**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?

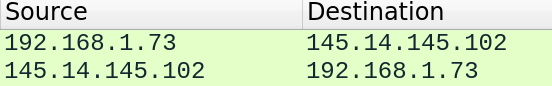
My browser is running in 1.1



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



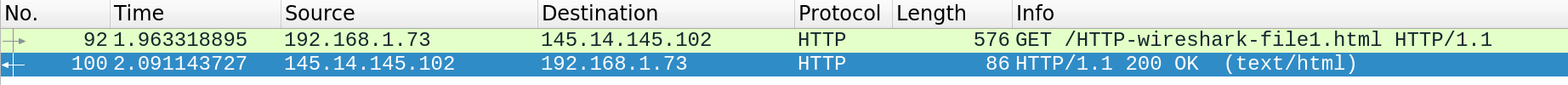
3. What is the IP address of your computer? Of the 000webhostapp.com server?



My ip address is the first source and the second destination : 192.168.1.73

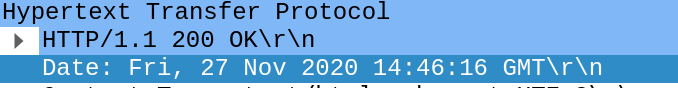
The 000webhostapp.com server ip address is 145.14.145.102.

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



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?



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?

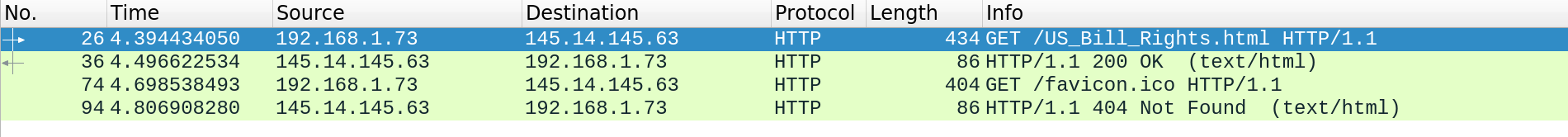


There are 2344 bytes that are returned.

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?



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?



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

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

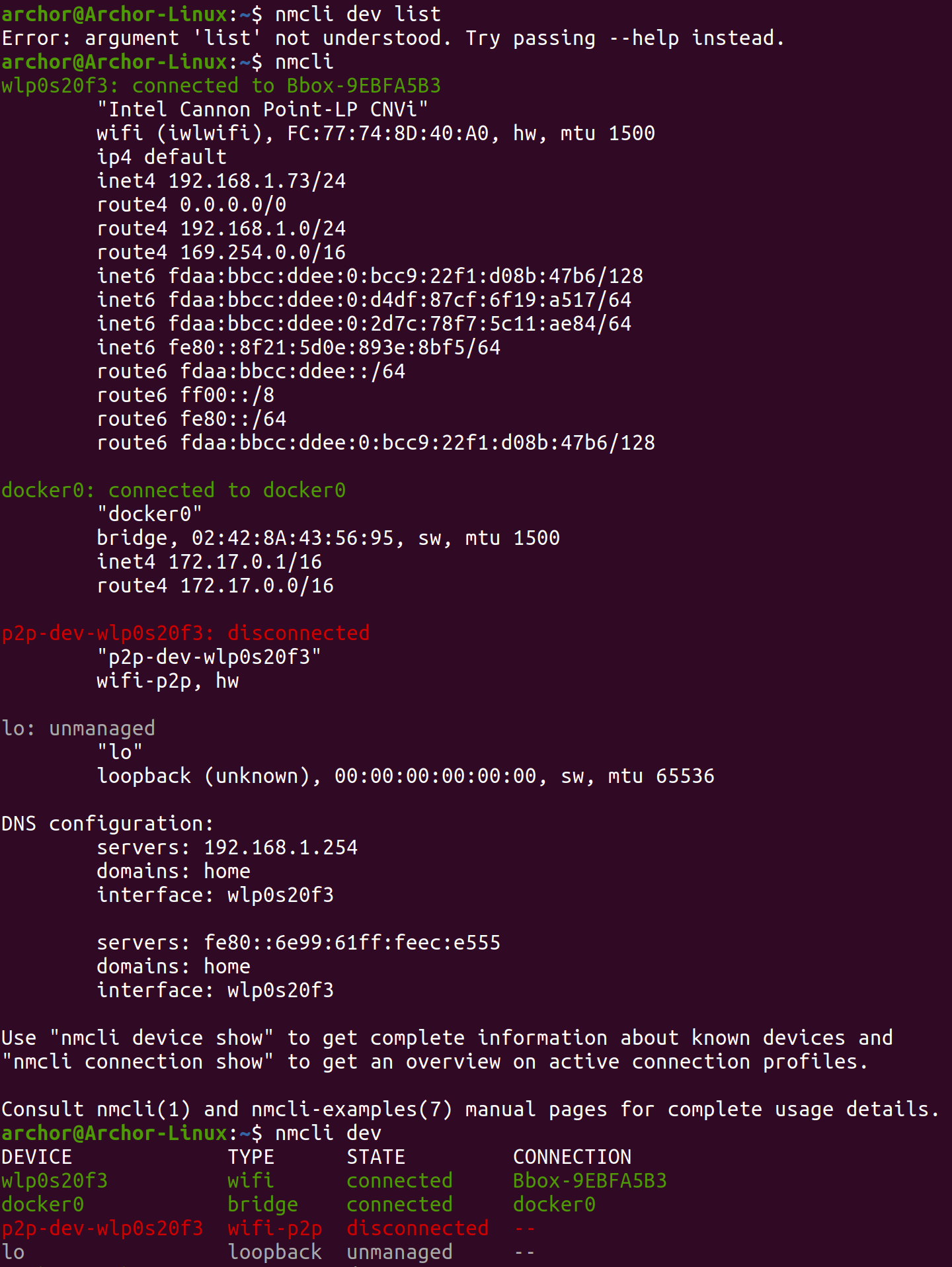
It change the type of the information query to NS

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



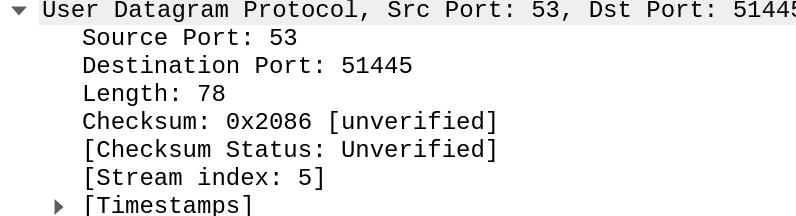
We can see from the result that the IPV6 addresses are very similar.

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”



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?



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.

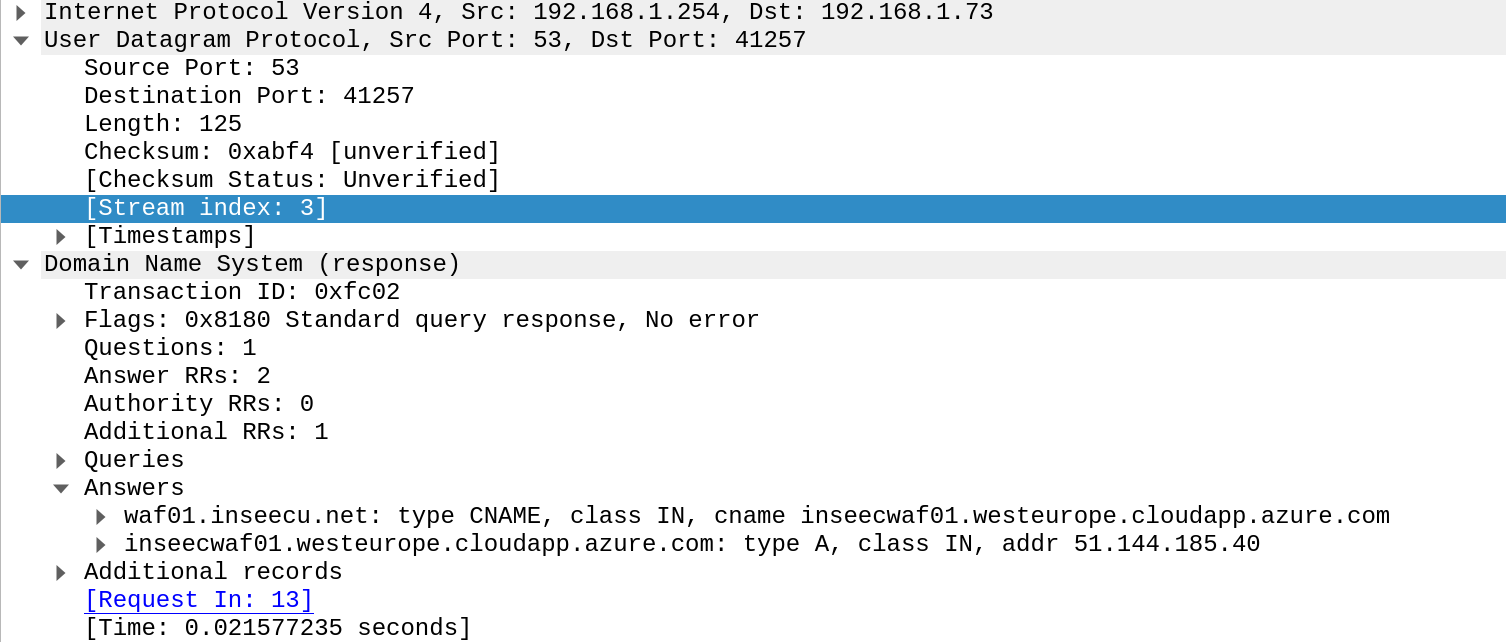
It was sent to 192.168.1.254 which is my DNS ip adress. They are the same adresses.

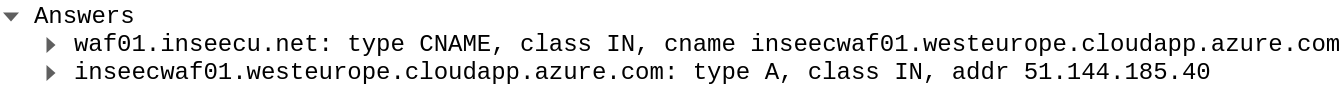
Q18) Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?



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?



There are 2 answers and they contain :****

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