Barret Jackson
66122573
October 2, 2020

COSC 328 Lab 2

1) SSL (and TSL) operates at the application layer. In order to implement it, a developer invokes an SSL (or TSL) library in both the client and server codebases. The client side will take clear text arguments, a password for example, and pass it to the SSL socket. The SSL socket will encrypt the data, send it to the server, then the server will use SSL code to decrypt the message.

2) The TCP requires a socket on the server side to handle the handshake from the client, then all the data received from the client is routed to the connection socket. UDP does not require a handshake between client and server, so the data is sent directly to the server socket from the client socket. For a TCP server with n simultaneous connections, the server will require one handshake or welcome socket plus n connection sockets, so n+1 sockets in total.

3) *a)* The average time to send an object over the access link is given by
$\Delta = L/R = 850{,}000\text{bits}/15{,}000{,}000 \text{ bps} = 0.0567 \text{ s}$
This means the average access delay is given by
$\Delta/(1-\Delta\beta) = 0.0567\text{s}/(1-0.0567\text{s} * 16 \text{ requests/s}) = 0.607 \text{ s/request}$
The average time from the router on the internet side of the access link to a given server is 3 s, so the total access delay is given by
0.607 s + 3 s = 3.607 s

b) If 60% of the requests are satisfied by the cache, this means overal traffic intensity is reduced by 60% as well. The average access delay will decrease as such:
$\Delta/(1-0.4\Delta\beta) + 3 \text{ s} = 0.0567\text{s}/(1-0.4*0.0567\text{s} * 16 \text{ requests/s}) + 3 \text{ s} = 3.889 \text{ s/request}$
Cached responses happen near instantaneously, at a frequency of 60%. The requests that actually access the internet occur 40% of the time, so the total response time is given by
0.6 * 0 s + 0.4 * 3.889 s = 1.236 s
a significant improvement over the 3.607 uncached response time.

4)

Distribution	F	u_s	d_i	u	N	D
Client-server	15 Gbits	30 Mbps	2 Mbps	300 Kbps	10	7680s
Client-server	15 Gbits	30 Mbps	2 Mbps	300 Kbps	1000	512,000s
Client-server	15 Gbits	30 Mbps	2 Mbps	2 Mbps	10	7680s
Client-server	15 Gbits	30 Mbps	2 Mbps	2 Mbps	1000	512,000s
P2P	15 Gbits	30 Mbps	2 Mbps	300 Kbps	10	7680s
P2P	15 Gbits	30 Mbps	2 Mbps	300 Kbps	1000	47558.78s
P2P	15 Gbits	30 Mbps	2 Mbps	2 Mbps	10	7680s
P2P	15 Gbits	30 Mbps	2 Mbps	2 Mbps	1000	7680s

For client-server distribution, the time to distribute a file of size F to N clients is given by
$D_{c\text{-}s} >= \max\{NF/u_s, F/d_{min}\}$
So the upload rate of peers u is irrelevant, and as an example, the total time to download for 10 clients is given by

$D_{c\text{-}s}$ >= max{NF/u_s, F/d_{min}} = max{10*15Gbit/30Mbps, 15Gbit/2Mbps}
= max{10*15*1024 Mbit/30Mbps, 15 * 1024 Gbit / 2 Mbps} = max{5120s, 7680s}
= 7680s = 2 hr 8 min
and similarly for the other three rows.
max{512,000s, 7680s}

For peer-to-peer distribution, the time is given by
D_{P2P} >= max{F/u_s, F/d_{min}, $NF/(u_s + \Sigma u)$}
As an example, the first row in the P2P table is calculated as:
D_{P2P} >= max{F/u_s, F/d_{min}, $NF/(u_s + \Sigma u)$}
= max{15Gbit/30Mbps, 15Gbit/2Mbps, 10*15Gbit/(30Mbps + 10*300Kbps)}
= max{15*1024Mbit/30Mbps, 15*1024Mbit/2Mbps, 10*15*1024Mbit/(30Mbps + 10*300/1024Mbps)}
= max{512s, 7680s, 4664.48s} = 7680 s = 2 hr 8 min
and similarly for the other three rows.
max{512s, 7680s, 47,558.78s}   max{512s, 7680s, 3072s}   max{512s, 7680s, 7566.50}

5) *a)* TCP   *b)* UDP   *c)* UDP   *d)* UDP   *e)* TCP   *f)* UDP

6) *a)* localhost/index.html
b) The browser is requesting a persistent connection; the Connection field of the request header indicates Keep-Alive, meaning keep the connection open until it times out.

7) *a)* Using non-persistent connections, the order of connections is as such:
i) Client initiates TCP connection
ii) Server acknowledges connection
iii) Client requests HTML document
iv) Server acknowledges requests and begins sending HTML document
v) Client receives HTML document
vi) Server closes connection
vii) Client unpacks HTML document, sees reference to four image files
viii) Client repeats above for all four images
This means each object will involve two TCP connections and the file transfer time, so the total time is given by:
t_{tot} = 0.1 s * 2 * 5 + 10,000bit / 10 * 1024^2 bps + 4 * 50,000bit / 10 * 1024^2 bps = 1.02 s

b) If the browser is able to open any number of parallel connections, the first step to obtain the HTML remains the same, but then all four images can be obtained concurrently. Hence
t_{tot} = 0.1 s * 2 * 2 + 10,000bit / 10 * 1024^2 bps + 50,000bit / 10 * 1024^2 bps = 0.406 s

c) In a persistent connection with no pipelining and parallel connections, the client will require two RTT to initiate the TCP handshake with server 1, then transfer the HTML document, see the references to the images, begin the transfer of the three images from server 1 while concurrently setting up a TCP handshake with server 2 and transferring the image file from there. In other words, four RTT times will be necessary plus the HTML file transfer and one image transfer time, or
t_{tot} = 0.1 s * 2 * 2 + 10,000bit / 10 * 1024^2 bps + 50,000bit / 10 * 1024^2 bps = 0.406 s

This is effectively the same result as a non-persistent connection with concurrency. However, with pipelining, the client will request the images as it encounters a reference to them in the HTML document. Unless the image on server 2 is at the very end of the HTML document, this means the TCP handshake will occur some time during the HTML document transfer. Assuming the image on server 2 is referenced at the very beginning of the HTML file, it will effectively negate the transfer time of the html file, or
$t_{tot} = 0.1\text{ s} * 2 * 2 + 50{,}000\text{bit} / 10 * 1024^2\text{ bps} = 0.405\text{ s}$
which is the fastest of the four options (although only by one ms).

8) *a)*

Time (ms)	Request type	Details
0	HTTP GET	m1.a.com performs a HTTP GET for the file at www.b.com. Message sent to local HTTP cache (based on question assumptions, no time taken)
~0	DNS REQUEST	m1.a.com performs a DNS REQUEST to obtain the IP for www.b.com from its local DNS server, since the local cache did not have the address. No time based on assumptions.
~0	DNS REQUEST	Local DNS server does not have the entry cached, requests from root-level DNS
50	DNS RESPONSE	DNS REQUEST arrives at root-level server, sends back DNS RESPONSE with top level domain (TLD)
100	DNS REQUEST	Local DNS receives the root-level DNS response, sends a DNS REQUEST to the TLD DNS
150	DNS RESPONSE	TLD DNS receives the request and send a response containing the authoritative DNS
200	DNS REQUEST	The local DNS receives the reply with the authoritative DNS, sends DNS REQUEST to authoritative DNS (25 ms to get to www.b.com servers)
225	DNS RESPONSE	Authoritative DNS in www.b.com domain receives the request and sends a DNS RESPONSE with the A record for www.b.com
250	DNS RESPONSE	DNS RESPONSE received by local DNS and forwarded to HTTP cache
~250	HTTP GET (TCP handshake init)	Local HTTP cache initiates TCP handshake with www.b.com for the file, requiring one RTT before the request can be sent
300	HTTP GET (SENT)	Local HTTP performs HTTP GET to www.b.com for the file
350	HTTP RESPONSE	www.b.com responds with the document, begins transmitting. t = 10 ms (b LAN) + 1000 ms (on 1 Mbps link) + 100 ms (a LAN) = 1110 ms
1460	HTTP RESPONSE	Local HTTP cache sends HTTP RESPONSE to m1.a.com, taking 100 ms to transmit
1560	None	File has arrived in full to m1.a.com

b)

Time (ms)	Request type	Details
0	HTTP GET	m2.a.com performs a HTTP GET for the file at www.b.com. Message sent to local HTTP cache (based on question assumptions, no time taken)
~0	HTTP GET	Local HTTP cache has a copy of the file and the IP address for www.b.com Sends HTTP conditional GET to www.b.com
75	HTTP RESPONSE	www.b.com receives the request and responds that the file is unchanged, and that it will not be transmitted.
100	HTTP RESPONSE	Local cache receives the message that the file from www.b.com is unchanged, sends HTTP RESPONSE with the file to m2.a.com t = 100 ms
200	None	File has arrived in full to m2.a.com

WIRESHARK LAB!!!!!

1.

```
nslookup en.whu.edu.cn
Server:         137.82.1.2
Address:        137.82.1.2#53

Non-authoritative answer:
Name: en.WHU.edu.cn
Address: 202.114.64.200
Name: en.WHU.edu.cn
Address: 2001:250:4001:1::1001
```

2.

```
nslookup -type=NS home.cern
Server:         137.82.1.2
Address:        137.82.1.2#53

Non-authoritative answer:
home.cern       nameserver = ext-dns-1.cern.ch.
home.cern       nameserver = ext-dns-2.cern.ch.

Authoritative answers can be found from:
ext-dns-2.cern.ch       internet address = 192.91.245.85
ext-dns-2.cern.ch       has AAAA address 2001:1458:1:2::100:85
```

3. Using the CERN DNS server gave no response

```
nslookup mail.yahoo.com ext-dns-1.cern.ch
Server:         ext-dns-1.cern.ch
Address:        192.65.187.5#53

** server can't find mail.yahoo.com: REFUSED
```

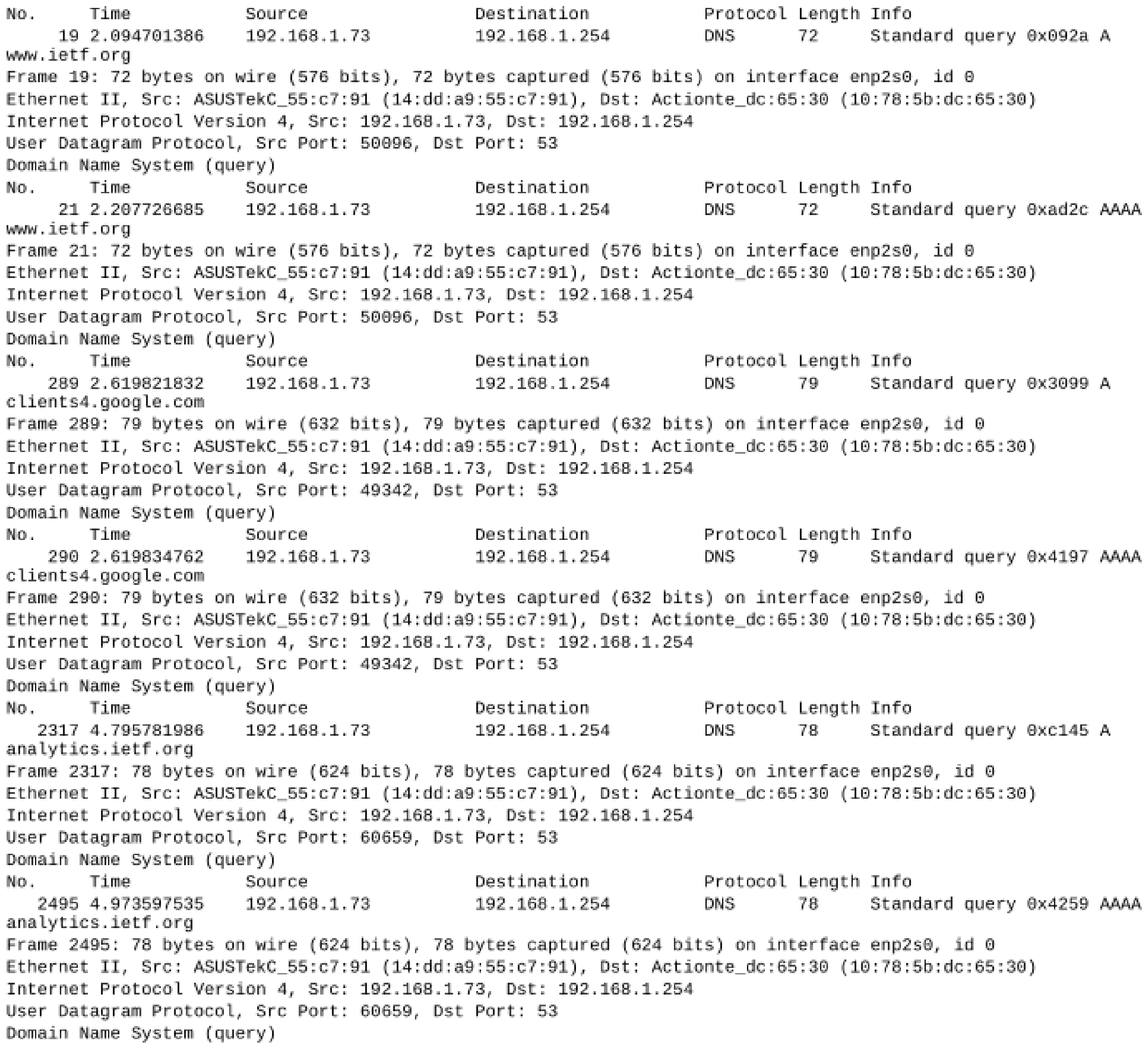
I tried again with DNS server 1.1.1.1 and got a response

```
nslookup mail.yahoo.com 1.1.1.1
Server:         1.1.1.1
Address:        1.1.1.1#53

Non-authoritative answer:
mail.yahoo.com      canonical name = edge.gycpi.b.yahoodns.net.
Name: edge.gycpi.b.yahoodns.net
Address: 69.147.80.15
Name: edge.gycpi.b.yahoodns.net
Address: 69.147.80.12
Name: edge.gycpi.b.yahoodns.net
Address: 2001:4998:64:800::6000
Name: edge.gycpi.b.yahoodns.net
Address: 2001:4998:64:800::6001
```

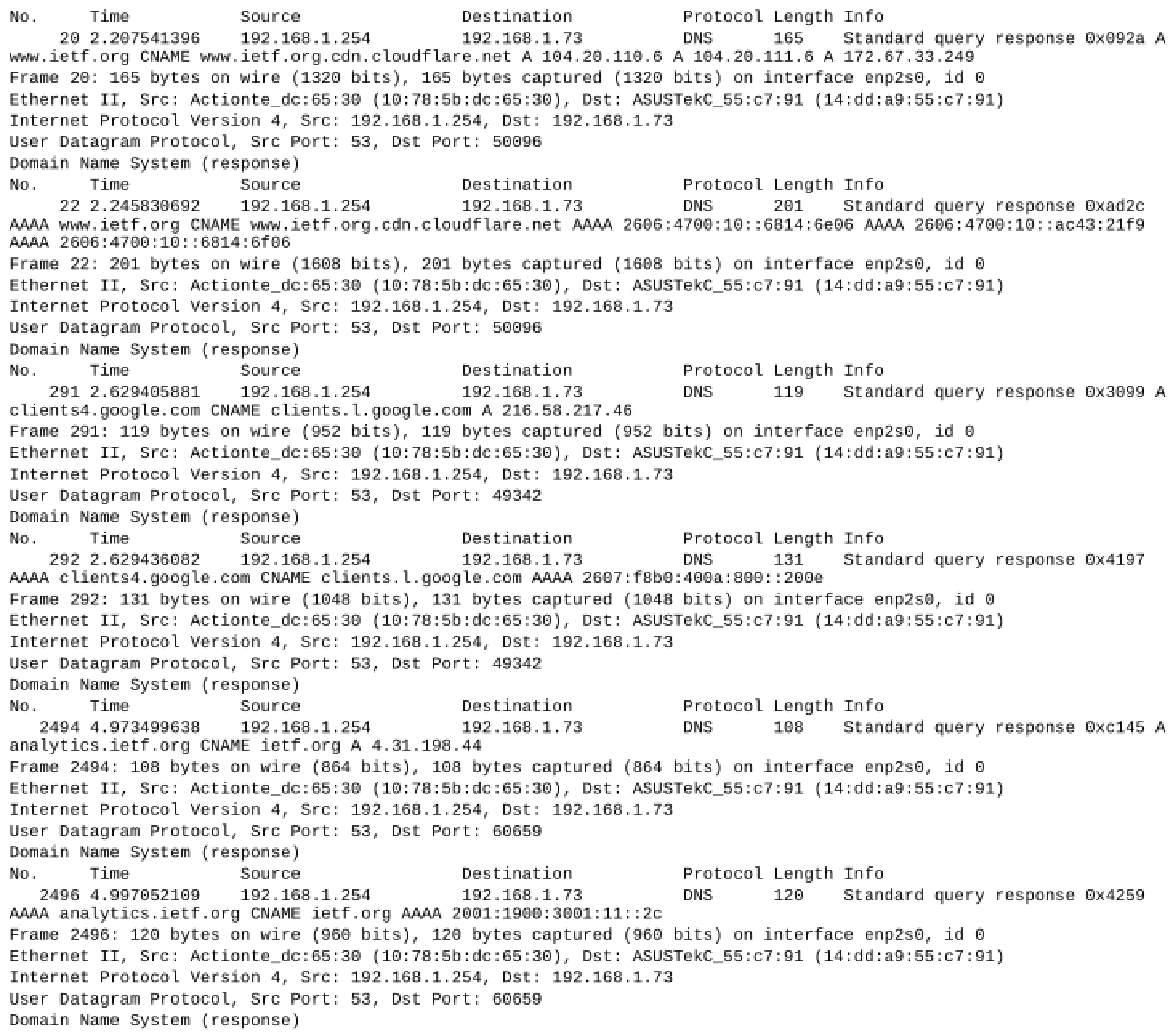
4. Wireshark setup: I’m running Wireshark on Arch Linux, and as far as I can tell, Linux does not cache DNS queries (see https://wiki.archlinux.org/index.php/Domain_name_resolution for further details). I therefore skipped the DNS flush operation.

Here are the captured DNS queries



```
No.     Time           Source                Destination           Protocol Length Info
     19 2.094701386    192.168.1.73          192.168.1.254         DNS      72     Standard query 0x092a A
www.ietf.org
Frame 19: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface enp2s0, id 0
Ethernet II, Src: ASUSTekC_55:c7:91 (14:dd:a9:55:c7:91), Dst: Actionte_dc:65:30 (10:78:5b:dc:65:30)
Internet Protocol Version 4, Src: 192.168.1.73, Dst: 192.168.1.254
User Datagram Protocol, Src Port: 50096, Dst Port: 53
Domain Name System (query)
No.     Time           Source                Destination           Protocol Length Info
     21 2.207726685    192.168.1.73          192.168.1.254         DNS      72     Standard query 0xad2c AAAA
www.ietf.org
Frame 21: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface enp2s0, id 0
Ethernet II, Src: ASUSTekC_55:c7:91 (14:dd:a9:55:c7:91), Dst: Actionte_dc:65:30 (10:78:5b:dc:65:30)
Internet Protocol Version 4, Src: 192.168.1.73, Dst: 192.168.1.254
User Datagram Protocol, Src Port: 50096, Dst Port: 53
Domain Name System (query)
No.     Time           Source                Destination           Protocol Length Info
    289 2.619821832    192.168.1.73          192.168.1.254         DNS      79     Standard query 0x3099 A
clients4.google.com
Frame 289: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface enp2s0, id 0
Ethernet II, Src: ASUSTekC_55:c7:91 (14:dd:a9:55:c7:91), Dst: Actionte_dc:65:30 (10:78:5b:dc:65:30)
Internet Protocol Version 4, Src: 192.168.1.73, Dst: 192.168.1.254
User Datagram Protocol, Src Port: 49342, Dst Port: 53
Domain Name System (query)
No.     Time           Source                Destination           Protocol Length Info
    290 2.619834762    192.168.1.73          192.168.1.254         DNS      79     Standard query 0x4197 AAAA
clients4.google.com
Frame 290: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface enp2s0, id 0
Ethernet II, Src: ASUSTekC_55:c7:91 (14:dd:a9:55:c7:91), Dst: Actionte_dc:65:30 (10:78:5b:dc:65:30)
Internet Protocol Version 4, Src: 192.168.1.73, Dst: 192.168.1.254
User Datagram Protocol, Src Port: 49342, Dst Port: 53
Domain Name System (query)
No.     Time           Source                Destination           Protocol Length Info
   2317 4.795781986    192.168.1.73          192.168.1.254         DNS      78     Standard query 0xc145 A
analytics.ietf.org
Frame 2317: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface enp2s0, id 0
Ethernet II, Src: ASUSTekC_55:c7:91 (14:dd:a9:55:c7:91), Dst: Actionte_dc:65:30 (10:78:5b:dc:65:30)
Internet Protocol Version 4, Src: 192.168.1.73, Dst: 192.168.1.254
User Datagram Protocol, Src Port: 60659, Dst Port: 53
Domain Name System (query)
No.     Time           Source                Destination           Protocol Length Info
   2495 4.973597535    192.168.1.73          192.168.1.254         DNS      78     Standard query 0x4259 AAAA
analytics.ietf.org
Frame 2495: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface enp2s0, id 0
Ethernet II, Src: ASUSTekC_55:c7:91 (14:dd:a9:55:c7:91), Dst: Actionte_dc:65:30 (10:78:5b:dc:65:30)
Internet Protocol Version 4, Src: 192.168.1.73, Dst: 192.168.1.254
User Datagram Protocol, Src Port: 60659, Dst Port: 53
Domain Name System (query)
```

And here are the captured DNS responses:



```
No.     Time           Source                Destination           Protocol Length Info
     20 2.207541396    192.168.1.254         192.168.1.73          DNS      165    Standard query response 0x092a A
www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.20.110.6 A 104.20.111.6 A 172.67.33.249
Frame 20: 165 bytes on wire (1320 bits), 165 bytes captured (1320 bits) on interface enp2s0, id 0
Ethernet II, Src: Actionte_dc:65:30 (10:78:5b:dc:65:30), Dst: ASUSTekC_55:c7:91 (14:dd:a9:55:c7:91)
Internet Protocol Version 4, Src: 192.168.1.254, Dst: 192.168.1.73
User Datagram Protocol, Src Port: 53, Dst Port: 50096
Domain Name System (response)
No.     Time           Source                Destination           Protocol Length Info
     22 2.245830692    192.168.1.254         192.168.1.73          DNS      201    Standard query response 0xad2c
AAAA www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net AAAA 2606:4700:10::6814:6e06 AAAA 2606:4700:10::ac43:21f9
AAAA 2606:4700:10::6814:6f06
Frame 22: 201 bytes on wire (1608 bits), 201 bytes captured (1608 bits) on interface enp2s0, id 0
Ethernet II, Src: Actionte_dc:65:30 (10:78:5b:dc:65:30), Dst: ASUSTekC_55:c7:91 (14:dd:a9:55:c7:91)
Internet Protocol Version 4, Src: 192.168.1.254, Dst: 192.168.1.73
User Datagram Protocol, Src Port: 53, Dst Port: 50096
Domain Name System (response)
No.     Time           Source                Destination           Protocol Length Info
    291 2.629405881    192.168.1.254         192.168.1.73          DNS      119    Standard query response 0x3099 A
clients4.google.com CNAME clients.l.google.com A 216.58.217.46
Frame 291: 119 bytes on wire (952 bits), 119 bytes captured (952 bits) on interface enp2s0, id 0
Ethernet II, Src: Actionte_dc:65:30 (10:78:5b:dc:65:30), Dst: ASUSTekC_55:c7:91 (14:dd:a9:55:c7:91)
Internet Protocol Version 4, Src: 192.168.1.254, Dst: 192.168.1.73
User Datagram Protocol, Src Port: 53, Dst Port: 49342
Domain Name System (response)
No.     Time           Source                Destination           Protocol Length Info
    292 2.629436082    192.168.1.254         192.168.1.73          DNS      131    Standard query response 0x4197
AAAA clients4.google.com CNAME clients.l.google.com AAAA 2607:f8b0:400a:800::200e
Frame 292: 131 bytes on wire (1048 bits), 131 bytes captured (1048 bits) on interface enp2s0, id 0
Ethernet II, Src: Actionte_dc:65:30 (10:78:5b:dc:65:30), Dst: ASUSTekC_55:c7:91 (14:dd:a9:55:c7:91)
Internet Protocol Version 4, Src: 192.168.1.254, Dst: 192.168.1.73
User Datagram Protocol, Src Port: 53, Dst Port: 49342
Domain Name System (response)
No.     Time           Source                Destination           Protocol Length Info
   2494 4.973499638    192.168.1.254         192.168.1.73          DNS      108    Standard query response 0xc145 A
analytics.ietf.org CNAME ietf.org A 4.31.198.44
Frame 2494: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface enp2s0, id 0
Ethernet II, Src: Actionte_dc:65:30 (10:78:5b:dc:65:30), Dst: ASUSTekC_55:c7:91 (14:dd:a9:55:c7:91)
Internet Protocol Version 4, Src: 192.168.1.254, Dst: 192.168.1.73
User Datagram Protocol, Src Port: 53, Dst Port: 60659
Domain Name System (response)
No.     Time           Source                Destination           Protocol Length Info
   2496 4.997052109    192.168.1.254         192.168.1.73          DNS      120    Standard query response 0x4259
AAAA analytics.ietf.org CNAME ietf.org AAAA 2001:1900:3001:11::2c
Frame 2496: 120 bytes on wire (960 bits), 120 bytes captured (960 bits) on interface enp2s0, id 0
Ethernet II, Src: Actionte_dc:65:30 (10:78:5b:dc:65:30), Dst: ASUSTekC_55:c7:91 (14:dd:a9:55:c7:91)
Internet Protocol Version 4, Src: 192.168.1.254, Dst: 192.168.1.73
User Datagram Protocol, Src Port: 53, Dst Port: 60659
Domain Name System (response)
```

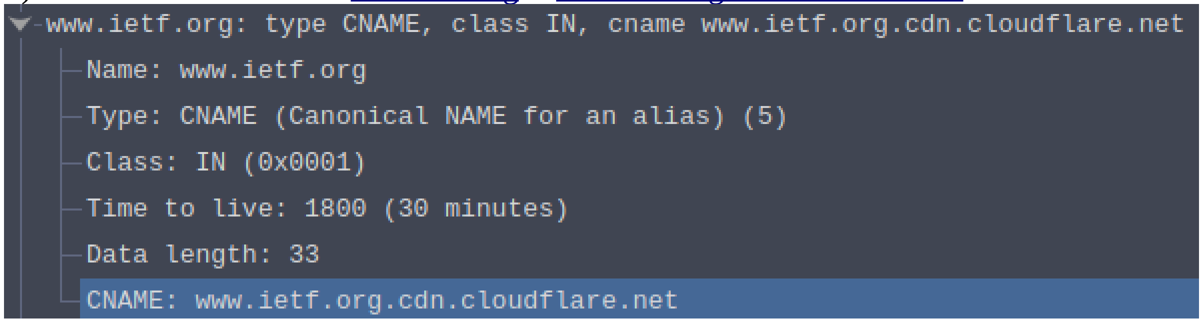
All DNS queries and responses are sent over UDP.

5. The destination port for the DNS queries is the same as the source port for the DNS responses, port 53.

6. The DNS queries are all sent to 192.168.1.254. When running (again, on Linux) cat /etc/resolv.conf, the first nameserver shown is also 192.168.1.254, which is a DNS hosted by Telus (I should really change that…).

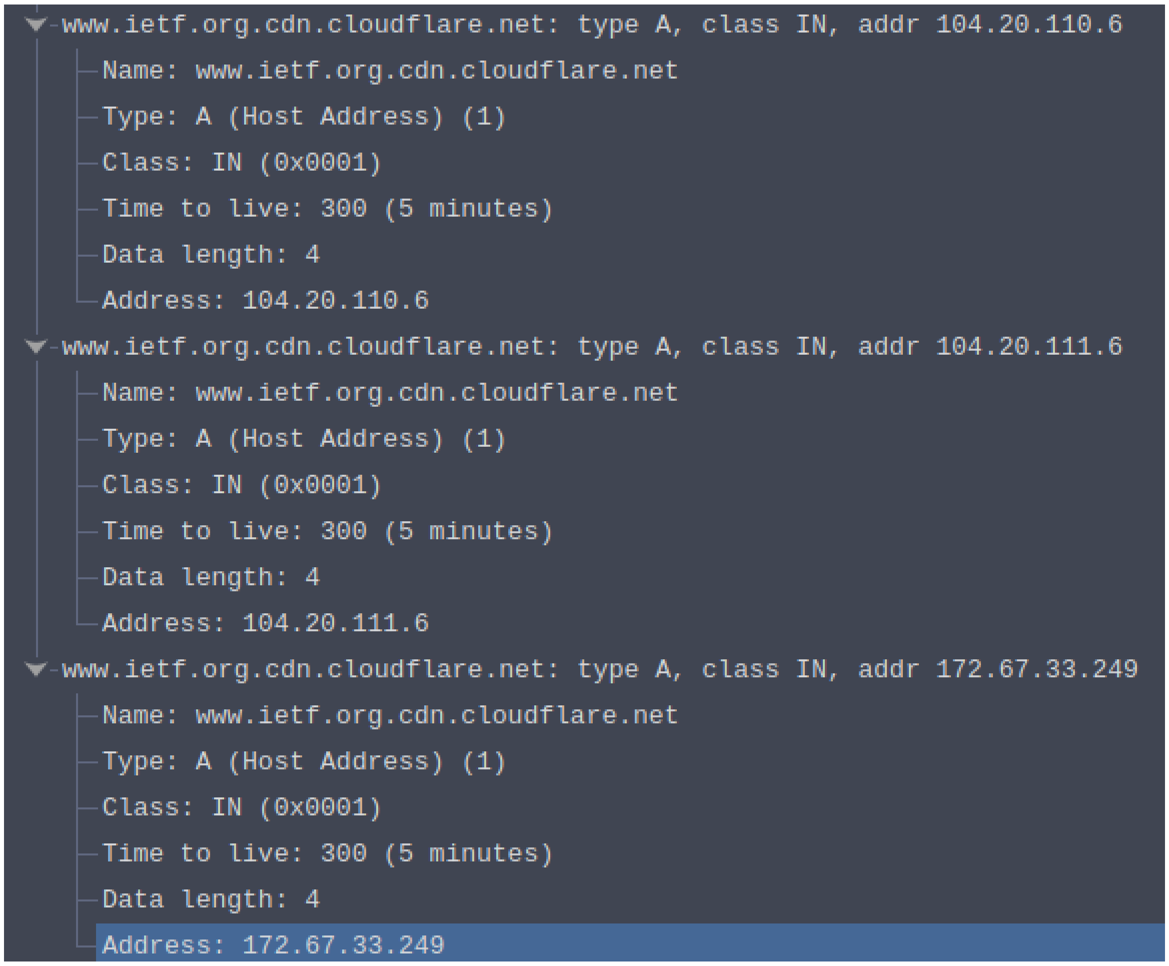
7. I will look at the first DNS query since the others all appear to be advertisers, trackers, etc. This is a standard query, and other than the requested URL, the source information and destination information, the message doesn’t really contain any useful information or answers.

8. The DNS response, on the other hand, contains four answers:
i) The canonical name for www.ietf.org is www.ietf.org.cdn.cloudflare.net



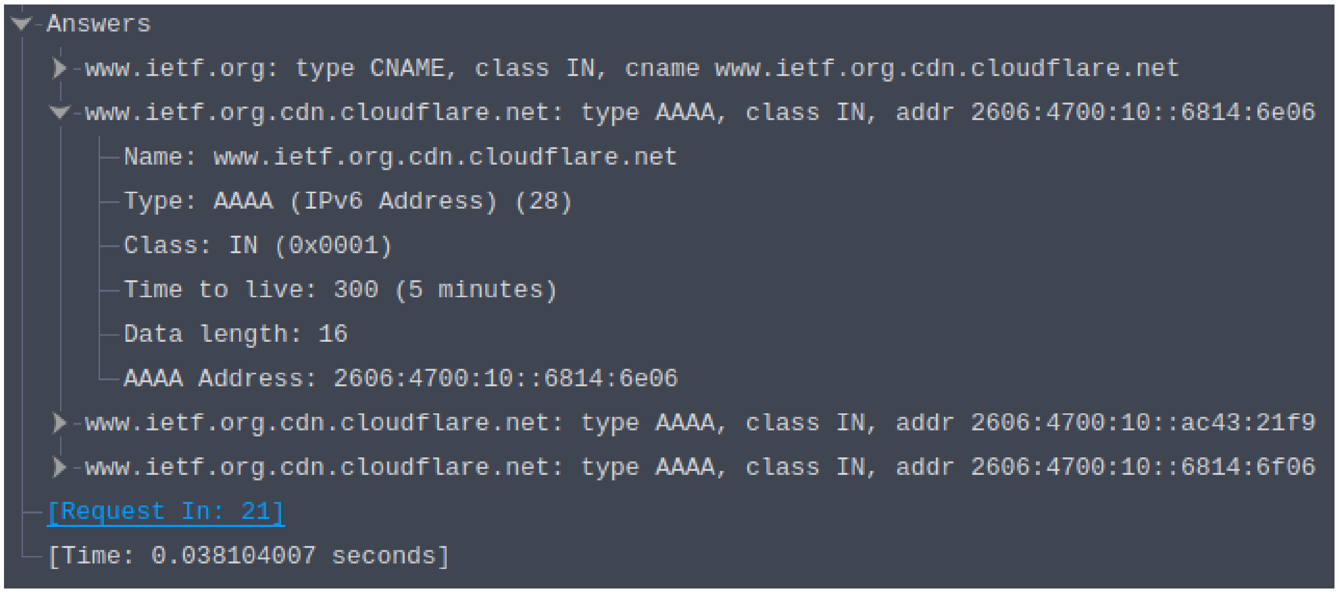
```
▼ www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
    Name: www.ietf.org
    Type: CNAME (Canonical NAME for an alias) (5)
    Class: IN (0x0001)
    Time to live: 1800 (30 minutes)
    Data length: 33
    CNAME: www.ietf.org.cdn.cloudflare.net
```

ii-iv) The next three answers give three separate IP addresses, 104.20.110.6, 104.20.111.6, and 172.67.33.249



```
▼ www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.110.6
    Name: www.ietf.org.cdn.cloudflare.net
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 300 (5 minutes)
    Data length: 4
    Address: 104.20.110.6
▼ www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.111.6
    Name: www.ietf.org.cdn.cloudflare.net
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 300 (5 minutes)
    Data length: 4
    Address: 104.20.111.6
▼ www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 172.67.33.249
    Name: www.ietf.org.cdn.cloudflare.net
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 300 (5 minutes)
    Data length: 4
    Address: 172.67.33.249
```

A subsequent DNS response also gives the canonical name for the site, and returns three different IP addresses in IPV6 format.



```
Answers
  www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
  www.ietf.org.cdn.cloudflare.net: type AAAA, class IN, addr 2606:4700:10::6814:6e06
    Name: www.ietf.org.cdn.cloudflare.net
    Type: AAAA (IPv6 Address) (28)
    Class: IN (0x0001)
    Time to live: 300 (5 minutes)
    Data length: 16
    AAAA Address: 2606:4700:10::6814:6e06
  www.ietf.org.cdn.cloudflare.net: type AAAA, class IN, addr 2606:4700:10::ac43:21f9
  www.ietf.org.cdn.cloudflare.net: type AAAA, class IN, addr 2606:4700:10::6814:6f06
[Request In: 21]
[Time: 0.038104007 seconds]
```

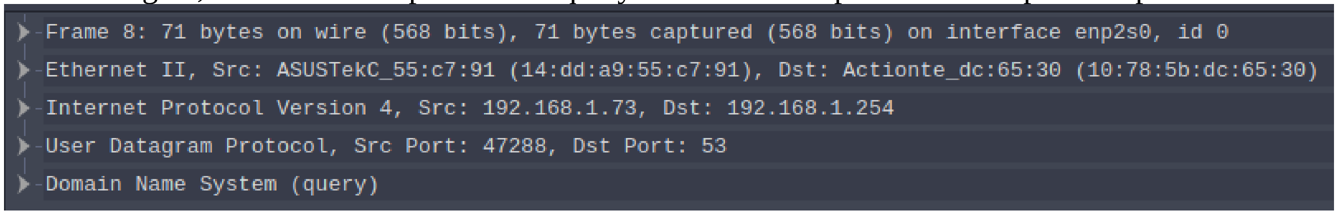
9. The SYN request decided to communicate using IPV6 protocols. Here’s a look at it:

```
No.     Time           Source                           Destination              Protocol Length Info
     23 2.246461290    2001:569:f9fa:3100:1d42:c80c:69e8:a73a 2606:4700:10::6814:6e06 TCP      94     58198 → 80
[SYN] Seq=0 Win=65535 Len=0 MSS=1440 SACK_PERM=1 TSval=3791716081 TSecr=0 WS=512
Frame 23: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface enp2s0, id 0
Ethernet II, Src: ASUSTekC_55:c7:91 (14:dd:a9:55:c7:91), Dst: Actionte_dc:65:30 (10:78:5b:dc:65:30)
Internet Protocol Version 6, Src: 2001:569:f9fa:3100:1d42:c80c:69e8:a73a, Dst: 2606:4700:10::6814:6e06
Transmission Control Protocol, Src Port: 58198, Dst Port: 80, Seq: 0, Len: 0
```

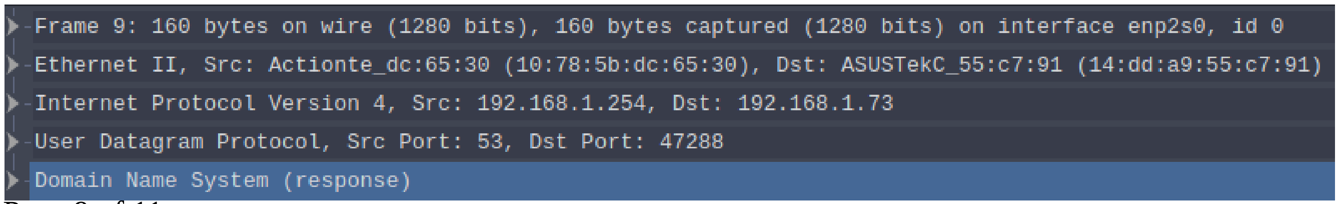
The destination IP address matches the first IP address given by the second DNS lookup (the one that returned IPV6 addresses).

10. Since most of the site seems to be encrypted via TLS, I only see one HTTP request from my machine. It occurs after the DNS responses and TCP handshake, so no, another DNS request is not made prior to requesting the image.

11. Once again, the destination port for the query and the source port for the response is port 53



```
Frame 8: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface enp2s0, id 0
Ethernet II, Src: ASUSTekC_55:c7:91 (14:dd:a9:55:c7:91), Dst: Actionte_dc:65:30 (10:78:5b:dc:65:30)
Internet Protocol Version 4, Src: 192.168.1.73, Dst: 192.168.1.254
User Datagram Protocol, Src Port: 47288, Dst Port: 53
Domain Name System (query)
```

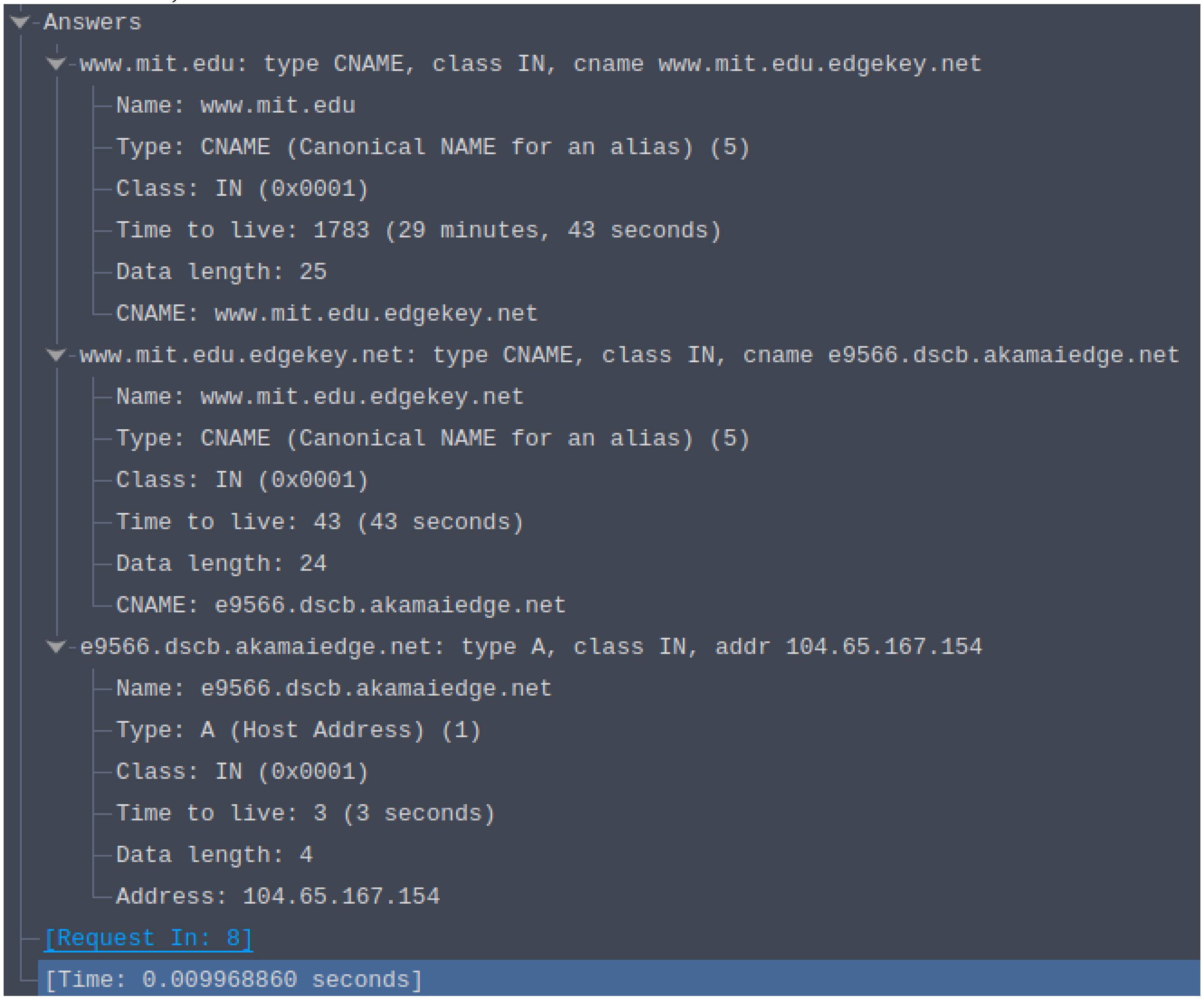


```
Frame 9: 160 bytes on wire (1280 bits), 160 bytes captured (1280 bits) on interface enp2s0, id 0
Ethernet II, Src: Actionte_dc:65:30 (10:78:5b:dc:65:30), Dst: ASUSTekC_55:c7:91 (14:dd:a9:55:c7:91)
Internet Protocol Version 4, Src: 192.168.1.254, Dst: 192.168.1.73
User Datagram Protocol, Src Port: 53, Dst Port: 47288
Domain Name System (response)
```

12. The query is once again sent to my default local DNS server 192.168.1.254

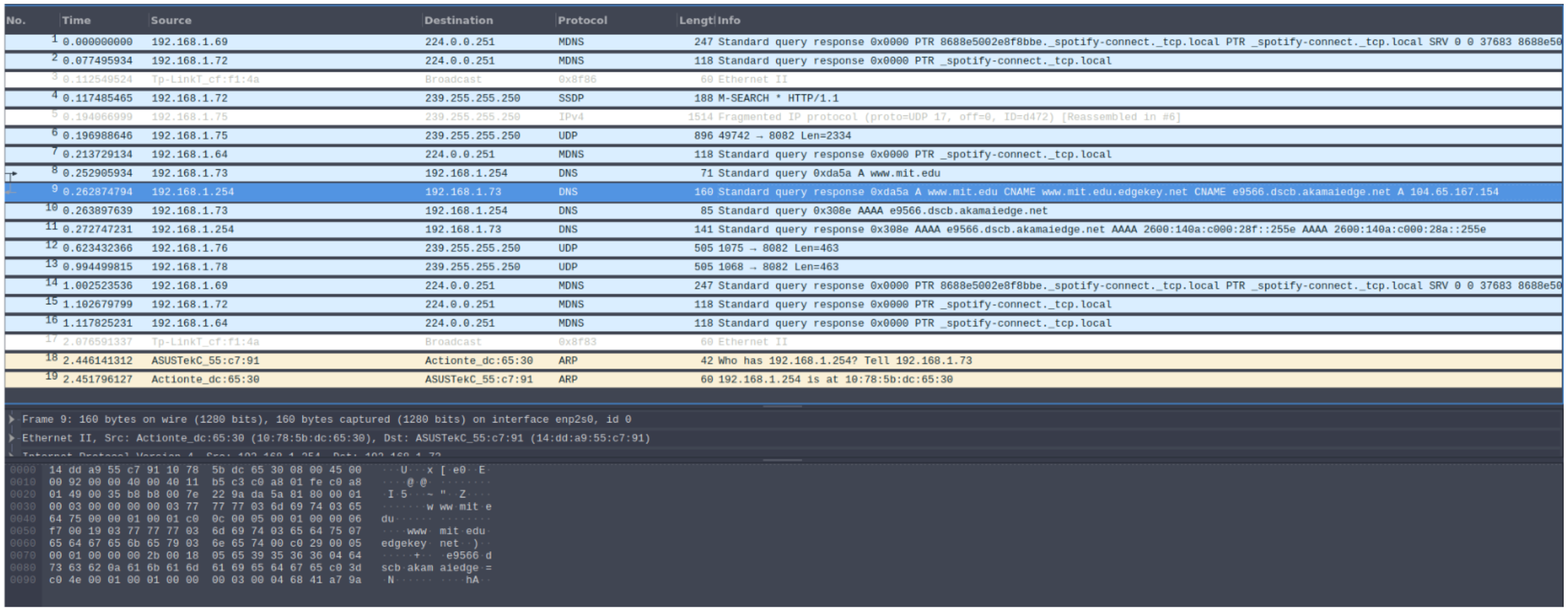
13. Once again, the query is a standard query and contains no answers.

14. The response contains three answers: the canonical hostname (www.mit.edu.edgekey.net), the canonical hostname for that canonical hostname (e9566.dscb.akamaiedge.net), and lastly the ip address for that last url, 104.65.167.154.



```
Answers
  www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
    Name: www.mit.edu
    Type: CNAME (Canonical NAME for an alias) (5)
    Class: IN (0x0001)
    Time to live: 1783 (29 minutes, 43 seconds)
    Data length: 25
    CNAME: www.mit.edu.edgekey.net
  www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
    Name: www.mit.edu.edgekey.net
    Type: CNAME (Canonical NAME for an alias) (5)
    Class: IN (0x0001)
    Time to live: 43 (43 seconds)
    Data length: 24
    CNAME: e9566.dscb.akamaiedge.net
  e9566.dscb.akamaiedge.net: type A, class IN, addr 104.65.167.154
    Name: e9566.dscb.akamaiedge.net
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 3 (3 seconds)
    Data length: 4
    Address: 104.65.167.154
[Request In: 8]
[Time: 0.009968860 seconds]
```

15. A screenshot of what? Here's one:



```
No.  Time         Source              Destination       Protocol  Lengt Info
   1 0.000000000  192.168.1.69        224.0.0.251       MDNS       247 Standard query response 0x0000 PTR 8688e5002e8f8bbe._spotify-connect._tcp.local PTR _spotify-connect._tcp.local SRV 0 0 37683 8688e50
   2 0.077495934  192.168.1.72        224.0.0.251       MDNS       118 Standard query response 0x0000 PTR _spotify-connect._tcp.local
   3 0.112549524  Tp-LinkT_cf:f1:4a   Broadcast         0x8f86      60 Ethernet II
   4 0.117485465  192.168.1.72        239.255.255.250   SSDP       188 M-SEARCH * HTTP/1.1
   5 0.194066999  192.168.1.75        239.255.255.250   IPv4      1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=d472) [Reassembled in #6]
   6 0.196988646  192.168.1.75        239.255.255.250   UDP        896 49742 → 8082 Len=2334
   7 0.213729134  192.168.1.64        224.0.0.251       MDNS       118 Standard query response 0x0000 PTR _spotify-connect._tcp.local
   8 0.252905934  192.168.1.73        192.168.1.254     DNS         71 Standard query 0xda5a A www.mit.edu
   9 0.262874794  192.168.1.254       192.168.1.73      DNS        160 Standard query response 0xda5a A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 104.65.167.154
  10 0.263897639  192.168.1.73        192.168.1.254     DNS         85 Standard query 0x308e AAAA e9566.dscb.akamaiedge.net
  11 0.272747231  192.168.1.254       192.168.1.73      DNS        141 Standard query response 0x308e AAAA e9566.dscb.akamaiedge.net AAAA 2600:140a:c000:28f::255e AAAA 2600:140a:c000:28a::255e
  12 0.623432366  192.168.1.76        239.255.255.250   UDP        505 1075 → 8082 Len=463
  13 0.994499815  192.168.1.78        239.255.255.250   UDP        505 1068 → 8082 Len=463
  14 1.002523536  192.168.1.69        224.0.0.251       MDNS       247 Standard query response 0x0000 PTR 8688e5002e8f8bbe._spotify-connect._tcp.local PTR _spotify-connect._tcp.local SRV 0 0 37683 8688e50
  15 1.102679799  192.168.1.72        224.0.0.251       MDNS       118 Standard query response 0x0000 PTR _spotify-connect._tcp.local
  16 1.117825231  192.168.1.64        224.0.0.251       MDNS       118 Standard query response 0x0000 PTR _spotify-connect._tcp.local
  17 2.076591337  Tp-LinkT_cf:f1:4a   Broadcast         0x8f83      60 Ethernet II
  18 2.446141312  ASUSTekC_55:c7:91   Actionte_dc:65:30 ARP         42 Who has 192.168.1.254? Tell 192.168.1.73
  19 2.451796127  Actionte_dc:65:30   ASUSTekC_55:c7:91 ARP         60 192.168.1.254 is at 10:78:5b:dc:65:30

▶ Frame 9: 160 bytes on wire (1280 bits), 160 bytes captured (1280 bits) on interface enp2s0, id 0
▶ Ethernet II, Src: Actionte_dc:65:30 (10:78:5b:dc:65:30), Dst: ASUSTekC_55:c7:91 (14:dd:a9:55:c7:91)
▶ Internet Protocol Version 4, Src: 192.168.1.254, Dst: 192.168.1.73

0000  14 dd a9 55 c7 91 10 78  5b dc 65 30 08 00 45 00   ···U···x [·e0··E·
0010  00 92 00 00 40 00 40 11  b5 c3 c0 a8 01 fe c0 a8   ····@·@· ········
0020  01 49 00 35 b8 b8 00 7e  22 9a da 5a 81 80 00 01   ·I·5···~ "··Z····
0030  00 03 00 00 00 00 03 77  77 77 03 6d 69 74 03 65   ·······w ww·mit·e
0040  64 75 00 00 01 00 01 c0  0c 00 05 00 01 00 00 06   du······ ········
0050  f7 00 19 03 77 77 77 03  6d 69 74 03 65 64 75 07   ····www· mit·edu·
0060  65 64 67 65 6b 65 79 03  6e 65 74 00 c0 29 00 05   edgekey· net··)··
0070  00 01 00 00 00 2b 00 18  05 65 39 35 36 36 04 64   ·····+·· ·e9566·d
0080  73 63 62 0a 61 6b 61 6d  61 69 65 64 67 65 c0 3d   scb·akam aiedge·=
0090  c0 4e 00 01 00 01 00 00  00 03 00 04 68 41 a7 9a   ·N······ ····hA··
```