**WireShark Labs**

**Intro**

Name: Giric Goyal

ID: ggoyal2

UIN: 657440995

1. TCP, HTTP, IGMPv2
2. 0.039561 secs
3. gaia.cs.umass.edu: 128.119.245.12

my: 192.168.1.109

1. Packet Sent:

Frame 349: 469 bytes on wire (3752 bits), 469 bytes captured (3752 bits) on interface 0

Ethernet II, Src: Apple\_42:b4:d4 (b8:e8:56:42:b4:d4), Dst: Cisco-Li\_b6:ac:38 (20:aa:4b:b6:ac:38)

Internet Protocol Version 4, Src: 192.168.1.109 (192.168.1.109), Dst: 128.119.245.12 (128.119.245.12)

Transmission Control Protocol, Src Port: 49359 (49359), Dst Port: http (80), Seq: 1, Ack: 1, Len: 403

Hypertext Transfer Protocol

GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n

Host: gaia.cs.umass.edu\r\n

Connection: keep-alive\r\n

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8\r\n

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_2) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.117 Safari/537.36\r\n

DNT: 1\r\n

Accept-Encoding: gzip,deflate,sdch\r\n

Accept-Language: en-US,en;q=0.8\r\n

\r\n

[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]

[HTTP request 1/2]

[Response in frame: 351]

[Next request in frame: 355]

Packet Received:

Frame 351: 446 bytes on wire (3568 bits), 446 bytes captured (3568 bits) on interface 0

Ethernet II, Src: Cisco-Li\_b6:ac:38 (20:aa:4b:b6:ac:38), Dst: Apple\_42:b4:d4 (b8:e8:56:42:b4:d4)

Internet Protocol Version 4, Src: 128.119.245.12 (128.119.245.12), Dst: 192.168.1.109 (192.168.1.109)

Transmission Control Protocol, Src Port: http (80), Dst Port: 49359 (49359), Seq: 1, Ack: 404, Len: 380

Hypertext Transfer Protocol

HTTP/1.1 200 OK\r\n

Date: Fri, 28 Feb 2014 01:17:46 GMT\r\n

Server: Apache/2.2.3 (CentOS)\r\n

Last-Modified: Fri, 28 Feb 2014 01:17:01 GMT\r\n

ETag: "8734b-51-31e63d40"\r\n

Accept-Ranges: bytes\r\n

Content-Length: 81\r\n

Keep-Alive: timeout=10, max=100\r\n

Connection: Keep-Alive\r\n

Content-Type: text/html; charset=UTF-8\r\n

\r\n

[HTTP response 1/2]

[Time since request: 0.039561000 seconds]

[Request in frame: 349]

[Next request in frame: 355]

[Next response in frame: 356]

Line-based text data: text/html

**HTTP**

The Basic HTTP GET/response interaction

Frame 17: 442 bytes on wire (3536 bits), 442 bytes captured (3536 bits) on interface 0

Ethernet II, Src: Apple\_42:b4:d4 (b8:e8:56:42:b4:d4), Dst: Cisco-Li\_b6:ac:38 (20:aa:4b:b6:ac:38)

Internet Protocol Version 4, Src: 192.168.1.109 (192.168.1.109), Dst: 128.119.245.12 (128.119.245.12)

Transmission Control Protocol, Src Port: 49741 (49741), Dst Port: http (80), Seq: 1, Ack: 1, Len: 376

Hypertext Transfer Protocol

GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n

Host: gaia.cs.umass.edu\r\n

Accept-Encoding: gzip, deflate\r\n

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8\r\n

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_2) AppleWebKit/537.74.9 (KHTML, like Gecko) Version/7.0.2 Safari/537.74.9\r\n

Accept-Language: en-us\r\n

DNT: 1\r\n

Connection: keep-alive\r\n

\r\n

[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]

[HTTP request 1/1]

[Response in frame: 19]

Frame 19: 446 bytes on wire (3568 bits), 446 bytes captured (3568 bits) on interface 0

Ethernet II, Src: Cisco-Li\_b6:ac:38 (20:aa:4b:b6:ac:38), Dst: Apple\_42:b4:d4 (b8:e8:56:42:b4:d4)

Internet Protocol Version 4, Src: 128.119.245.12 (128.119.245.12), Dst: 192.168.1.109 (192.168.1.109)

Transmission Control Protocol, Src Port: http (80), Dst Port: 49741 (49741), Seq: 1, Ack: 377, Len: 380

Hypertext Transfer Protocol

HTTP/1.1 200 OK\r\n

Date: Fri, 28 Feb 2014 01:41:02 GMT\r\n

Server: Apache/2.2.3 (CentOS)\r\n

Last-Modified: Fri, 28 Feb 2014 01:41:01 GMT\r\n

ETag: "8734b-51-87bae540"\r\n

Accept-Ranges: bytes\r\n

Content-Length: 81\r\n

Keep-Alive: timeout=10, max=100\r\n

Connection: Keep-Alive\r\n

Content-Type: text/html; charset=UTF-8\r\n

\r\n

[HTTP response 1/1]

[Time since request: 0.049926000 seconds]

[Request in frame: 17]

Line-based text data: text/html

1. http version 1.1
2. en-us
3. My Computer: 192.168.1.10

gaia.cs.umass.edu server: 128.119.245.12

1. 200
2. Fri, 28 Feb 2014 01:41:01 GMT
3. 81
4. No, I can see all the headers in the packet content window that are listed in the packet-listing window.

The HTTP CONDITIONAL GET/response interaction

1. No
2. Yes. There is a content-type header with value text/html. That means the server returned content explicitly.
3. Yes, the time the file was cached follows the If-Modified-Since header, i.e. Fri, 28 Feb 2014 02:21:01 GMT
4. The server returns 304 Not Modified status code and phrase. No, the server didn’t explicitly return the contents of the file, since the status code is 304 and also there is no content-type header.

Retrieving Long Documents

1. The browser sent just one GET message. Since only one message was sent so, packet 1 contains the GET message for the Bill of Rights.
2. Packet 1 contains the status code and phrase associated with the response to the HTTP GET request
3. 200 OK
4. Four

HTML Documents with Embedded Objects

1. Four GET messages were sent. These were sent to:

128.119.245.12

165.193.140.14

128.119.240.90

128.119.240.90

1. The two images were downloaded serially since my browser first sent GET message for first image, it got the response from the server. Then it sent the GET message for the second image and got the response from the server.

5 HTTP Authentication

1. 401 Authorization Required
2. In the second GET method, Authorization header is included.

**DNS**

**nslookup**

1. The IP address is 59.180.210.191.

nslookup www.mtnl.net.in

Server: 75.75.75.75

Address: 75.75.75.75#53

Non-authoritative answer:

Name: www.mtnl.net.in

Address: 59.180.210.191

2. The IP address of an authoritative server is 163.1.2.190.

nslookup -type=NS ox.ac.uk

Server: 75.75.75.75

Address: 75.75.75.75#53

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.

Authoritative answers can be found from:

dns2.ox.ac.uk internet address = 163.1.2.190

ns2.ja.net internet address = 193.63.105.17

ns2.ja.net has AAAA address 2001:630:0:45::11

3. The server from (2) could not get the IP for yahoo mail.

nslookup -type=MX yahoo.com dns2.ox.ac.uk

Server: dns2.ox.ac.uk

Address: 163.1.2.190#53

\*\* server can't find yahoo.com.hsd1.il.comcast.net: REFUSED

**Tracing DNS with Wireshark**

**ipconfig**

Frame 23: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface 0

Ethernet II, Src: Apple\_42:b4:d4 (b8:e8:56:42:b4:d4), Dst: Cisco-Li\_b6:ac:38 (20:aa:4b:b6:ac:38)

Internet Protocol Version 4, Src: 192.168.1.109 (192.168.1.109), Dst: 75.75.75.75 (75.75.75.75)

User Datagram Protocol, Src Port: 53936 (53936), Dst Port: domain (53)

Domain Name System (query)

[Response In: 26]

Transaction ID: 0x2256

Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

Queries

www.ietf.org: type A, class IN

Frame 26: 88 bytes on wire (704 bits), 88 bytes captured (704 bits) on interface 0

Ethernet II, Src: Cisco-Li\_b6:ac:38 (20:aa:4b:b6:ac:38), Dst: Apple\_42:b4:d4 (b8:e8:56:42:b4:d4)

Internet Protocol Version 4, Src: 75.75.75.75 (75.75.75.75), Dst: 192.168.1.109 (192.168.1.109)

User Datagram Protocol, Src Port: domain (53), Dst Port: 53936 (53936)

Domain Name System (response)

[Request In: 23]

[Time: 0.026403000 seconds]

Transaction ID: 0x2256

Flags: 0x8180 Standard query response, No error

Questions: 1

Answer RRs: 1

Authority RRs: 0

Additional RRs: 0

Queries

www.ietf.org: type A, class IN

Answers

www.ietf.org: type A, class IN, addr 4.31.198.44

Frame 9: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface 0

Ethernet II, Src: Apple\_42:b4:d4 (b8:e8:56:42:b4:d4), Dst: Cisco-Li\_b6:ac:38 (20:aa:4b:b6:ac:38)

Internet Protocol Version 4, Src: 192.168.1.109 (192.168.1.109), Dst: 4.31.198.44 (4.31.198.44)

Transmission Control Protocol, Src Port: 51537 (51537), Dst Port: http (80), Seq: 0, Len: 0

Source port: 51537 (51537)

Destination port: http (80)

[Stream index: 3]

Sequence number: 0 (relative sequence number)

Header length: 44 bytes

Flags: 0x002 (SYN)

Window size value: 65535

[Calculated window size: 65535]

Checksum: 0x1dff [validation disabled]

Options: (24 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), Timestamps, SACK permitted, End of Option List (EOL)

4. They are sent over UDP

5. Destination Port for DNS query message is: domain (53)

and the source Port for DNS response message is: domain (53)

6. DNS query message is sent to 75.75.75.75. Yes both the IP addresses are same.

7. It is a Standard query. There is no response in the message.

8. Only one answer is provided. The answer contains

www.ietf.org: type A, class IN, addr 4.31.198.449.

9. Yes, both the IP address of the TCP SYC and the one provided by the DNS response message are same.

10. Yes it issues new DNS queries.

**nslookup** [**www.mit.edu**](http://www.mit.edu)

Frame 9: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface 0

Ethernet II, Src: Apple\_42:b4:d4 (b8:e8:56:42:b4:d4), Dst: Cisco-Li\_b6:ac:38 (20:aa:4b:b6:ac:38)

Internet Protocol Version 4, Src: 192.168.1.109 (192.168.1.109), Dst: 75.75.75.75 (75.75.75.75)

User Datagram Protocol, Src Port: 51639 (51639), Dst Port: domain (53)

Domain Name System (query)

[Response In: 10]

Transaction ID: 0x1844

Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

Queries

www.mit.edu: type A, class IN

Frame 10: 157 bytes on wire (1256 bits), 157 bytes captured (1256 bits) on interface 0

Ethernet II, Src: Cisco-Li\_b6:ac:38 (20:aa:4b:b6:ac:38), Dst: Apple\_42:b4:d4 (b8:e8:56:42:b4:d4)

Internet Protocol Version 4, Src: 75.75.75.75 (75.75.75.75), Dst: 192.168.1.109 (192.168.1.109)

User Datagram Protocol, Src Port: domain (53), Dst Port: 51639 (51639)

Domain Name System (response)

[Request In: 9]

[Time: 0.017232000 seconds]

Transaction ID: 0x1844

Flags: 0x8180 Standard query response, No error

Questions: 1

Answer RRs: 3

Authority RRs: 0

Additional RRs: 0

Queries

www.mit.edu: type A, class IN

Answers

www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net

www.mit.edu.edgekey.net: type CNAME, class IN, cname e7086.b.akamaiedge.net

e7086.b.akamaiedge.net: type A, class IN, addr 23.210.70.151

11. Destination Port for DNS query is domain (53) and Source Port for DNS response is domain (53).

12. DNS query message is sent to 75.75.75.75. It is same the default local DNS server.

13. It is a standard query with no answers in the query message.

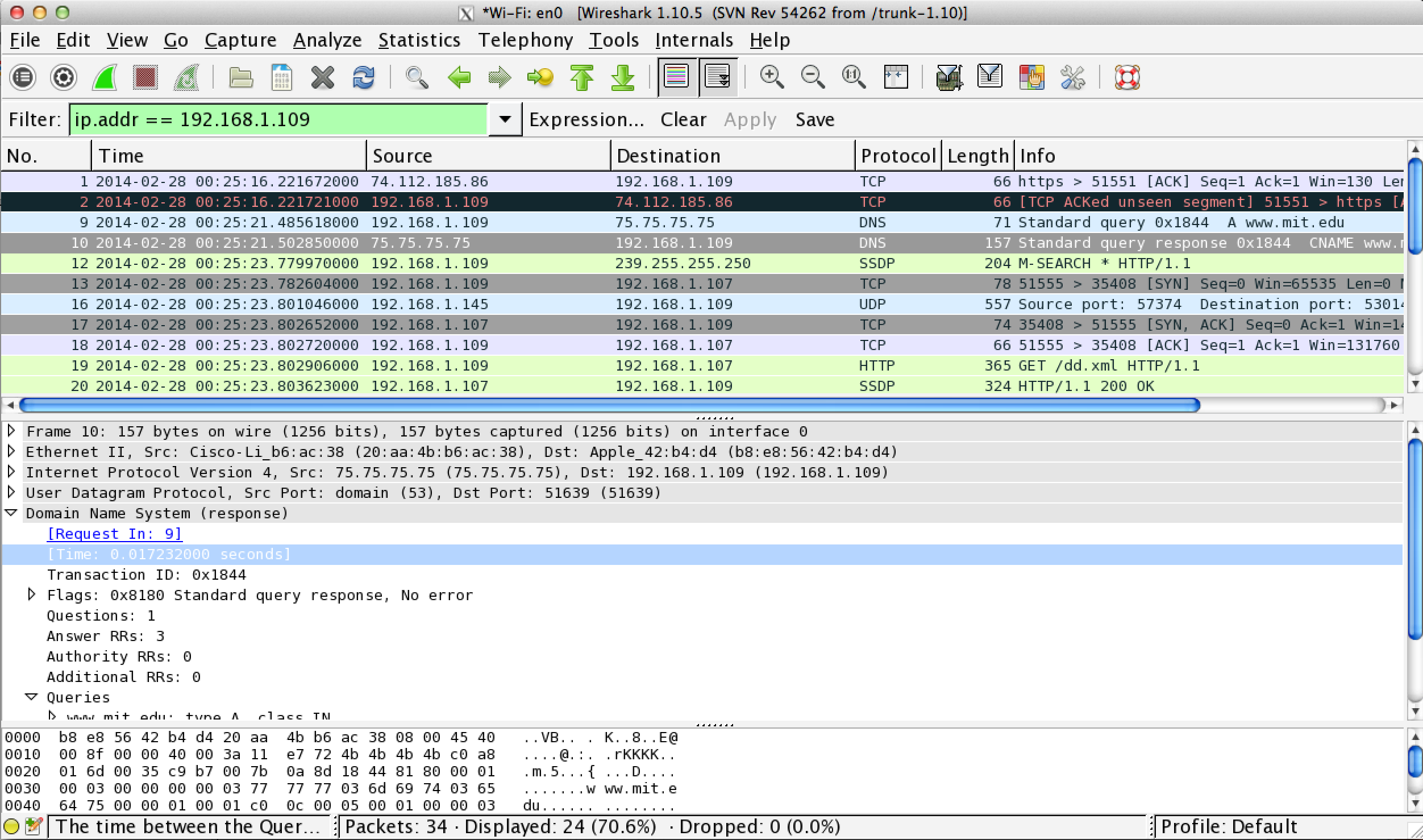
14. There are three answers in the response message. They are:

www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net

www.mit.edu.edgekey.net: type CNAME, class IN, cname e7086.b.akamaiedge.net

e7086.b.akamaiedge.net: type A, class IN, addr 23.210.70.151

15. Screenshot



**nslookup –type=NS mit.edu**

Frame 206: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface 0

Ethernet II, Src: Apple\_42:b4:d4 (b8:e8:56:42:b4:d4), Dst: Cisco-Li\_b6:ac:38 (20:aa:4b:b6:ac:38)

Internet Protocol Version 4, Src: 192.168.1.109 (192.168.1.109), Dst: 75.75.75.75 (75.75.75.75)

User Datagram Protocol, Src Port: 53313 (53313), Dst Port: domain (53)

Domain Name System (query)

[Response In: 207]

Transaction ID: 0x3d5d

Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

Queries

mit.edu: type NS, class IN

Frame 207: 374 bytes on wire (2992 bits), 374 bytes captured (2992 bits) on interface 0

Ethernet II, Src: Cisco-Li\_b6:ac:38 (20:aa:4b:b6:ac:38), Dst: Apple\_42:b4:d4 (b8:e8:56:42:b4:d4)

Internet Protocol Version 4, Src: 75.75.75.75 (75.75.75.75), Dst: 192.168.1.109 (192.168.1.109)

User Datagram Protocol, Src Port: domain (53), Dst Port: 53313 (53313)

Domain Name System (response)

[Request In: 206]

[Time: 0.016274000 seconds]

Transaction ID: 0x3d5d

Flags: 0x8180 Standard query response, No error

Questions: 1

Answer RRs: 8

Authority RRs: 0

Additional RRs: 8

Queries

mit.edu: type NS, class IN

Answers

mit.edu: type NS, class IN, ns usw2.akam.net

mit.edu: type NS, class IN, ns use2.akam.net

mit.edu: type NS, class IN, ns asia1.akam.net

mit.edu: type NS, class IN, ns asia2.akam.net

mit.edu: type NS, class IN, ns use5.akam.net

mit.edu: type NS, class IN, ns ns1-173.akam.net

mit.edu: type NS, class IN, ns eur5.akam.net

mit.edu: type NS, class IN, ns ns1-37.akam.net

Additional records

use2.akam.net: type A, class IN, addr 23.62.62.195

asia1.akam.net: type A, class IN, addr 96.7.251.129

asia2.akam.net: type A, class IN, addr 195.10.36.47

use5.akam.net: type A, class IN, addr 2.16.40.64

use5.akam.net: type AAAA, class IN, addr 2600:1401:1::64

ns1-173.akam.net: type A, class IN, addr 193.108.91.173

eur5.akam.net: type A, class IN, addr 23.74.25.64

usw2.akam.net: type A, class IN, addr 184.26.161.64

16. The DNS query is sent to 75.75.75.75. It is same as the default local DNS server.

17. The DNS query type is Standard Query. It has no answers in the query message.

18. The DNS response provides

use2.akam.net

asia1.akam.net

asia2.akam.net

use5.akam.net

use5.akam.net

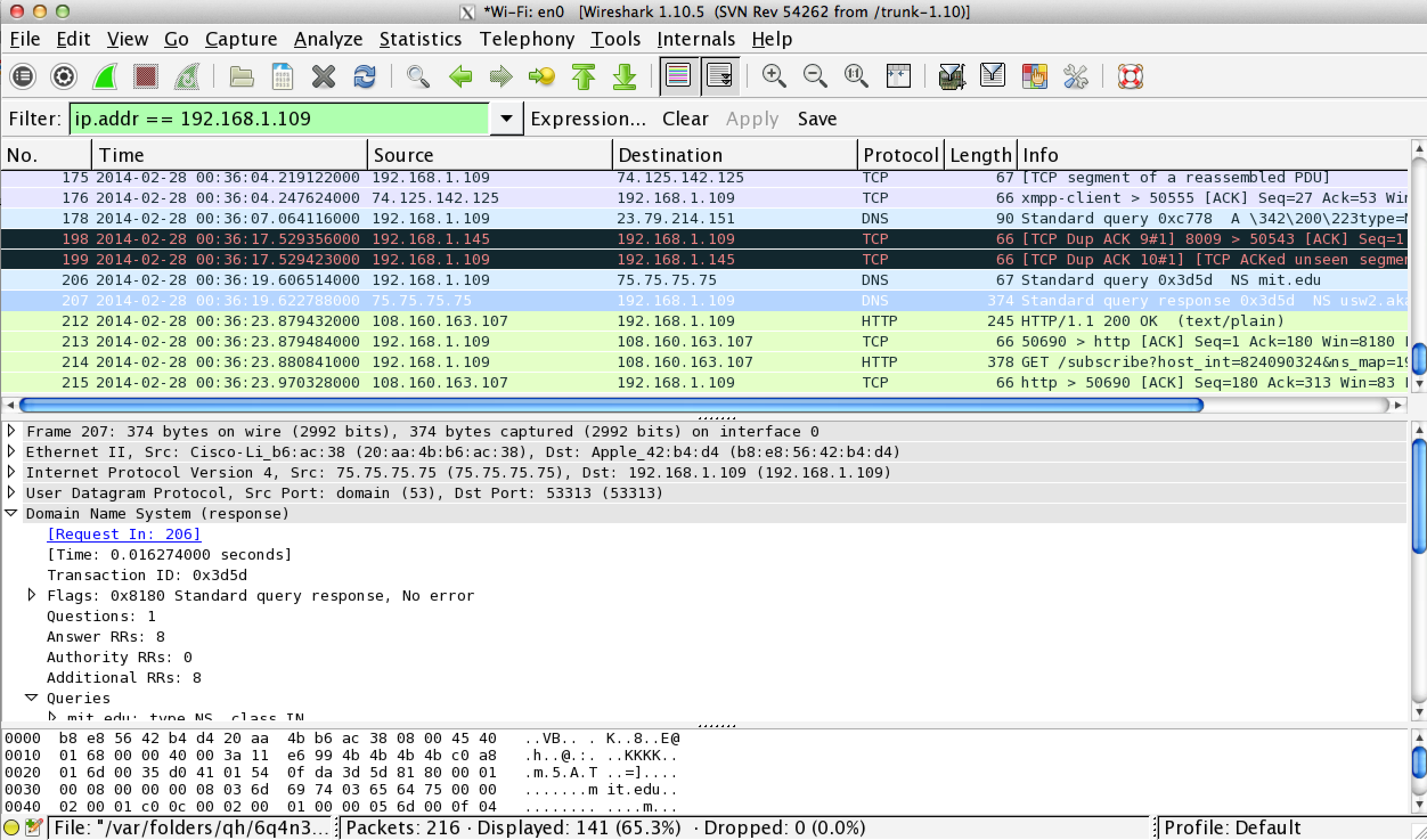
ns1-173.akam.net

eur5.akam.net

usw2.akam.net

It also provides IP addresses.

19. Screenshot



**nslookup www.aiit.or.kr bitsy.mit.edu**

Frame 64: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0

Ethernet II, Src: Apple\_42:b4:d4 (b8:e8:56:42:b4:d4), Dst: Cisco-Li\_b6:ac:38 (20:aa:4b:b6:ac:38)

Internet Protocol Version 4, Src: 192.168.1.109 (192.168.1.109), Dst: 18.72.0.3 (18.72.0.3)

User Datagram Protocol, Src Port: 54812 (54812), Dst Port: domain (53)

Domain Name System (query)

Transaction ID: 0xc585

Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

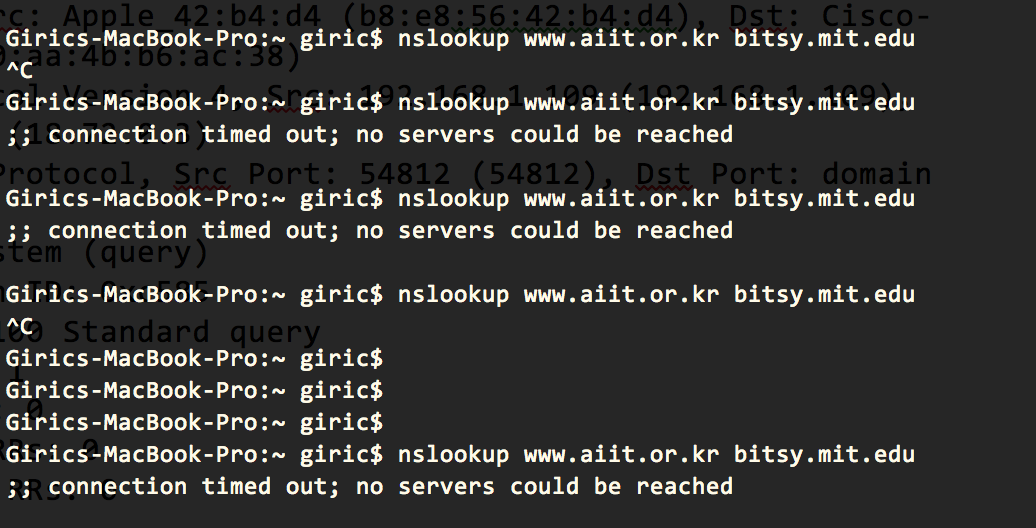
Queries

www.aiit.or.kr: type A, class IN

20. The DNS query message is sent to 18.72.0.3. It is not the same as my default local DNS. It corresponds to bitsy.mit.edu

21. The DNS response is of Standard Query type. It has no responses.

22. Couldn’t get the response message since the connection timed out.



23. Screenshot

