**CCN LAB – 08**

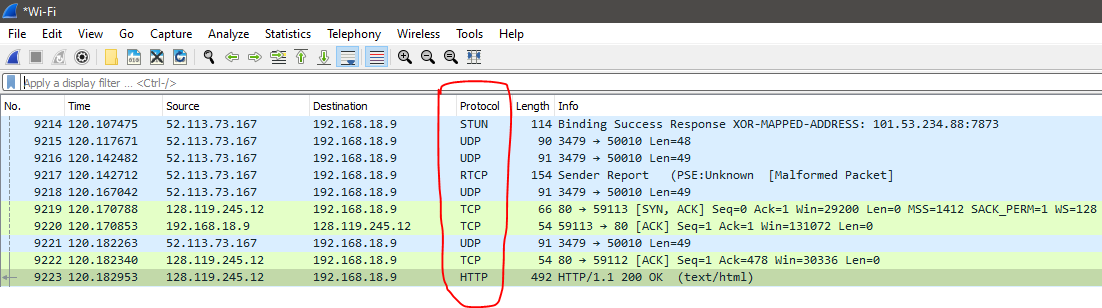
**Task-01**

**Explore the packets you captured from the test run and answer the following questions.**

**1.**

List up to 4 different protocols that appear in the protocol column in the unfiltered packet-listing window.

**Answer:**

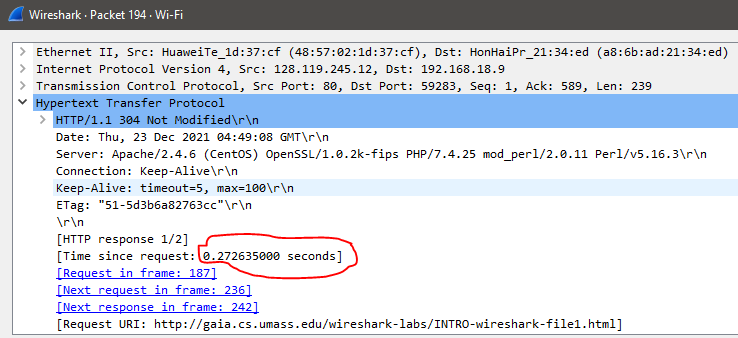


In the unfiltered list we can see protocols such as STUN, UDP, TCP, HTTP.

**2.**

What is the response time against HTTP GET Request?

**Answer:**

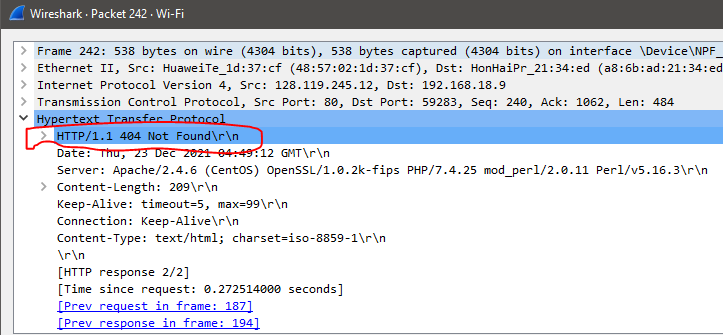


The response time against http get request is 0.272635000 seconds.

**3.**

Was the second Get Request successful? How can you tell it from the corresponding response packet?

**Answer:**

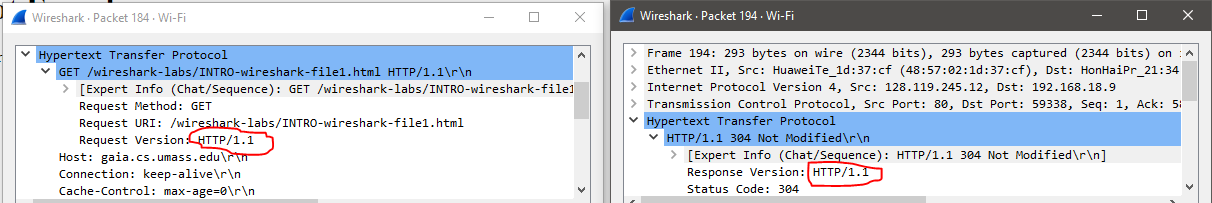


The second GET request was unsuccessful as the HTTP response message shows a status code of 404 not found.

**4.**

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

**Answer:**

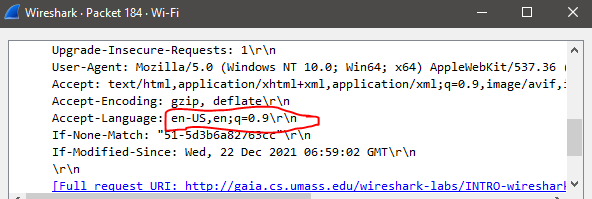


Both Client and server are running HTTP version 1.1

**5.**

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

**Answer:**

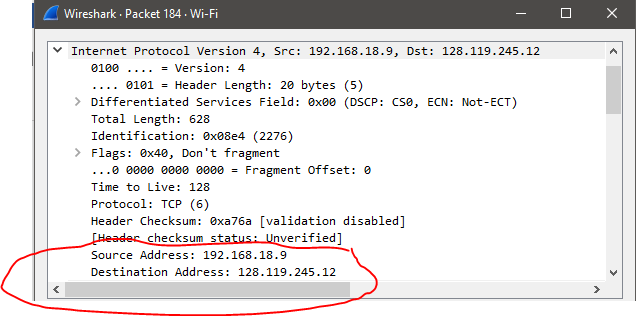


The browser indicates US English language that it can accept to the server.

**6.**

What is the IP address of the gaia.cs.umass.edu server and your computer?

**Answer:**

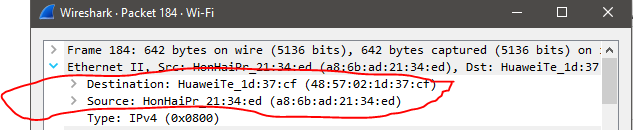


The server (destination) ip address is 128.119.245.12 and the computer (source) ip address is 192.168.18.9

**7.**

What is the MAC address of the server and your computer?

**Answer:**

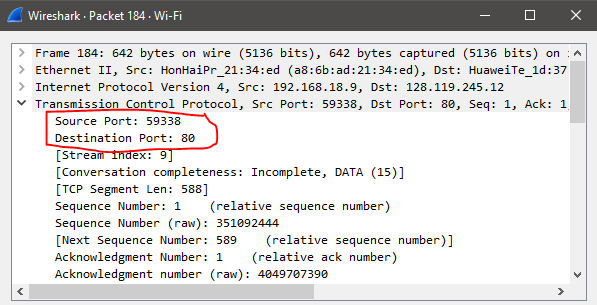


The server (destination) MAC address is (48:57:02:1d:37:cf) and the computer (source) MAC address is (a8:6b:ad:21:34:ed)

**8.**

What is sending and receiving Port Number? What does Port No. 80 represents

**Answer:**

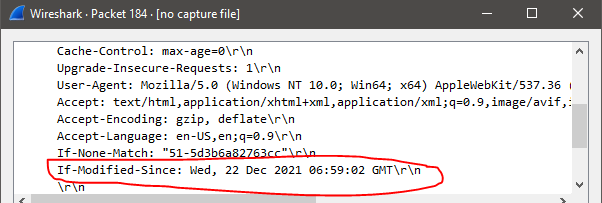


The sending port is 59338 of my computer and the receiving port is 80 of the server. Port 80 represents HTTP protocol port that fixed for it.

**9.**

When was the HTML file, that you are retrieving, last modified at the server?

**Answer:**

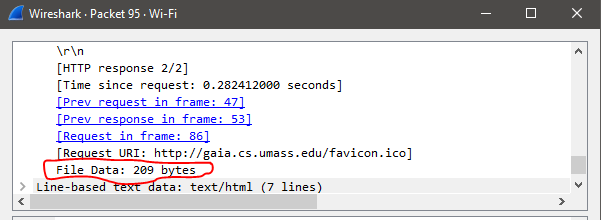


The last modified at the server was Wednesday, 22 December 2021 06:59:02 GMT.

**10.**

How many bytes of total packet content are being returned to your browser?

**Answer:**



209 bytes of total packet content are being returned to our browser.

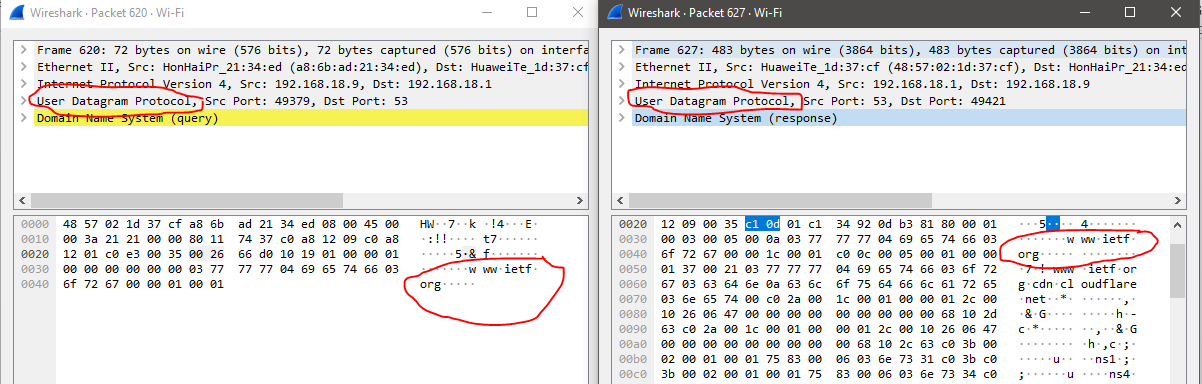
**Task-02**

**Tracing DNS with Wireshark.**

**1.**

Locate the DNS query and response messages. Are they sent over UDP or TCP?

**Answer:**

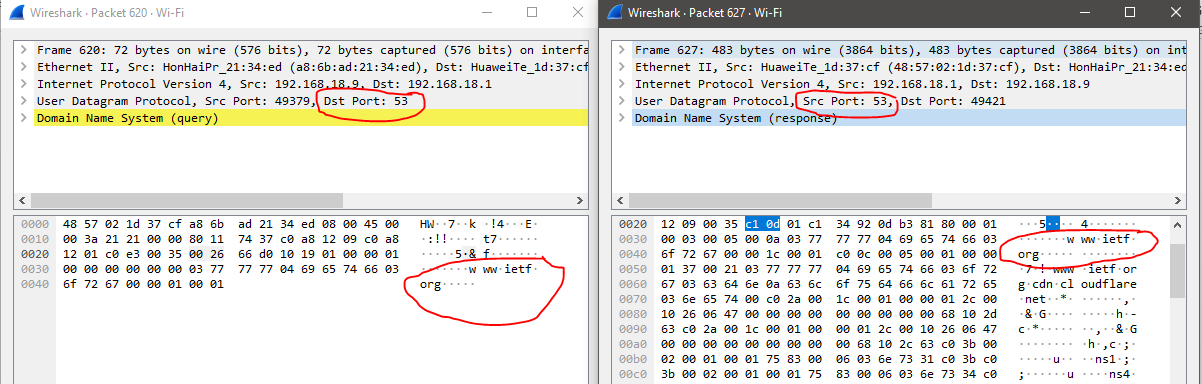


Both request and response messages of the DNS Query are sent over UDP protocol.

**2.**

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

**Answer:**

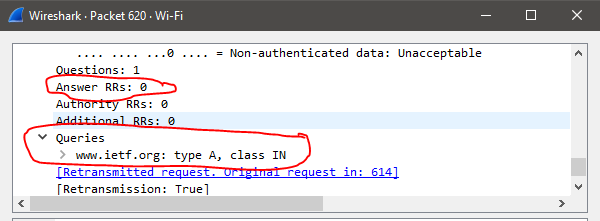


The destination port of DNS query message is 53 and the source port of the DNS response message is also 53.

**3.**

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

**Answer:**

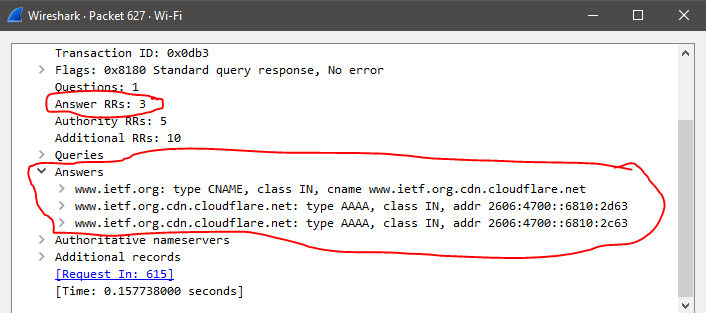


The DNS Query message is of Type A and the query message has no answers as there are zero resource records for answers.

**4.**

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

**Answer:**



The DNS response message contains 3 answers.

1.CNAME RR of [www.ietf.org](http://www.ietf.org)

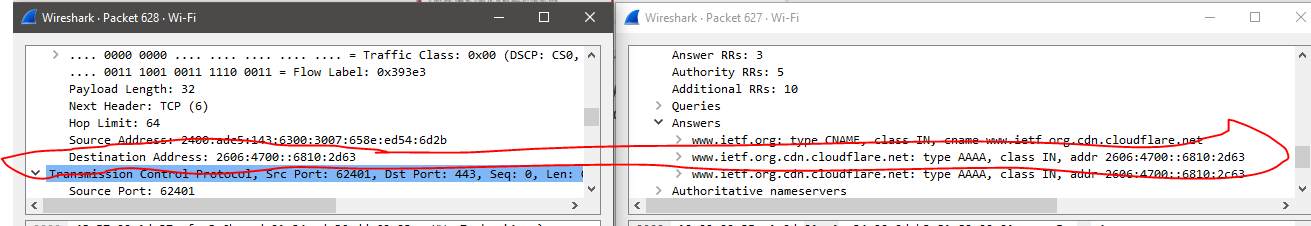
2.Type A RR of [www.ietf.org](http://www.ietf.org) authoritative DNS Server one.

3.Type A RR of [www.ietf.org](http://www.ietf.org) authoritative Server two.

**5.**

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?

**Answer:**



The destination ip address of the SYN packet is the same address that was provided in the DNS response message as the type “A” address of the webpage.