CS 408 Homework 3

Oytun Kuday Duran 28357

1. What is the IP address of http://www.columbia.edu/~fdc/sample.html website?

128.59.105.24 is the destination address while 192.168.1.104 is my ipv4 address (We can check from cmd using ipconfig.) I filtered for http requests and checked which of the requests have Hypertext Transfer Protocol to Columbia website.

2. What are the source port and destination port of the HTTP request to

http://www.columbia.edu/~fdc/sample.html ?

Src Port: 51835, Dst Port 80. I filtered for http on wireshark and then found my request for website. By double clicking on wireshark, we can see detailed information.

3. What is the IP address of example.com domain?

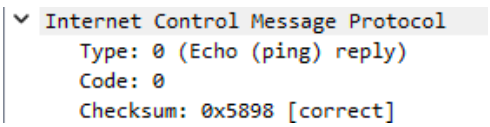
93.184.216.34. Ip address can be seen on cmd when we are pinging. I filtered for ICMP on wireshark to doublecheck.

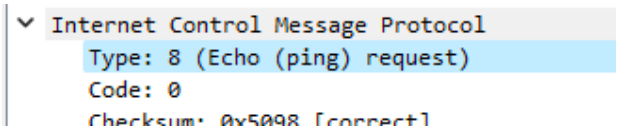
4. What is the IP address of your default gateway?

192.168.1.1 which is different from my ipv4. Found by typing ipconfig to cmd.

5. What are the type numbers of your ICMP Echo request and ICMP Echo reply?

By filtering for icmp on wireshark, I found all “ping”s. From what I observed, the type number is 0 for reply and 8 for the request as you can see below.





6. What is the length of the Data field of ICMP Echo reply packet from “example.com”?

```
Data (32 bytes)
    Data: 6162636465666768696a6b6c6d6e6f707172737475767761626364656667686 9
    [Length: 32]
```

As we double click fort he icmp protocols containing same ip adress as we saw in cmd (Which is of example.com) We always see that in data field, length is 32 similar to that we send 32 bytes of data while pinging. Also, 74 bytes captured. Picture included above.

7. Write a Wireshark filter for showing packets with destination IP address 192.168.19.15 and destination port 5656?

ip.dst == 192.168.19.15 && tcp.dstport == 5656

(I am not sure here whether we should use udp.dstport or tcp.dstport, but in slides it is tcp so I used it.)

8. What is the Target IP Address of your ARP Request packet?

```
Opcode: request (1)
Sender MAC address: IntelCor_7e:8a:9c (14:18:c3:7e:8a:9c)
Sender IP address: 192.168.1.104
Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
Target IP address: 192.168.1.106
```

192.168.1.106 while sender ip address is my ipv4 address.

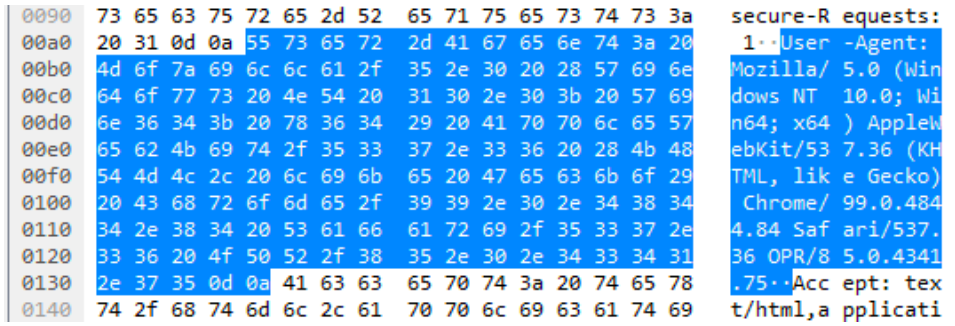
I simply filtered for arp on wireshark. Then checked which ones are requests. There are other ARP Requests too as you can see below. There are some other requests that having my default gateway (192.168.1.1) as sender and my ipv4 address (192.168.1.104) as target ip address. The other combinations can also be seen. In info part, we see that it also informs the connection between MAC address, default gateway and ipv4 address.

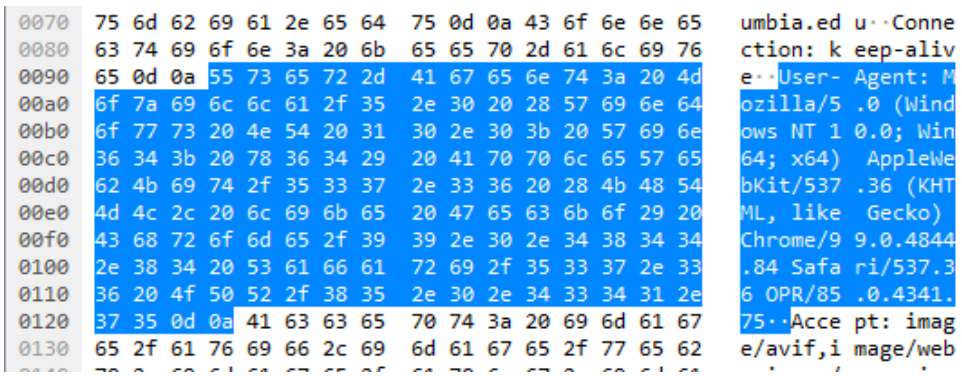
No.	Time	Source	Destination	Protocol	Length	Info
34	4.581717	IntelCor_7e:8a:9c	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.104
35	4.584328	HuaweiDe_dd:a4:01	IntelCor_7e:8a:9c	ARP	42	192.168.1.1 is at 10:32:7e:dd:a4:01
38	5.107874	IntelCor_7e:8a:9c	Broadcast	ARP	42	Who has 192.168.1.106? Tell 192.168.1.104
39	5.118575	BeijingX_13:2a:95	IntelCor_7e:8a:9c	ARP	42	192.168.1.106 is at 8c:5a:f8:13:2a:95
471	33.105915	HuaweiDe_dd:a4:01	IntelCor_7e:8a:9c	ARP	42	Who has 192.168.1.104? Tell 192.168.1.1
472	33.105930	IntelCor_7e:8a:9c	HuaweiDe_dd:a4:01	ARP	42	192.168.1.104 is at 14:18:c3:7e:8a:9c
26327	76.756355	HuaweiDe_dd:a4:01	IntelCor_7e:8a:9c	ARP	42	Who has 192.168.1.104? Tell 192.168.1.1
26328	76.756398	IntelCor_7e:8a:9c	HuaweiDe_dd:a4:01	ARP	42	192.168.1.104 is at 14:18:c3:7e:8a:9c
26736	120.386834	HuaweiDe_dd:a4:01	IntelCor_7e:8a:9c	ARP	42	Who has 192.168.1.104? Tell 192.168.1.1
26737	120.386849	IntelCor_7e:8a:9c	HuaweiDe_dd:a4:01	ARP	42	192.168.1.104 is at 14:18:c3:7e:8a:9c
28013	163.997273	HuaweiDe_dd:a4:01	IntelCor_7e:8a:9c	ARP	42	Who has 192.168.1.104? Tell 192.168.1.1
28014	163.997288	IntelCor_7e:8a:9c	HuaweiDe_dd:a4:01	ARP	42	192.168.1.104 is at 14:18:c3:7e:8a:9c

9. What is the value of the User-Agent header field of HTTP requests sent by your browser?

I filtered for http on wireshark. Then checked my requests. They have User-Agent fields that are all identical. For you to see, I am including samples from 2 different requests below.

In addition, I observed that from a windowsupdate that showed up in wireshark, it doesn't have a user-agent part since it's not requested by a browser.

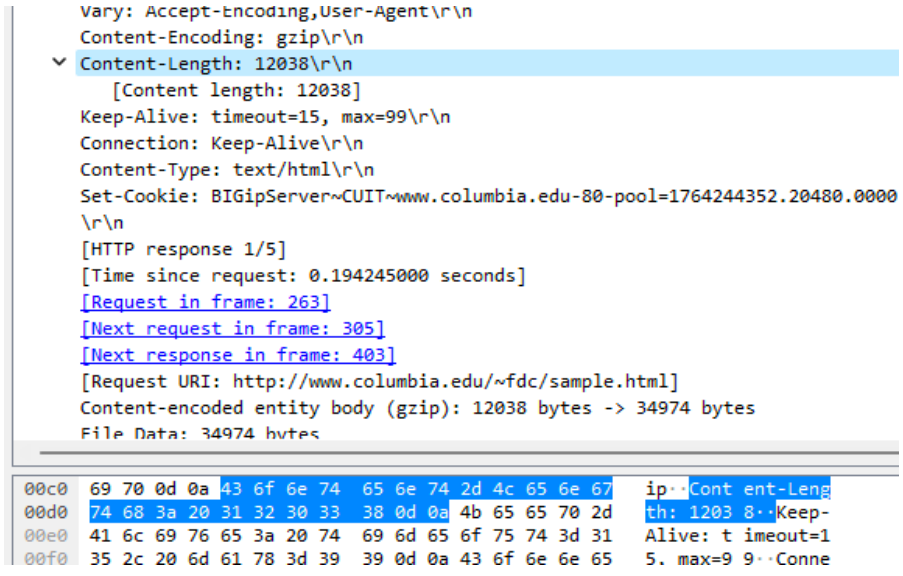




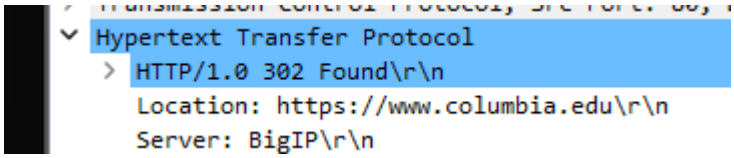
10. What is the Content-Length header field of HTTP response for

"http://www.columbia.edu/~fdc/sample.html"?

I simply filtered for http requests on wireshark. The ones with status codes are responses. I found which one is regarding to the website and in details, we can see content length header field as you can see below. The content length is also 12038.

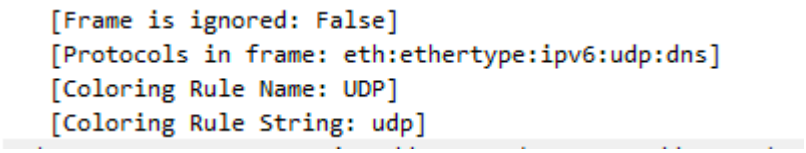


11. What is the HTTP Status Code of HTTP response for "http://www.columbia.edu" ?



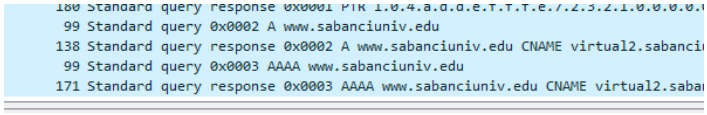
302 Found for the response to first requests (And 200 ok for later images/icons from website). I simply filtered for http protocols and checked which ones have my ip address as destination. We can also see URL's and locations to find which one is regarding to website.

12. Locate the DNS query and response messages for "www.sabanciuniv.edu". Are they sent over UDP or TCP?

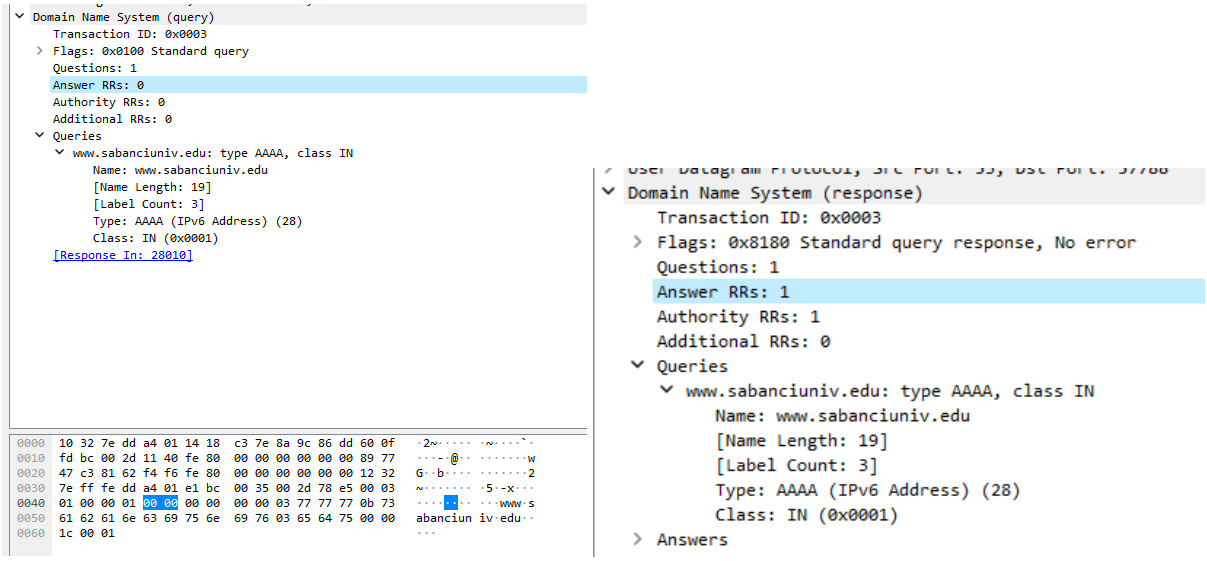


UDP. I filtered for dns on wireshark then looked fort he ones regarding to www.sabanciuniv.edu. Both standard query and standard quest response ones are sent over UDP as you can see from the screenshot above.

13. Examine the DNS query message for "www.sabanciuniv.edu". What "Type" of DNS query is it? Does the query message contain any "answers"?



As you can see from the screenshots above, there are both A(Host address or IPv4) and AAAA(IPv6 address) type standard queries for www.sabanciuniv.edu. They don't contain any answers but questions as you can see below. However, the response DNS queries both contain Questions and Answers (right screenshot). A response DNS query's type matches with its request(or the one that we send) DNS query type.



14. Examine the DNS response message. How many "answers" are provided for IPv4? If you obtain more than one answer, what do each of these answers contain, what is the data length of the answers?

Some of the responses have 1 while some of the responses have more than 1 answers. I could only find 2 response queries from sabanciuniv on wireshark. Data length of CNAME type is 11 while of type A (IPv4 or Host Address) is 4. One of these have 1 answer for type A (IPv4) while other one has none. Content of the answers can be seen from the screenshots below (Name, Type, Class, Lifespan, Data length, and Address regarding to its type).