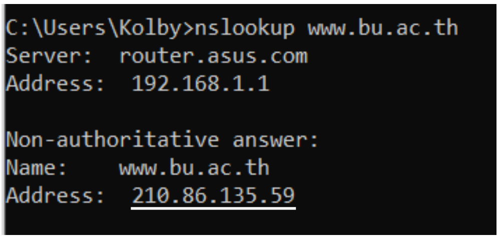
Kolby Sarson
Anthony Azar

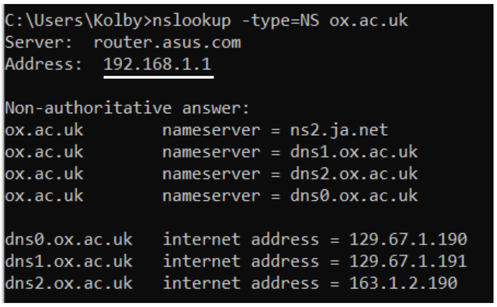
PART 1

1. I used www.bu.ac.th (Bangkok University, Thailand) which has the IP address 210.86.135.59.



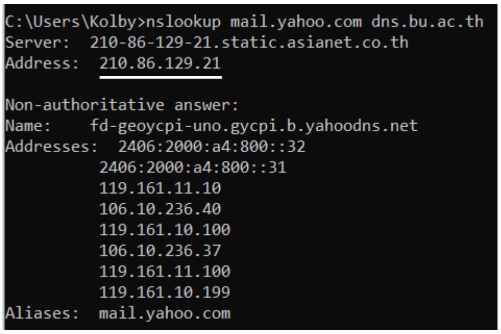
```
C:\Users\Kolby>nslookup www.bu.ac.th
Server:  router.asus.com
Address:  192.168.1.1

Non-authoritative answer:
Name:    www.bu.ac.th
Address:  210.86.135.59
```

2. I used ox.ac.uk (Oxford University, UK) which has the IP address 192.168.1.1.



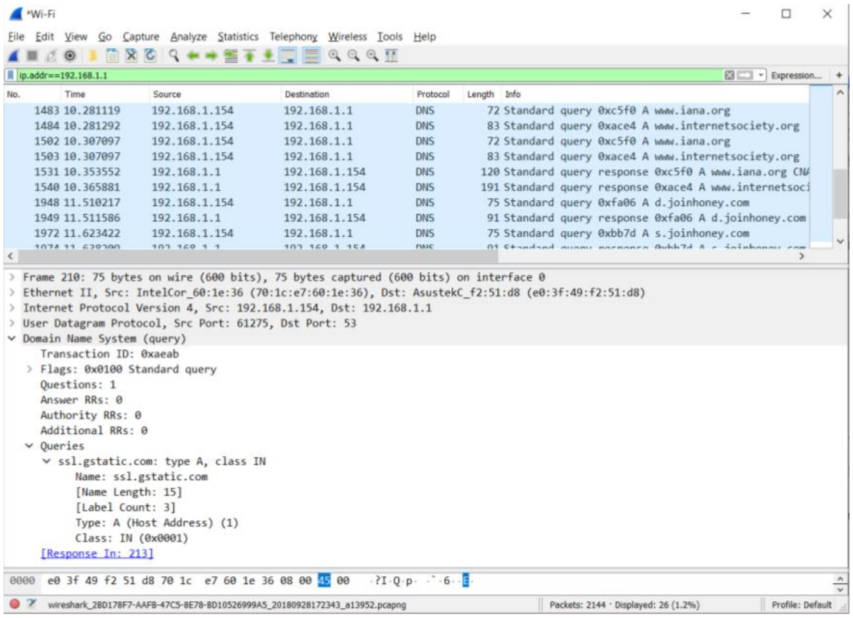
```
C:\Users\Kolby>nslookup -type=NS ox.ac.uk
Server:  router.asus.com
Address:  192.168.1.1

Non-authoritative answer:
ox.ac.uk        nameserver = ns2.ja.net
ox.ac.uk        nameserver = dns1.ox.ac.uk
ox.ac.uk        nameserver = dns2.ox.ac.uk
ox.ac.uk        nameserver = dns0.ox.ac.uk

dns0.ox.ac.uk   internet address = 129.67.1.190
dns1.ox.ac.uk   internet address = 129.67.1.191
dns2.ox.ac.uk   internet address = 163.1.2.190
```

3. I used dns.bu.ac.th (From part 1 server as part 2 server got DNS timeout) which has the address 210.86.129.21.



```
C:\Users\Kolby>nslookup mail.yahoo.com dns.bu.ac.th
Server:  210-86-129-21.static.asianet.co.th
Address:  210.86.129.21

Non-authoritative answer:
Name:    fd-geoycpi-uno.gycpi.b.yahoodns.net
Addresses:  2406:2000:a4:800::32
          2406:2000:a4:800::31
          119.161.11.10
          106.10.236.40
          119.161.10.100
          106.10.236.37
          119.161.11.100
          119.161.10.199
Aliases:  mail.yahoo.com
```

PART 2


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...

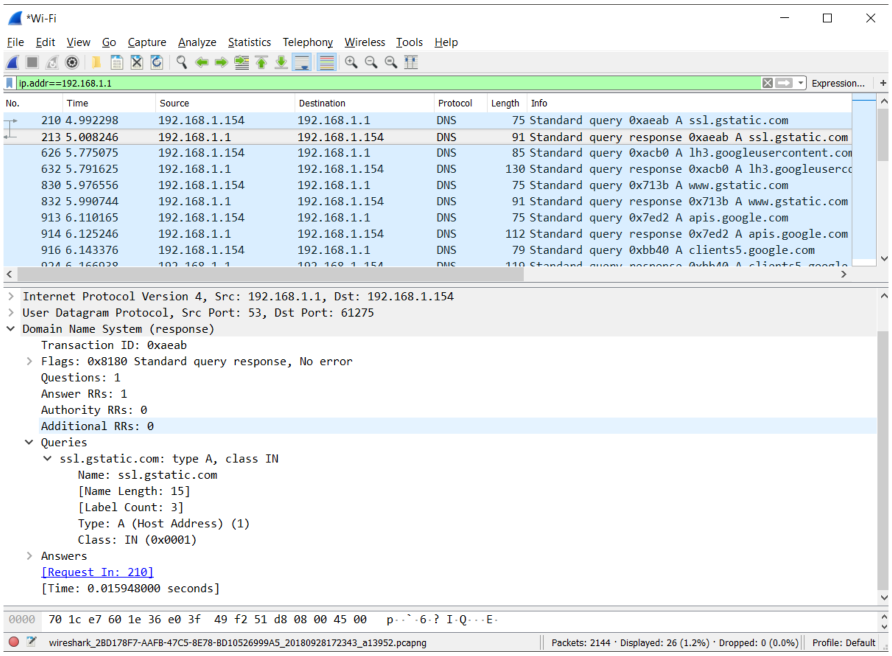
```
ip.addr==192.168.1.1
```

```
No.     Time       Source          Destination     Protocol  Length Info
   1483 10.281119  192.168.1.154   192.168.1.1     DNS        72 Standard query 0xc5f0 A www.iana.org
   1484 10.281292  192.168.1.154   192.168.1.1     DNS        83 Standard query 0xace4 A www.internetsociety.org
   1502 10.307097  192.168.1.154   192.168.1.1     DNS        72 Standard query 0xc5f0 A www.iana.org
   1503 10.307097  192.168.1.154   192.168.1.1     DNS        83 Standard query 0xace4 A www.internetsociety.org
   1531 10.353552  192.168.1.1     192.168.1.154   DNS       120 Standard query response 0xc5f0 A www.iana.org CN/
   1540 10.365881  192.168.1.1     192.168.1.154   DNS       191 Standard query response 0xace4 A www.internetsoci
   1948 11.510217  192.168.1.154   192.168.1.1     DNS        75 Standard query 0xfa06 A d.joinhoney.com
   1949 11.511586  192.168.1.1     192.168.1.154   DNS        91 Standard query response 0xfa06 A d.joinhoney.com
   1972 11.623422  192.168.1.154   192.168.1.1     DNS        75 Standard query 0xbb7d A s.joinhoney.com
```

```
> Frame 210: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface 0
> Ethernet II, Src: IntelCor_60:1e:36 (70:1c:e7:60:1e:36), Dst: AsustekC_f2:51:d8 (e0:3f:49:f2:51:d8)
> Internet Protocol Version 4, Src: 192.168.1.154, Dst: 192.168.1.1
> User Datagram Protocol, Src Port: 61275, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0xaeab
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v ssl.gstatic.com: type A, class IN
        Name: ssl.gstatic.com
        [Name Length: 15]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
    [Response In: 213]
```

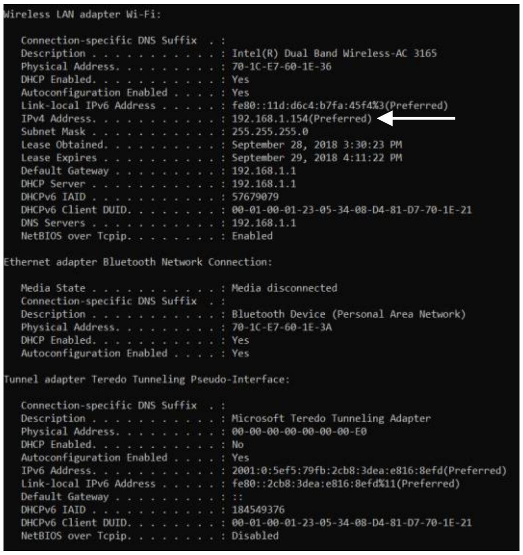
```
0000  e0 3f 49 f2 51 d8 70 1c  e7 60 1e 36 08 00 45 00   ·?I·Q·p· ·`·6··E·
```

```
wireshark_2BD178F7-AAFB-47C5-8E78-BD10526999A5_20180928172343_a13952.pcapng    Packets: 2144 · Displayed: 26 (1.2%)    Profile: Default
```


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...

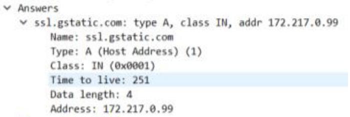
```
ip.addr==192.168.1.1

No.   Time       Source          Destination     Protocol  Length Info
  210 4.992298   192.168.1.154   192.168.1.1     DNS         75 Standard query 0xaeab A ssl.gstatic.com
  213 5.008246   192.168.1.1     192.168.1.154   DNS         91 Standard query response 0xaeab A ssl.gstatic.com
  626 5.775075   192.168.1.154   192.168.1.1     DNS         85 Standard query 0xacb0 A lh3.googleusercontent.com
  632 5.791625   192.168.1.1     192.168.1.154   DNS        130 Standard query response 0xacb0 A lh3.googleuserco
  830 5.976556   192.168.1.154   192.168.1.1     DNS         75 Standard query 0x713b A www.gstatic.com
  832 5.990744   192.168.1.1     192.168.1.154   DNS         91 Standard query response 0x713b A www.gstatic.com
  913 6.110165   192.168.1.154   192.168.1.1     DNS         75 Standard query 0x7ed2 A apis.google.com
  914 6.125246   192.168.1.1     192.168.1.154   DNS        112 Standard query response 0x7ed2 A apis.google.com
  916 6.143376   192.168.1.154   192.168.1.1     DNS         79 Standard query 0xbb40 A clients5.google.com
  924 6.166938   192.168.1.1     192.168.1.154   DNS        110 Standard query response 0xbb40 A clients5.google

> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.154
> User Datagram Protocol, Src Port: 53, Dst Port: 61275
v Domain Name System (response)
    Transaction ID: 0xaeab
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v ssl.gstatic.com: type A, class IN
        Name: ssl.gstatic.com
        [Name Length: 15]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
  > Answers
    [Request In: 210]
    [Time: 0.015948000 seconds]

0000  70 1c e7 60 1e 36 e0 3f  49 f2 51 d8 08 00 45 00   p··`·6·? I·Q···E·

wireshark_2BD178F7-AAFB-47C5-8E78-BD10526999A5_20180928172343_a13952.pcapng   Packets: 2144 · Displayed: 26 (1.2%) · Dropped: 0 (0.0%)   Profile: Default
```

4. They are sent over UPD.
5. The destination port for the DNS query message is 53 and the source port of the DNS response message is 53.



```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Dual Band Wireless-AC 3165
   Physical Address. . . . . . . . . : 70-1C-E7-60-1E-36
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::11d:d6c4:b7fa:45f4%3(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.154(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : September 28, 2018 3:30:23 PM
   Lease Expires . . . . . . . . . . : September 29, 2018 4:11:22 PM
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 57679079
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-23-05-34-08-D4-81-D7-70-1E-21
   DNS Servers . . . . . . . . . . . : 192.168.1.1
   NetBIOS over Tcpip. . . . . . . . : Enabled

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Bluetooth Device (Personal Area Network)
   Physical Address. . . . . . . . . : 70-1C-E7-60-1E-3A
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Tunnel adapter Teredo Tunneling Pseudo-Interface:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Teredo Tunneling Adapter
   Physical Address. . . . . . . . . : 00-00-00-00-00-00-00-E0
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : 2001:0:5ef5:79fb:2cb8:3dea:e816:8efd(Preferred)
   Link-local IPv6 Address . . . . . : fe80::2cb8:3dea:e816:8efd%11(Preferred)
   Default Gateway . . . . . . . . . : ::
   DHCPv6 IAID . . . . . . . . . . . : 184549376
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-23-05-34-08-D4-81-D7-70-1E-21
   NetBIOS over Tcpip. . . . . . . . : Disabled
```

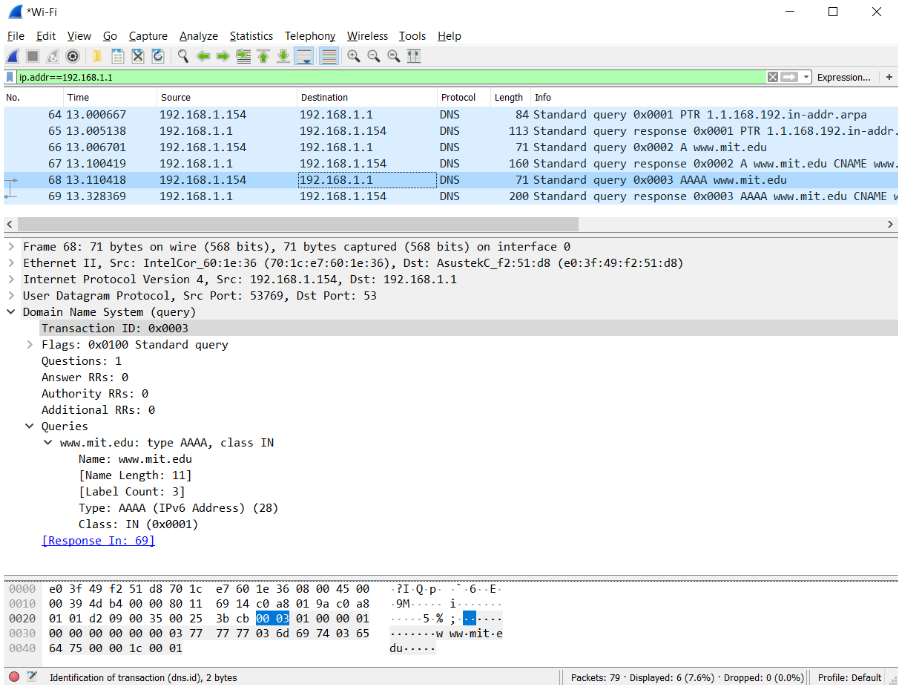
6. It's sent to 192.168.1.154, which corresponds to the IPv4 address.
7. The query is type A and does not contain any answers.
8. There is one answer and it contains the following:



```
v Answers
  v ssl.gstatic.com: type A, class IN, addr 172.217.0.99
      Name: ssl.gstatic.com
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 251
      Data length: 4
      Address: 172.217.0.99
```

9. The first SYN packet was sent to 172.217.0.99, which corresponds to the IP of the answer acquired in the DNS response message.
10. No.

PART 3



*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

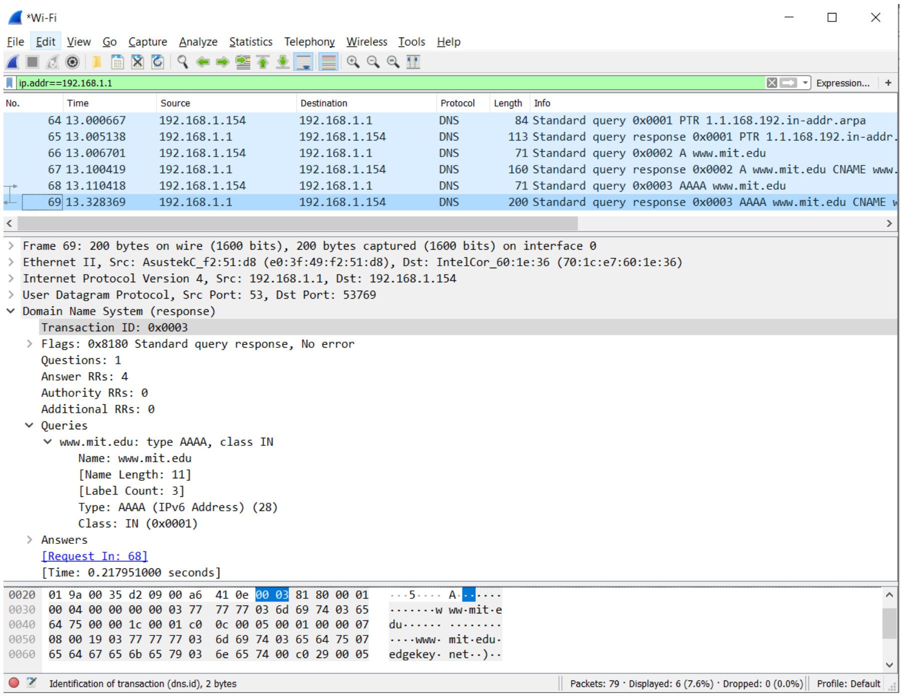
ip.addr==192.168.1.1

```
No.   Time       Source          Destination     Protocol Length Info
   64 13.000667  192.168.1.154   192.168.1.1     DNS         84 Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
   65 13.005138  192.168.1.1     192.168.1.154   DNS        113 Standard query response 0x0001 PTR 1.1.168.192.in-addr.
   66 13.006701  192.168.1.154   192.168.1.1     DNS         71 Standard query 0x0002 A www.mit.edu
   67 13.100419  192.168.1.1     192.168.1.154   DNS        160 Standard query response 0x0002 A www.mit.edu CNAME www.
   68 13.110418  192.168.1.154   192.168.1.1     DNS         71 Standard query 0x0003 AAAA www.mit.edu
   69 13.328369  192.168.1.1     192.168.1.154   DNS        200 Standard query response 0x0003 AAAA www.mit.edu CNAME w
```

```
> Frame 68: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface 0
> Ethernet II, Src: IntelCor_60:1e:36 (70:1c:e7:60:1e:36), Dst: AsustekC_f2:51:d8 (e0:3f:49:f2:51:d8)
> Internet Protocol Version 4, Src: 192.168.1.154, Dst: 192.168.1.1
> User Datagram Protocol, Src Port: 53769, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x0003
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v www.mit.edu: type AAAA, class IN
        Name: www.mit.edu
        [Name Length: 11]
        [Label Count: 3]
        Type: AAAA (IPv6 Address) (28)
        Class: IN (0x0001)
    [Response In: 69]
```

```
0000  e0 3f 49 f2 51 d8 70 1c  e7 60 1e 36 08 00 45 00   ·?I·Q·p· ·`·6··E·
0010  00 39 4d b4 00 00 80 11  69 14 c0 a8 01 9a c0 a8   ·9M····· i·······
0020  01 01 d2 09 00 35 00 25  3b cb 00 03 01 00 00 01   ·····5·% ;·······
0030  00 00 00 00 00 00 03 77  77 77 03 6d 69 74 03 65   ·······w ww·mit·e
0040  64 75 00 00 1c 00 01                               du·····
```

Identification of transaction (dns.id), 2 bytes | Packets: 79 · Displayed: 6 (7.6%) · Dropped: 0 (0.0%) | Profile: Default



*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr==192.168.1.1

```
No.   Time       Source          Destination     Protocol Length Info
   64 13.000667  192.168.1.154   192.168.1.1     DNS         84 Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
   65 13.005138  192.168.1.1     192.168.1.154   DNS        113 Standard query response 0x0001 PTR 1.1.168.192.in-addr.
   66 13.006701  192.168.1.154   192.168.1.1     DNS         71 Standard query 0x0002 A www.mit.edu
   67 13.100419  192.168.1.1     192.168.1.154   DNS        160 Standard query response 0x0002 A www.mit.edu CNAME www.
   68 13.110418  192.168.1.154   192.168.1.1     DNS         71 Standard query 0x0003 AAAA www.mit.edu
   69 13.328369  192.168.1.1     192.168.1.154   DNS        200 Standard query response 0x0003 AAAA www.mit.edu CNAME w
```

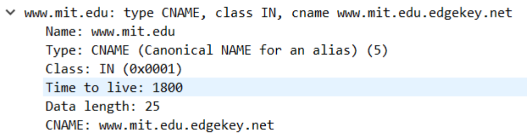
```
> Frame 69: 200 bytes on wire (1600 bits), 200 bytes captured (1600 bits) on interface 0
> Ethernet II, Src: AsustekC_f2:51:d8 (e0:3f:49:f2:51:d8), Dst: IntelCor_60:1e:36 (70:1c:e7:60:1e:36)
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.154
> User Datagram Protocol, Src Port: 53, Dst Port: 53769
v Domain Name System (response)
    Transaction ID: 0x0003
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 4
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v www.mit.edu: type AAAA, class IN
        Name: www.mit.edu
        [Name Length: 11]
        [Label Count: 3]
        Type: AAAA (IPv6 Address) (28)
        Class: IN (0x0001)
  > Answers
    [Request In: 68]
    [Time: 0.217951000 seconds]
```

```
0020  01 9a 00 35 d2 09 00 a6  41 0e 00 03 81 80 00 01   ···5···· A·······
0030  00 04 00 00 00 00 03 77  77 77 03 6d 69 74 03 65   ·······w ww·mit·e
0040  64 75 00 00 1c 00 01 c0  0c 00 05 00 01 00 00 07   du······ ········
0050  08 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··)··
```

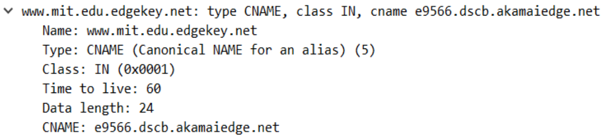
Identification of transaction (dns.id), 2 bytes | Packets: 79 · Displayed: 6 (7.6%) · Dropped: 0 (0.0%) | Profile: Default

11. The destination port for the DNS query message is 53 and the source port of the DNS response message is 53.
12. It is sent to 192.168.1.1, which is the default gateway.
13. It is type AAAA and it does not contain any answers.

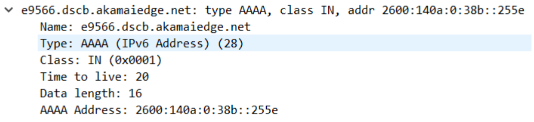
14. The response contains 4 answers, containing the following:



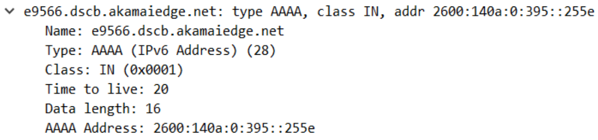
```
⌄ www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
      Name: www.mit.edu
      Type: CNAME (Canonical NAME for an alias) (5)
      Class: IN (0x0001)
      Time to live: 1800
      Data length: 25
      CNAME: www.mit.edu.edgekey.net
```



```
⌄ 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: 60
      Data length: 24
      CNAME: e9566.dscb.akamaiedge.net
```



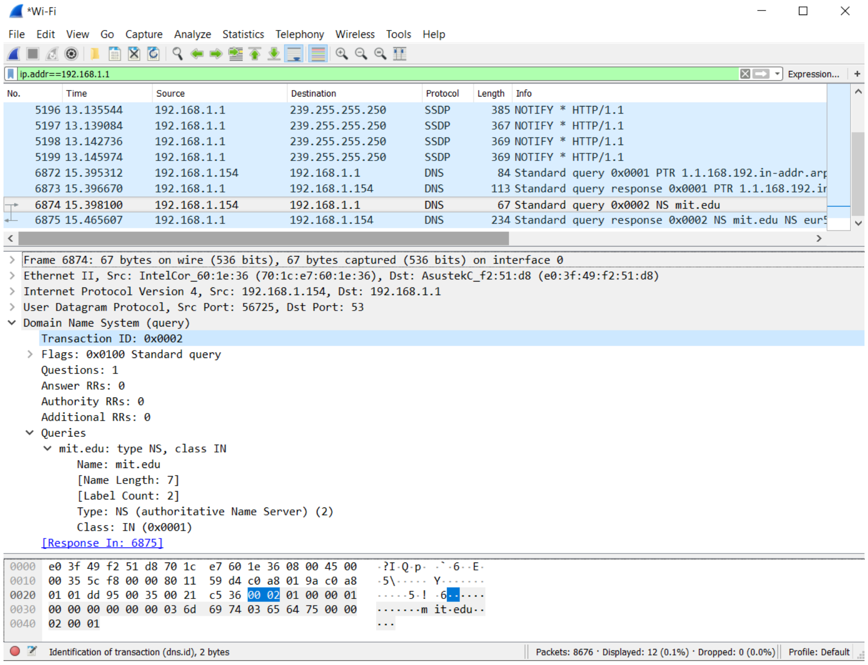
```
⌄ e9566.dscb.akamaiedge.net: type AAAA, class IN, addr 2600:140a:0:38b::255e
      Name: e9566.dscb.akamaiedge.net
      Type: AAAA (IPv6 Address) (28)
      Class: IN (0x0001)
      Time to live: 20
      Data length: 16
      AAAA Address: 2600:140a:0:38b::255e
```



```
⌄ e9566.dscb.akamaiedge.net: type AAAA, class IN, addr 2600:140a:0:395::255e
      Name: e9566.dscb.akamaiedge.net
      Type: AAAA (IPv6 Address) (28)
      Class: IN (0x0001)
      Time to live: 20
      Data length: 16
      AAAA Address: 2600:140a:0:395::255e
```

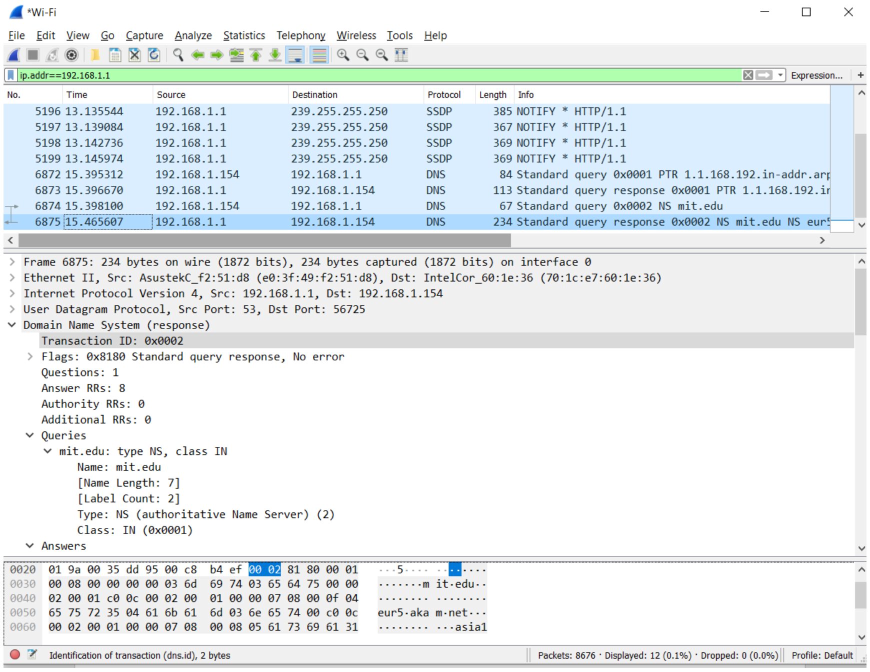
15. Screenshots provided throughout.

PART 4



*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...

```
ip.addr==192.168.1.1

No.   Time       Source         Destination      Protocol  Length Info
 5196 13.135544  192.168.1.1    239.255.255.250  SSDP      385 NOTIFY * HTTP/1.1
 5197 13.139084  192.168.1.1    239.255.255.250  SSDP      367 NOTIFY * HTTP/1.1
 5198 13.142736  192.168.1.1    239.255.255.250  SSDP      369 NOTIFY * HTTP/1.1
 5199 13.145974  192.168.1.1    239.255.255.250  SSDP      369 NOTIFY * HTTP/1.1
 6872 15.395312  192.168.1.154  192.168.1.1      DNS        84 Standard query 0x0001 PTR 1.1.168.192.in-addr.arp
 6873 15.396670  192.168.1.1    192.168.1.154    DNS       113 Standard query response 0x0001 PTR 1.1.168.192.ir
 6874 15.398100  192.168.1.154  192.168.1.1      DNS        67 Standard query 0x0002 NS mit.edu
 6875 15.465607  192.168.1.1    192.168.1.154    DNS       234 Standard query response 0x0002 NS mit.edu NS eur5

> Frame 6874: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface 0
> Ethernet II, Src: IntelCor_60:1e:36 (70:1c:e7:60:1e:36), Dst: AsustekC_f2:51:d8 (e0:3f:49:f2:51:d8)
> Internet Protocol Version 4, Src: 192.168.1.154, Dst: 192.168.1.1
> User Datagram Protocol, Src Port: 56725, Dst Port: 53
⌄ Domain Name System (query)
    Transaction ID: 0x0002
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ⌄ Queries
    ⌄ mit.edu: type NS, class IN
        Name: mit.edu
        [Name Length: 7]
        [Label Count: 2]
        Type: NS (authoritative Name Server) (2)
        Class: IN (0x0001)
    [Response In: 6875]

0000  e0 3f 49 f2 51 d8 70 1c  e7 60 1e 36 08 00 45 00   ·?I·Q·p· ·`·6··E·
0010  00 35 5c f8 00 00 80 11  59 d4 c0 a8 01 9a c0 a8   ·5\····· Y·······
0020  01 01 dd 95 00 35 00 21  c5 36 00 02 01 00 00 01   ·····5·! ·6······
0030  00 00 00 00 00 00 03 6d  69 74 03 65 64 75 00 00   ·······m it·edu··
0040  02 00 01                                           ···

Identification of transaction (dns.id), 2 bytes    Packets: 8676 · Displayed: 12 (0.1%) · Dropped: 0 (0.0%)    Profile: Default
```

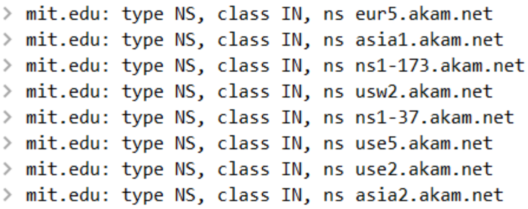


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...

```
ip.addr==192.168.1.1

No.   Time       Source         Destination      Protocol  Length Info
 5196 13.135544  192.168.1.1    239.255.255.250  SSDP      385 NOTIFY * HTTP/1.1
 5197 13.139084  192.168.1.1    239.255.255.250  SSDP      367 NOTIFY * HTTP/1.1
 5198 13.142736  192.168.1.1    239.255.255.250  SSDP      369 NOTIFY * HTTP/1.1
 5199 13.145974  192.168.1.1    239.255.255.250  SSDP      369 NOTIFY * HTTP/1.1
 6872 15.395312  192.168.1.154  192.168.1.1      DNS        84 Standard query 0x0001 PTR 1.1.168.192.in-addr.arp
 6873 15.396670  192.168.1.1    192.168.1.154    DNS       113 Standard query response 0x0001 PTR 1.1.168.192.ir
 6874 15.398100  192.168.1.154  192.168.1.1      DNS        67 Standard query 0x0002 NS mit.edu
 6875 15.465607  192.168.1.1    192.168.1.154    DNS       234 Standard query response 0x0002 NS mit.edu NS eur5

> Frame 6875: 234 bytes on wire (1872 bits), 234 bytes captured (1872 bits) on interface 0
> Ethernet II, Src: AsustekC_f2:51:d8 (e0:3f:49:f2:51:d8), Dst: IntelCor_60:1e:36 (70:1c:e7:60:1e:36)
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.154
> User Datagram Protocol, Src Port: 53, Dst Port: 56725
⌄ Domain Name System (response)
    Transaction ID: 0x0002
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 8
    Authority RRs: 0
    Additional RRs: 0
  ⌄ Queries
    ⌄ mit.edu: type NS, class IN
        Name: mit.edu
        [Name Length: 7]
        [Label Count: 2]
        Type: NS (authoritative Name Server) (2)
        Class: IN (0x0001)
  ⌄ Answers

0020  01 9a 00 35 dd 95 00 c8  b4 ef 00 02 81 80 00 01   ···5···· ········
0030  00 08 00 00 00 00 03 6d  69 74 03 65 64 75 00 00   ·······m it·edu··
0040  02 00 01 c0 0c 00 02 00  01 00 00 07 08 00 0f 04   ········ ········
0050  65 75 72 35 04 61 6b 61  6d 03 6e 65 74 00 c0 0c   eur5·aka m·net···
0060  00 02 00 01 00 00 07 08  00 08 05 61 73 69 61 31   ········ ···asia1

Identification of transaction (dns.id), 2 bytes    Packets: 8676 · Displayed: 12 (0.1%) · Dropped: 0 (0.0%)    Profile: Default
```

Kolby Sarson
Anthony Azar

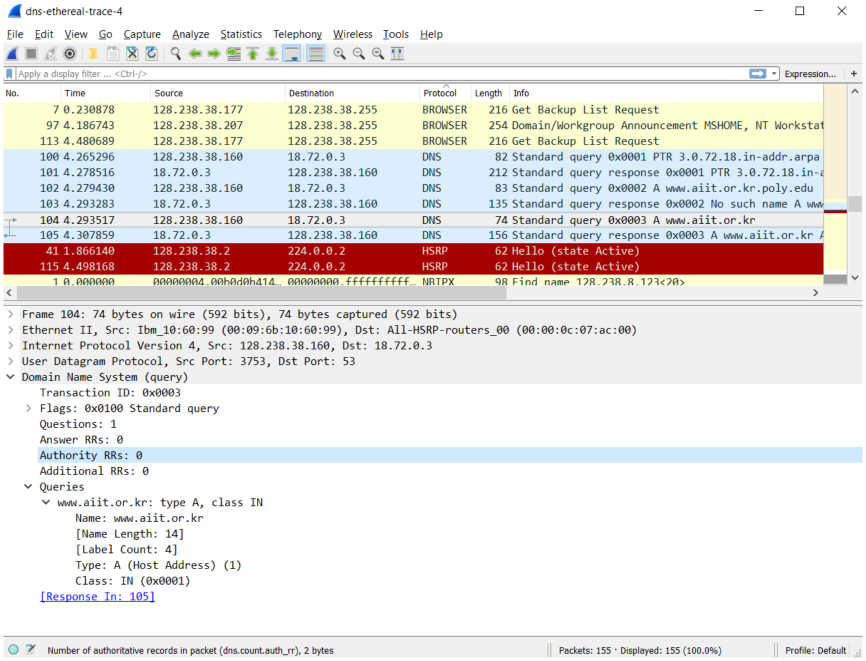
16. The destination IP for the DNS query message is 192.168.1.1 and this is my default DNS server.
17. It is type NS and it does not contain any answers.
18. The MIT nameservers are as follows:
    They do not include the IP addresses



```
> mit.edu: type NS, class IN, ns eur5.akam.net
> mit.edu: type NS, class IN, ns asia1.akam.net
> mit.edu: type NS, class IN, ns ns1-173.akam.net
> mit.edu: type NS, class IN, ns usw2.akam.net
> mit.edu: type NS, class IN, ns ns1-37.akam.net
> mit.edu: type NS, class IN, ns use5.akam.net
> mit.edu: type NS, class IN, ns use2.akam.net
> mit.edu: type NS, class IN, ns asia2.akam.net
```

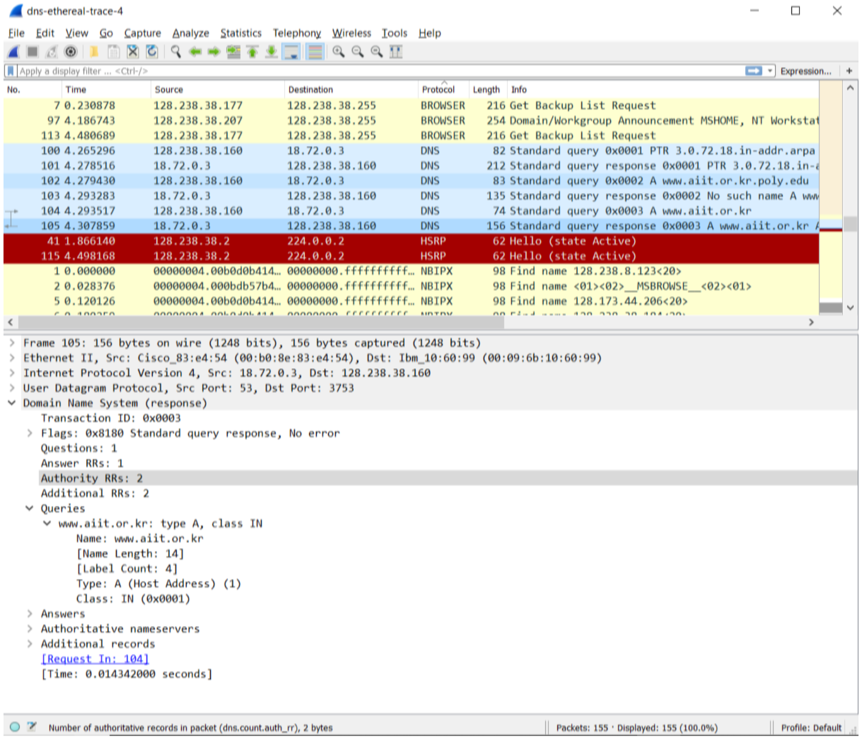
19. Screenshots provided throughout.

PART 5



dns-ethereal-trace-4
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...

```
No.   Time      Source                Destination           Protocol  Length Info
    7 0.230878  128.238.38.177        128.238.38.255        BROWSER   216 Get Backup List Request
   97 4.186743  128.238.38.207        128.238.38.255        BROWSER   254 Domain/Workgroup Announcement MSHOME, NT Workstat
  113 4.480689  128.238.38.177        128.238.38.255        BROWSER   216 Get Backup List Request
  100 4.265296  128.238.38.160        18.72.0.3             DNS        82 Standard query 0x0001 PTR 3.0.72.18.in-addr.arpa
  101 4.278516  18.72.0.3             128.238.38.160        DNS       212 Standard query response 0x0001 PTR 3.0.72.18.in-a
  102 4.279430  128.238.38.160        18.72.0.3             DNS        83 Standard query 0x0002 A www.aiit.or.kr.poly.edu
  103 4.293283  18.72.0.3             128.238.38.160        DNS       135 Standard query response 0x0002 No such name A www
  104 4.293517  128.238.38.160        18.72.0.3             DNS        74 Standard query 0x0003 A www.aiit.or.kr
  105 4.307859  18.72.0.3             128.238.38.160        DNS       156 Standard query response 0x0003 A www.aiit.or.kr A
   41 1.866140  128.238.38.2          224.0.0.2             HSRP       62 Hello (state Active)
  115 4.498168  128.238.38.2          224.0.0.2             HSRP       62 Hello (state Active)
    1 0.000000  00000004.00b0d0b414…  00000000.ffffffffff…  NBIPX      98 Find name 128.238.8.123<20>

> Frame 104: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
> Ethernet II, Src: Ibm_10:60:99 (00:09:6b:10:60:99), Dst: All-HSRP-routers_00 (00:00:0c:07:ac:00)
> Internet Protocol Version 4, Src: 128.238.38.160, Dst: 18.72.0.3
> User Datagram Protocol, Src Port: 3753, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x0003
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v www.aiit.or.kr: type A, class IN
        Name: www.aiit.or.kr
        [Name Length: 14]
        [Label Count: 4]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
    [Response In: 105]

Number of authoritative records in packet (dns.count.auth_rr), 2 bytes    Packets: 155 · Displayed: 155 (100.0%)    Profile: Default
```

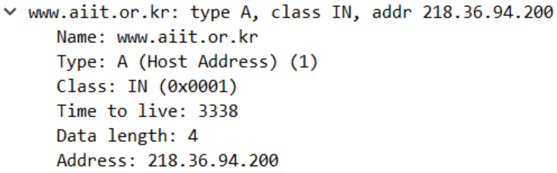


dns-ethereal-trace-4
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...

```
No.   Time      Source                Destination           Protocol  Length Info
    7 0.230878  128.238.38.177        128.238.38.255        BROWSER   216 Get Backup List Request
   97 4.186743  128.238.38.207        128.238.38.255        BROWSER   254 Domain/Workgroup Announcement MSHOME, NT Workstat
  113 4.480689  128.238.38.177        128.238.38.255        BROWSER   216 Get Backup List Request
  100 4.265296  128.238.38.160        18.72.0.3             DNS        82 Standard query 0x0001 PTR 3.0.72.18.in-addr.arpa
  101 4.278516  18.72.0.3             128.238.38.160        DNS       212 Standard query response 0x0001 PTR 3.0.72.18.in-a
  102 4.279430  128.238.38.160        18.72.0.3             DNS        83 Standard query 0x0002 A www.aiit.or.kr.poly.edu
  103 4.293283  18.72.0.3             128.238.38.160        DNS       135 Standard query response 0x0002 No such name A www
  104 4.293517  128.238.38.160        18.72.0.3             DNS        74 Standard query 0x0003 A www.aiit.or.kr
  105 4.307859  18.72.0.3             128.238.38.160        DNS       156 Standard query response 0x0003 A www.aiit.or.kr A
   41 1.866140  128.238.38.2          224.0.0.2             HSRP       62 Hello (state Active)
  115 4.498168  128.238.38.2          224.0.0.2             HSRP       62 Hello (state Active)
    1 0.000000  00000004.00b0d0b414…  00000000.ffffffffff…  NBIPX      98 Find name 128.238.8.123<20>
    2 0.028376  00000004.000bdb57b4…  00000000.ffffffffff…  NBIPX      98 Find name <01><02>__MSBROWSE__<02><01>
    5 0.120126  00000004.00b0d0b414…  00000000.ffffffffff…  NBIPX      98 Find name 128.173.44.206<20>

> Frame 105: 156 bytes on wire (1248 bits), 156 bytes captured (1248 bits)
> Ethernet II, Src: Cisco_83:e4:54 (00:b0:8e:83:e4:54), Dst: Ibm_10:60:99 (00:09:6b:10:60:99)
> Internet Protocol Version 4, Src: 18.72.0.3, Dst: 128.238.38.160
> User Datagram Protocol, Src Port: 53, Dst Port: 3753
v Domain Name System (response)
    Transaction ID: 0x0003
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 2
    Additional RRs: 2
  v Queries
    v www.aiit.or.kr: type A, class IN
        Name: www.aiit.or.kr
        [Name Length: 14]
        [Label Count: 4]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
  > Answers
  > Authoritative nameservers
  > Additional records
    [Request In: 104]
    [Time: 0.014342000 seconds]

Number of authoritative records in packet (dns.count.auth_rr), 2 bytes    Packets: 155 · Displayed: 155 (100.0%)    Profile: Default
```

Kolby Sarson
Anthony Azar

20. The query is sent to 18.72.0.3, which is bitsy.mit.edu.
21. The query is type A and does not contain any answers.
22. There is one answer and it contains the following:



```
⌄ www.aiit.or.kr: type A, class IN, addr 218.36.94.200
    Name: www.aiit.or.kr
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 3338
    Data length: 4
    Address: 218.36.94.200
```

23. Screenshots provided throughout.