNS[1]:                             89.2.0.1
IP4.DNS[2]:                             89.2.0.2
IP4.DOMAIN[1]:                          numericable.fr
IP6.ADDRESS[1]:                         fe80::41f2:c9c0:bdda:5519/64
IP6.GATEWAY:                            --
IP6.ROUTE[1]:                           dst = fe80::/64, nh = ::, mt = 600
```

It’s the same IP

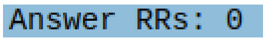
Q18) Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?



```
▾ Additional records
  ▾ <Root>: type OPT
      Name: <Root>
      Type: OPT (41)
```

Type : OPT

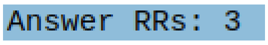
The query message does'nt constaint answers



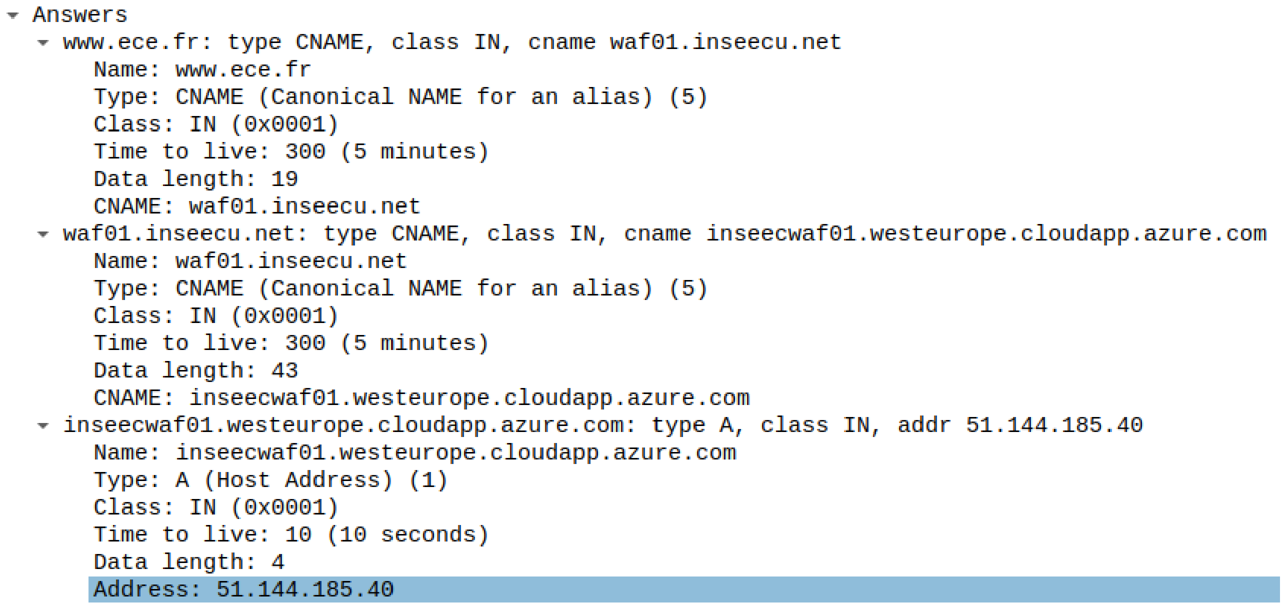
```
Answer RRs: 0
```

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

3 answers are provided



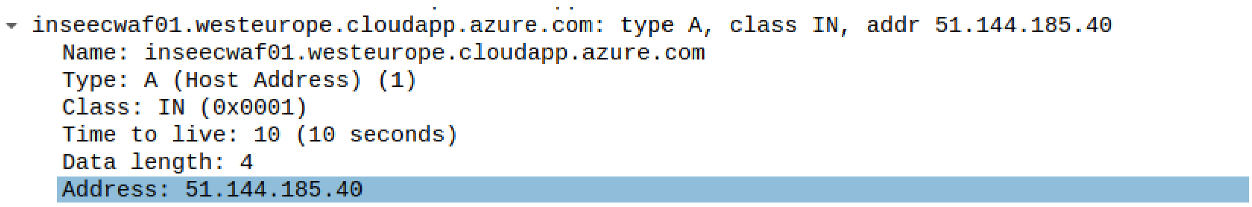
```
Answer RRs: 3
```



```
▾ Answers
  ▾ www.ece.fr: type CNAME, class IN, cname waf01.inseecu.net
      Name: www.ece.fr
      Type: CNAME (Canonical NAME for an alias) (5)
      Class: IN (0x0001)
      Time to live: 300 (5 minutes)
      Data length: 19
      CNAME: waf01.inseecu.net
  ▾ waf01.inseecu.net: type CNAME, class IN, cname inseecwaf01.westeurope.cloudapp.azure.com
      Name: waf01.inseecu.net
      Type: CNAME (Canonical NAME for an alias) (5)
      Class: IN (0x0001)
      Time to live: 300 (5 minutes)
      Data length: 43
      CNAME: inseecwaf01.westeurope.cloudapp.azure.com
  ▾ inseecwaf01.westeurope.cloudapp.azure.com: type A, class IN, addr 51.144.185.40
      Name: inseecwaf01.westeurope.cloudapp.azure.com
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 10 (10 seconds)
      Data length: 4
      Address: 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 TCP SYN packet is send to the server whose address is present in the response provider by the dns server : here it's 51.144.185.40



```
▾ inseecwaf01.westeurope.cloudapp.azure.com: type A, class IN, addr 51.144.185.40
    Name: inseecwaf01.westeurope.cloudapp.azure.com
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 10 (10 seconds)
    Data length: 4
    Address: 51.144.185.40
```

filter : tcp.flags.syn