

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 ping. 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.

```
▼ Internet Control Message Protocol
  Type: 0 (Echo (ping) reply)
  Code: 0
  Checksum: 0x5898 [correct]

▼ Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0
  Checksum: 0x5098 [correct]
```

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

[Response: 32 bytes]

 Data (32 bytes)

 Data: 6162636465666768696a6b6c6d6e6f7071727374757677616263646566676869

 [Length: 32]

As we double click for the icmp protocols containing same ip address 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?

PROTOCOL SIZE: 4

 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.

0090	73 65 63 75 72 65 2d 52 65 71 75 65 73 74 73 3a	secure-R equests:
00a0	20 31 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20	1--User -Agent:
00b0	4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 57 69 6e	Mozilla/ 5.0 (Win
00c0	64 6f 77 73 20 4e 54 20 31 30 2e 30 3b 20 57 69	dows NT 10.0; Wi
00d0	6e 36 34 3b 20 78 36 34 29 20 41 70 70 6c 65 57	n64; x64) AppleW
00e0	65 62 4b 69 74 2f 35 33 37 2e 33 36 20 28 4b 48	ebKit/53 7.36 (KH
00f0	54 4d 4c 2c 20 6c 69 6b 65 20 47 65 63 6b 6f 29	TML, lik e Gecko)
0100	20 43 68 72 6f 6d 65 2f 39 39 2e 30 2e 34 38 34	Chrome/ 99.0.484
0110	34 2e 38 34 20 53 61 66 61 72 69 2f 35 33 37 2e	4.84 Saf ari/537.
0120	33 36 20 4f 50 52 2f 38 35 2e 30 2e 34 33 34 31	36 OPR/8 5.0.4341
0130	2e 37 35 0d 0a 41 63 63 65 70 74 3a 20 74 65 78	.75--Acc ept: tex
0140	74 2f 68 74 6d 6c 2c 61 70 70 6c 69 63 61 74 69	t/html,a pplicati

0070	75 6d 62 69 61 2e 65 64 75 0d 0a 43 6f 6e 6e 65	umbia.ed u--Conne
0080	63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76	ction: k eep-aliv
0090	65 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d	e--User- Agent: M
00a0	6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 57 69 6e 64	ozilla/5 .0 (Wind
00b0	6f 77 73 20 4e 54 20 31 30 2e 30 3b 20 57 69 6e	ows NT 1 0.0; Win
00c0	36 34 3b 20 78 36 34 29 20 41 70 70 6c 65 57 65	64; x64) AppleWe
00d0	62 4b 69 74 2f 35 33 37 2e 33 36 20 28 4b 48 54	bKit/537 .36 (KHT
00e0	4d 4c 2c 20 6c 69 6b 65 20 47 65 63 6b 6f 29 20	ML, like Gecko)
00f0	43 68 72 6f 6d 65 2f 39 39 2e 30 2e 34 38 34 34	Chrome/9 9.0.4844
0100	2e 38 34 20 53 61 66 61 72 69 2f 35 33 37 2e 33	.84 Safa ri/537.3
0110	36 20 4f 50 52 2f 38 35 2e 30 2e 34 33 34 31 2e	6 OPR/85 .0.4341.
0120	37 35 0d 0a 41 63 63 65 70 74 3a 20 69 6d 61 67	75--Acce pt: imag
0130	65 2f 61 76 69 66 2c 69 6d 61 67 65 2f 77 65 62	e/avif,i mage/web

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

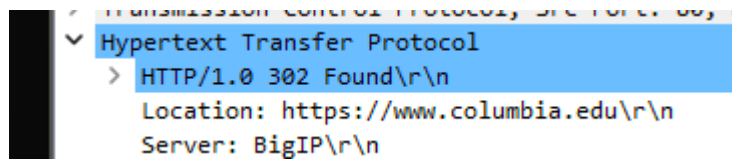
“http://www.columbia.edu/~fdc/sample.html”?

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.

	Vary: Accept-Encoding,User-Agent\r\n	
	Content-Encoding: gzip\r\n	
▼	Content-Length: 12038\r\n	
	[Content length: 12038]	
	Keep-Alive: timeout=15, max=99\r\n	
	Connection: Keep-Alive\r\n	
	Content-Type: text/html\r\n	
	Set-Cookie: BIGipServer~CUIT~www.columbia.edu-80-pool=1764244352.20480.0000\r\n	
	[HTTP response 1/5]	
	[Time since request: 0.194245000 seconds]	
	[Request in frame: 263]	
	[Next request in frame: 305]	
	[Next response in frame: 403]	
	[Request URI: http://www.columbia.edu/~fdc/sample.html]	
	Content-encoded entity body (gzip): 12038 bytes -> 34974 bytes	
	File Data: 34974 bytes	

00c0	69 70 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67	ip--Cont ent-Leng
00d0	74 68 3a 20 31 32 30 33 38 0d 0a 4b 65 65 70 2d	th: 1203 8--Keep-
00e0	41 6c 69 76 65 3a 20 74 69 6d 65 6f 75 74 3d 31	Alive: t imeout=1
00f0	35 2c 20 6d 61 78 3d 39 39 0d 0a 43 6f 6e 6e 65	5. max=9 9--Conne

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?

```
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ipv6:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
```

UDP. I filtered for dns on wireshark then looked for the ones regarding to www.sabanciuniv.edu. Both standard query and standard query 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”?

```
180 Standard query response 0x0001 Pk 1.0.4.a.d.d.e.T.T.E./2.3.2.1.0.0.0.1
99 Standard query 0x0002 A www.sabanciuniv.edu
138 Standard query response 0x0002 A www.sabanciuniv.edu CNAME virtual2.sabanci
99 Standard query 0x0003 AAAA www.sabanciuniv.edu
171 Standard query response 0x0003 AAAA www.sabanciuniv.edu CNAME virtual2.sabai
```

As you can see from the screenshots above, there are both A(Host address or IPv4 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.

Domain Name System (query)
Transaction ID: 0x0003
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
www.sabanciuniv.edu: type AAAA, class IN
Name: www.sabanciuniv.edu
[Name Length: 19]
[Label Count: 3]
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)
[Response In: 28010]

User Datagram Protocol, Src Port: 55, Dst Port: 57780
Domain Name System (response)
Transaction ID: 0x0003
Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 1
Authority RRs: 1
Additional RRs: 0
Queries
www.sabanciuniv.edu: type AAAA, class IN
Name: www.sabanciuniv.edu
[Name Length: 19]
[Label Count: 3]
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)
Answers

0000 10 32 7e dd a4 01 14 18 c3 7e 8a 9c 86 dd 60 0f2.....w
0010 fd bc 00 2d 11 40 fe 00 00 00 00 00 00 09 77@.....w
0020 47 c3 81 62 f4 f6 fe 00 00 00 00 00 00 12 32 G..b.....2
0030 7e ff fe dd a4 01 e1 bc 00 35 00 2d 78 e5 00 035-X...
0040 01 00 00 01 00 00 00 00 00 03 77 77 77 0b 73www.s
0050 61 62 61 6e 63 69 75 6e 69 76 03 65 64 75 00 00 abanciuniv.edu..
0060 1c 00 01

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).

Answers
www.sabanciuniv.edu: type CNAME, class IN, cname virtual2.sabanciuniv.edu
Name: www.sabanciuniv.edu
Type: CNAME (Canonical NAME for an alias) (5)
Class: IN (0x0001)
Time to live: 300 (5 minutes)
Data length: 11
CNAME: virtual2.sabanciuniv.edu
virtual2.sabanciuniv.edu: type A, class IN, addr 159.20.64.46
Name: virtual2.sabanciuniv.edu
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 62 (1 minute, 2 seconds)
Data length: 4
Address: 159.20.64.46
[Request In: 28007]
[Time: 0.058527000 seconds]

0000 14 18 c3 7e 8a 9c 10 32 7e dd a4 01 86 dd 60 082.....
0010 bc 42 00 54 11 40 fe 00 00 00 00 00 00 12 32 .B.T.@.....2
0020 7e ff fe dd a4 01 fe 00 00 00 00 00 00 08 77w
0030 47 c3 81 62 f4 f6 00 35 e1 bb 00 54 b9 c9 00 02 G..b.....5...T...
0040 81 80 00 01 00 02 00 00 00 00 03 77 77 77 0b 73www.s
0050 61 62 61 6e 63 69 75 6e 69 76 03 65 64 75 00 00 abanciuniv.edu..
0060 01 00 01 c0 0c 00 05 00 01 00 00 01 2c 00 0b 081.....
0070 76 69 72 74 75 61 6c 32 c0 10 c0 31 00 01 00 01 virtual2...1....
0080 00 00 00 3e 00 04 9f 14 40 2e@.

Answers
www.sabanciuniv.edu: type CNAME, class IN, cname virtual2.sabanciuniv.edu
Name: www.sabanciuniv.edu
Type: CNAME (Canonical NAME for an alias) (5)
Class: IN (0x0001)
Time to live: 300 (5 minutes)
Data length: 11
CNAME: virtual2.sabanciuniv.edu