

Lab2 Report – Xinyu Yun (xyun@uwo.ca)

Wireshark Lab: HTTP v6.1

1. The Basic HTTP GET/response interaction

Request Details:

The screenshot shows the Wireshark interface with the following details:

- Filter:** http
- Selected Row (Frame 859):**
 - Source: 128.119.245.12
 - Destination: 172.30.86.149
 - Protocol: HTTP
 - Length: 554
 - Info: HTTP/1.1 200 OK (text/html)
- Request Headers:**
 - GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
 - Host: gaia.cs.umass.edu
 - Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
 - User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/46.0.2490.71 Safari/537.36
 - Accept-Encoding: gzip, deflate, sdch
 - Accept-Language: zh-CN,zh;q=0.8,zh-en;q=0.6,zh-TW;q=0.4
- Full request URL:** <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html>
- Text item (text), 56 bytes:** [REDACTED]

Response details:

The screenshot shows the Wireshark interface with the following details:

- Selected Row (Frame 859):**
 - Source: 128.119.245.12
 - Destination: 172.30.86.149
 - Protocol: HTTP
 - Length: 554
 - Info: HTTP/1.1 200 OK (text/html)
- Response Headers:**
 - HTTP/1.1 200 OK
 - Date: Tue, 20 Oct 2015 19:50:09 GMT
 - Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2e-fips PHP/5.4.16 mod_perl/2.0.9dev Perl/v5.16.3
 - Last-Modified: Tue, 20 Oct 2015 05:59:01 GMT
 - ETag: "80-52282f55df712"
 - Accept-Ranges: bytes
 - Content-Length: 128
 - Keep-Alive: timeout=5, max=100
 - Connection: Keep-Alive
 - Content-Type: text/html; charset=UTF-8
- Text item (text), 56 bytes:** [REDACTED]

1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?

Answer: my browser is running HTTP 1.1; the response package also shows the HTTP version is 1.1.

2. What languages (if any) does your browser indicate that it can accept to the server?

Answer: As showed in request header:

"Accept-Language:zh-CN,zh;q=0.8,en;q=0.6,zh-TW;q=0.4", the browser will support both English and Chinese.

3. What is the IP address of your computer? Of the gaia.cs.umass.edu server?

Answer: in the request package, my IP is the source "172.30.86.149"; the destination IP of the server is "128.119.245.12"

4. What is the status code returned from the server to your browser?

Answer: As shown in response package: Status Code: 200

5. When was the HTML file that you are retrieving last modified at the server?

Answer: Last-Modified: Tue, 20 Oct 2015 05:59:01 GMT

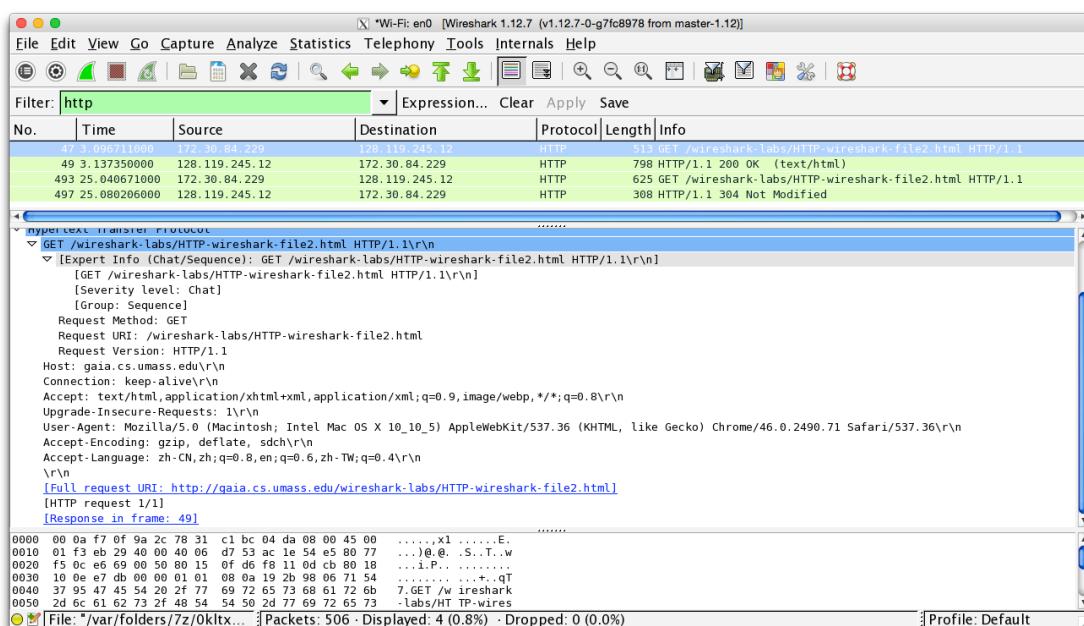
6. How many bytes of content are being returned to your browser?

Answer: Content length: 128

7. By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one.

Answer: As I check, all the message in [] will not be displayed in raw data.

2. The HTTP CONDITIONAL GET/response interaction



8. Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE” line in the HTTP GET?

Answer: No, I do not see the line in first HTTP GET message.

9. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?

Answer: yes, the server explicitly return the contents of HTML file. I can tell from the response context with <html> and 5 lines content.

Frame	Source IP	Destination IP	Protocol	Status
49 3.137350000	128.119.245.12	172.30.84.229	HTTP	798 HTTP/1.1 200 OK (text/html)
493 25.040671000	172.30.84.229	128.119.245.12	HTTP	625 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP
497 25.080206000	128.119.245.12	172.30.84.229	HTTP	308 HTTP/1.1 304 Not Modified

```

Accept-Ranges: bytes\r\n
Content-Length: 371\r\n
Keep-Alive: timeout=5, 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: 0.040639000 seconds]
[Request in frame: 47]

```

Line-based text data: text/html

```

<n
<html>\n
<n
Congratulations again! Now you've downloaded the file lab2-2.html. <br>\n
This file's last modification date will not change. <p>\n
Thus if you download this multiple times on your browser, a complete copy <br>\n
will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE<br>\n
field in your browser's HTTP GET request to the server.\n
<n
</html>\n

```

10. Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE:” line in the HTTP GET? If so, what information follows the “IF-MODIFIED-SINCE:” header?

Answer: yes I see the line from second HTTP GET:

If-Modified-Since: Wed, 21 Oct 2015 05:59:01 GMT

11. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.

Answer: in the second HTTP GET, the status is: HTTP/1.1 304 Not Modified
The server did not return any content for HTML file, judging from the length of response and details bellowed:

Frame	Source IP	Destination IP	Protocol	Status
497 25.080206000	128.119.245.12	172.30.84.229	HTTP	308 HTTP/1.1 304 Not Modified

```

Frame 497: 308 bytes on wire (2464 bits), 308 bytes captured (2464 bits) on interface 0
Ethernet II, Src: Broadcom_0f:9a:2c (00:0a:f7:0f:9a:2c), Dst: Apple_bc:04:da (78:31:c1:bc:04:da)
Internet Protocol Version 4, Src: 128.119.245.12 (128.119.245.12), Dst: 172.30.84.229 (172.30.84.229)
Transmission Control Protocol, Src Port: 80 (80), Dst Port: 58990 (58990), Seq: 1, Ack: 560, Len: 242

```

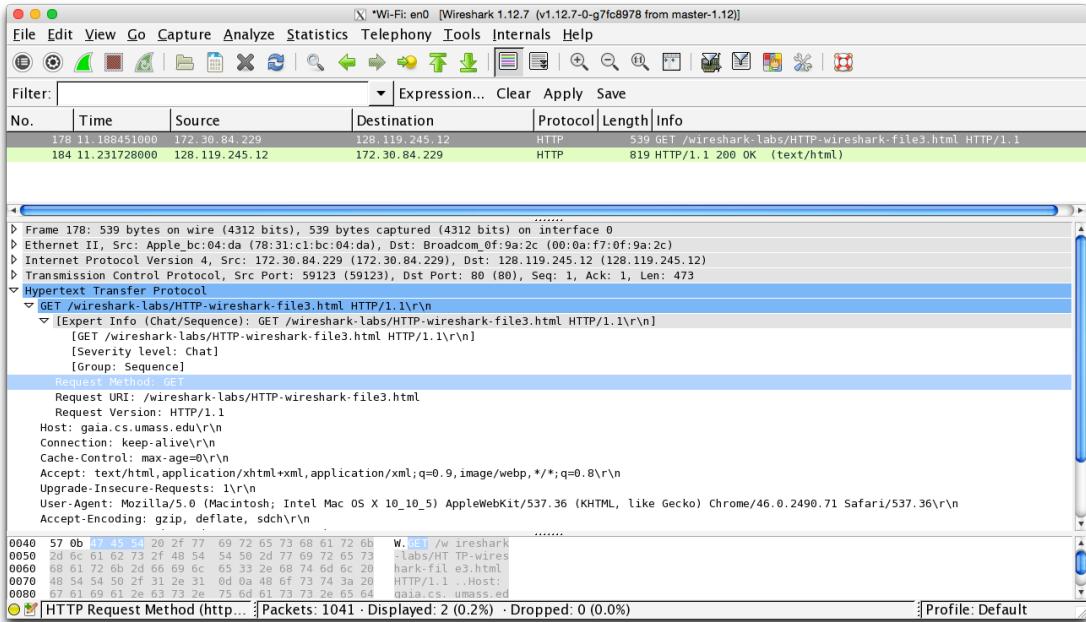
Hypertext Transfer Protocol

```

HTTP/1.1 304 Not Modified\r\n
Date: Wed, 21 Oct 2015 13:56:06 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2e-fips PHP/5.4.16 mod_perl/2.0.9dev Perl/v5.16.3\r\n
Connection: Keep-Alive\r\n
Keep-Alive: timeout=5, max=100\r\n
ETag: "173-52297134120c6"\r\n
\r\n
[HTTP response 1/1]
[Time since request: 0.039535000 seconds]
[Request in frame: 493]

```

3. Retrieving Long Documents



12. How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill or Rights?

Answer: Only 1 HTTP GET message was sent, and the packet number is 178.

13. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?

Answer: NO 184 packet contains the status code to response the HTTP GET request.

14. What is the status code and phrase in the response?

Answer: Status Code: 200

15. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?

Answer: as shown bellowed, 4 TCP segments carry all messages of the response and the text.

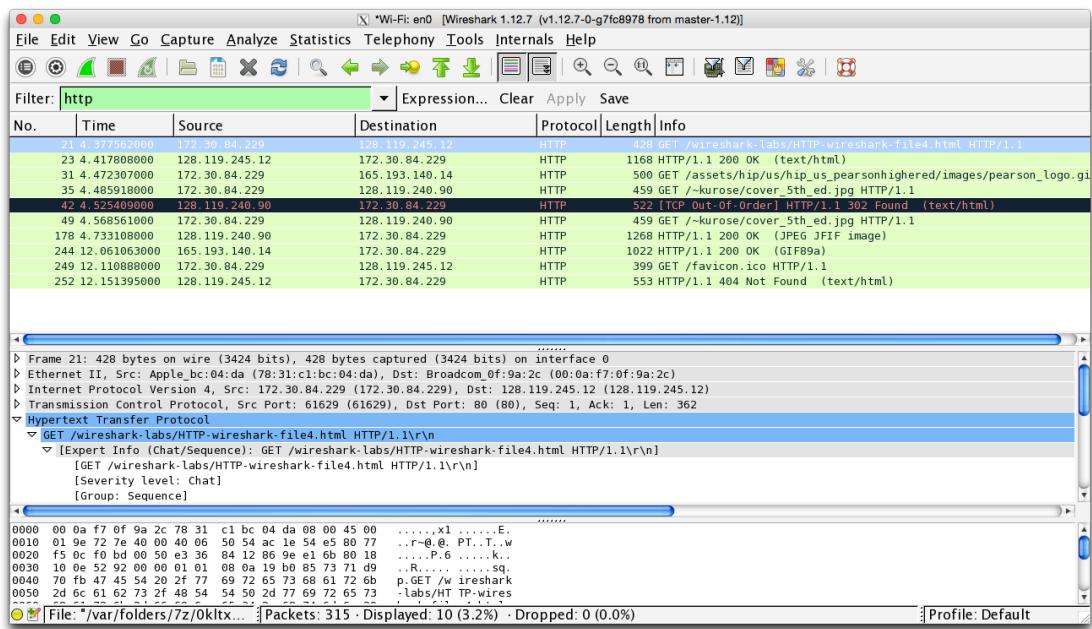
No.	Time	Source	Destination	Protocol
178	11.188451000	172.30.84.229	128.119.245.12	HTTP
184	11.231728000	128.119.245.12	172.30.84.229	HTTP

```

Window size value: 122
[Calculated window size: 15616]
[Window size scaling factor: 128]
▷ Checksum: 0x446c [validation disabled]
Urgent pointer: 0
▷ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
▷ [SEQ/ACK analysis]
TCP segment data (753 bytes)
▽ [4 Reassembled TCP Segments (4863 bytes): #180(1370), #181(1370), #183(1370), #184(71)]
  [Frame: 180, payload: 0-1369 (1370 bytes)]
  [Frame: 181, payload: 1370-2739 (1370 bytes)]
  [Frame: 183, payload: 2740-4109 (1370 bytes)]
  [Frame: 184, payload: 4110-4862 (753 bytes)]
  [Segment count: 4]
  [Reassembled TCP length: 4863]
  [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a2057...]
▽ Hypertext Transfer Protocol
  ▽ HTTP/1.1 200 OK\r\n
    ▽ [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
      [HTTP/1.1 200 OK\r\n]
0000 48 54 54 50 2f 31 2e 31 20 32 30 30 20 4f 4b 0d  HTTP/1.1 200 OK.
0010 0a 44 61 74 65 3a 20 57 65 64 2c 20 32 31 20 4f  .Date: W ed, 21 O
0020 63 74 20 32 30 31 35 20 31 34 3a 34 31 3a 34 35  ct 2015 14:41:45

```

4. HTML Documents with Embedded Objects



16. How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?

Answer: As shown from above screenshot, except the GET request to 'GET /favicon.ico' there are 4 HTTP GET requests have been sent to 3 destinations:

1. To 128.119.245.12 to get the html page
 2. To 165.193.140.14 to retrieve the pearson_logo.gif
 3. To 172.30.84.299 to retrieve cover_5th_ed.jpg, request has been sent twice because the first GET request got the '302 Found'
17. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain.

Answer: As checked the image files are transferred in TCP layer through the same port 80, so the images downloading is serially.

179.4.733108000	128.119.240.90	172.30.84.229	HTTP	1268 HTTP/1.1 200 OK (JPEG/JFIF image)
244.12.061063000	165.193.140.14	172.30.84.229	HTTP	1022 HTTP/1.1 200 OK (GIF89a)
249.12.110888000	172.30.84.229	128.119.245.12	HTTP	399 GET /favicon.ico HTTP/1.1
252.12.151395000	128.119.245.12	172.30.84.229	HTTP	553 HTTP/1.1 404 Not Found (text/html)

Frame 178: 1268 bytes on wire (10144 bits), 1268 bytes captured (10144 bits) on interface 0
Ethernet II, Src: Broadcom_0f:9a:2c (00:0a:f7:0f:9a:2c), Dst: Apple_bc:04:da (78:31:c1:bc:04:da)
Internet Protocol Version 4, Src: 128.119.240.90 (128.119.240.90), Dst: 172.30.84.229 (172.30.84.229)
Transmission Control Protocol, Src Port: 80 (80), Dst Port: 61633 (61633), Seq: 100011, Ack: 394, Len: 1202
Source Port: 80 (80)
Destination Port: 61633 (61633)
[Stream index: 14]
[TCP Segment Len: 1202]
Sequence number: 100011 (relative sequence number)
[Next sequence number: 101213 (relative sequence number)]
Acknowledgment number: 394 (relative ack number)

244.12.061063000	165.193.140.14	172.30.84.229	HTTP	1022 HTTP/1.1 200 OK (GIF89a)
249.12.110888000	172.30.84.229	128.119.245.12	HTTP	399 GET /favicon.ico HTTP/1.1
252.12.151395000	128.119.245.12	172.30.84.229	HTTP	553 HTTP/1.1 404 Not Found (text/html)

Frame 244: 1022 bytes on wire (8176 bits), 1022 bytes captured (8176 bits) on interface 0
Ethernet II, Src: Broadcom_0f:9a:2c (00:0a:f7:0f:9a:2c), Dst: Apple_bc:04:da (78:31:c1:bc:04:da)
Internet Protocol Version 4, Src: 165.193.140.14 (165.193.140.14), Dst: 172.30.84.229 (172.30.84.229)
Transmission Control Protocol, Src Port: 80 (80), Dst Port: 61631 (61631), Seq: 1635, Ack: 435, Len: 956
Source Port: 80 (80)
Destination Port: 61631 (61631)
[Stream index: 12]
[TCP Segment Len: 956]
Sequence number: 1635 (relative sequence number)
[Next sequence number: 2591 (relative sequence number)]
Acknowledgment number: 435 (relative ack number)

5 HTTP Authentications

18. What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser?

Answer: as shown bellowed, the initial response from destination server is: 401 Unauthorized

Wireshark 1.12.7 (v1.12.7-0-g7fc8978 from master-1.12)						
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help						
Filter: http Expression... Clear Apply Save						
No.	Time	Source	Destination	Protocol	Length	Info
153	43.964801000	172.30.84.229	128.119.245.12	HTTP	529	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5
155	44.005318000	128.119.245.12	172.30.84.229	HTTP	785	HTTP/1.1 401 Unauthorized (text/html)
172	56.887146000	172.30.84.229	128.119.245.12	HTTP	588	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5
174	56.928574000	128.119.245.12	172.30.84.229	HTTP	558	HTTP/1.1 200 OK (text/html)

Frame 155: 785 bytes on wire (6280 bits), 785 bytes captured (6280 bits) on interface 0						
Frame 155: 785 bytes on wire (6280 bits), 785 bytes captured (6280 bits) on interface 0						
Ethernet II, Src: Broadcom_0f:9a:2c (00:0a:f7:0f:9a:2c), Dst: Apple_bc:04:da (78:31:c1:bc:04:da)						
Internet Protocol Version 4, Src: 128.119.245.12 (128.119.245.12), Dst: 172.30.84.229 (172.30.84.229)						
Transmission Control Protocol, Src Port: 80 (80), Dst Port: 62632 (62632), Seq: 1, Ack: 464, Len: 719						
HyperText Transfer Protocol						
HTTP/1.1 401 Unauthorized\r\n						
[Expert Info (Chat/Sequence): HTTP/1.1 401 Unauthorized\r\n]						
Request Version: HTTP/1.1						
Status Code: 401						
Response Phrase: Unauthorized						
Date: Wed, 21 Oct 2015 17:10:19 GMT\r\n						
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2e-fips PHP/5.4.16 mod_perl/2.0.9dev Perl/v5.16.3\r\n						
Content-Type: text/html; charset=UTF-8\r\n						
0000	78 31 c1 bc 04 da 00 0a f7 0f 9a 2c 08 00 45 28 x1..... . . . E					
0010	03 02 0b 03 40 00 2e 06 c8 42 80 77 f5 0c ac 1e .. .@... .B.w...					
0020	54 e5 00 50 f4 a8 91 b3 50 11 17 3e 28 d8 80 18 T.P.... P.>{...					

19. When your browser's sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?

Answer: compared to the first GET request, new field called Authorization is included with the basic token and credentials message:

Filter: http						
No.	Time	Source	Destination	Protocol	Length	Info
153	43.964801000	172.30.84.229	128.119.245.12	HTTP	529	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5
155	44.005318000	128.119.245.12	172.30.84.229	HTTP	785	HTTP/1.1 401 Unauthorized (text/html)
172	56.887146000	172.30.84.229	128.119.245.12	HTTP	588	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5
174	56.928574000	128.119.245.12	172.30.84.229	HTTP	558	HTTP/1.1 200 OK (text/html)

Host: gaia.cs.umass.edu\r\nConnection: keep-alive\r\nAuthorization: Basic d2lyZXNoYXJrLXN0dWlbnRz0m5ldHdvcm5=						
Credentials: wireshark-students:network						
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n						
Upgrade-Insecure-Requests: 1\r\n						
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/46.0.2490.71 Safari/537.36\r\n						
Accept-Encoding: gzip, deflate, sdch\r\n						
Accept-Language: zh-CN,zh;q=0.8,en;q=0.6,zh-TW;q=0.4\r\n						
\r\n						
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html]						
[HTTP request 1/1]						

Wireshark Lab: DNS v6.01

1. Nslookup

- nslookup www.mit.edu

```
XinyuYun:~ duoduo$ nslookup
> www.mit.edu
Server:      172.30.80.1
Address:     172.30.80.1#53

Non-authoritative answer:
www.mit.edu canonical name = www.mit.edu.edgekey.net.
www.mit.edu.edgekey.net canonical name = e9566.dscb.akamaiedge.net.
Name:   e9566.dscb.akamaiedge.net
Address: 184.86.32.128

- nslookup -type=NS mit.edu
```

```
XinyuYun:~ duoduo$ nslookup -type=NS mit.edu
Server:      172.30.80.1
Address:     172.30.80.1#53

Non-authoritative answer:
mit.edu nameserver = usw2.akam.net.
mit.edu nameserver = asia2.akam.net.
mit.edu nameserver = use5.akam.net.
mit.edu nameserver = ns1-37.akam.net.
mit.edu nameserver = ns1-173.akam.net.
mit.edu nameserver = eur5.akam.net.
mit.edu nameserver = asia1.akam.net.
mit.edu nameserver = use2.akam.net.

Authoritative answers can be found from:
eur5.akam.net  internet address = 23.74.25.64
use2.akam.net   internet address = 96.7.49.64
use5.akam.net   internet address = 2.16.40.64
usw2.akam.net   internet address = 184.26.161.64
asia1.akam.net  internet address = 95.100.175.64
asia2.akam.net  internet address = 95.101.36.64
ns1-37.akam.net internet address = 193.108.91.37
ns1-173.akam.net internet address = 193.108.91.173
```

- nslookup www.aiit.or.kr bitsy.mit.edu (**no servers could be reached!**)

1. Run nslookup to obtain the IP address of a Web server in Asia. What is the IP address of that server?

Answer: I picked 'www.yhd.cn' to test, 2 mapping IP addresses are found as shown bellowed:

```
XinyuYun:~ duoduo$ nslookup www.yhd.cn
Server:      172.30.80.1
Address:     172.30.80.1#53

Non-authoritative answer:
Name:   www.yhd.cn
Address: 50.117.116.117
Name:   www.yhd.cn
Address: 50.117.120.253
```

XinyuYun:~ duoduo\$ █

- Run nslookup to determine the authoritative DNS servers for a university in Europe.

Answer: I select Humboldt-Universität in Berlin(hu-berlin.de) to test, the authoritative DNS servers listed as bellowed:

```
XinyuYun:~ duoduo$ nslookup -type=NS hu-berlin.de
Server:      192.168.199.1
Address:     192.168.199.1#53

Non-authoritative answer:
hu-berlin.de      nameserver = suncom.rz.hu-berlin.de.
hu-berlin.de      nameserver = ws-was.win-ip.dfn.de.
hu-berlin.de      nameserver = ns.tu-berlin.de.
hu-berlin.de      nameserver = hpcom.rz.hu-berlin.de.
hu-berlin.de      nameserver = buffy.cms.hu-berlin.de.

Authoritative answers can be found from:
ns.tu-berlin.de  internet address = 130.149.7.7
buffy.cms.hu-berlin.de  internet address = 141.20.2.3
hpcom.rz.hu-berlin.de  internet address = 141.20.1.3
hpcom.rz.hu-berlin.de  has AAAA address 2001:638:813:1::3
suncom.rz.hu-berlin.de  internet address = 141.20.1.31
ws-was.win-ip.dfn.de  internet address = 193.174.75.110
ws-was.win-ip.dfn.de  internet address = 193.174.75.126
```

- Run nslookup so that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! mail. What is its IP address?

Answer: Here I selected the last DNS server ‘ws-was.win-ip.dfn.de’ from results in Question 2 as the specific DNS server to query the yahoo mail server ‘mail.yahoo.com’; the result bellowed shows the mail server’s IP is 188.125.80.138.

```
XinyuYun:~ duoduo$ nslookup mail.yahoo.com ws-was.win-ip.dfn.de
Server:      ws-was.win-ip.dfn.de
Address:     193.174.75.126#53

Non-authoritative answer:
mail.yahoo.com canonical name = login.yahoo.com.
login.yahoo.com canonical name = fo-ds-ats.member.g02.yahoodns.net.
Name:      fo-ds-ats.member.g02.yahoodns.net
Address:   188.125.80.138
```

2. Ipconfig

Answer: in Mac OS, I used ‘ifconfig’ to test:

```

XinyuYun:~ duoduo$ ifconfig -a
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
    options=3<RXCSUM,TXCSUM>
    inet6 ::1 prefixlen 128
        inet 127.0.0.1 netmask 0xff000000
    inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
        nd6 options=1<PERFORMNUD>
gif0: flags=8010<POINTOPOINT,MULTICAST> mtu 1280
stf0: flags=0<> mtu 1280
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    ether 78:31:c1:bc:04:da
    inet6 fe80::7a31:c1ff:febc:4da%en0 prefixlen 64 scopeid 0x4
        inet 192.168.199.214 netmask 0xfffffff0 broadcast 192.168.199.255
        nd6 options=1<PERFORMNUD>
    media: autoselect
    status: active
en1: flags=8963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
    options=60<TS04,TS06>
    ether 72:00:02:3f:d3:90
    media: autoselect <full-duplex>
    status: inactive
en2: flags=8963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
    options=60<TS04,TS06>
    ether 72:00:02:3f:d3:91
    media: autoselect <full-duplex>
    status: inactive
bridge0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    options=63<RXCSUM,TXCSUM,TS04,TS06>
    ether 7a:31:c1:cb:9a:00
    Configuration:
        id 0:0:0:0:0:0 priority 0 hellotime 0 fwddelay 0
        maxage 0 holdcnt 0 proto stp maxaddr 100 timeout 1200
        root id 0:0:0:0:0:0 priority 0 ifcost 0 port 0
        ipfilter disabled flags 0x2
    member: en1 flags=3<LEARNING,DISCOVER>
        ifmaxaddr 0 port 5 priority 0 path cost 0
    member: en2 flags=3<LEARNING,DISCOVER>
        ifmaxaddr 0 port 6 priority 0 path cost 0
    nd6 options=1<PERFORMNUD>
    media: <unknown type>
    status: inactive
p2p0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 2304
    ether 0a:31:c1:bc:04:da
    media: autoselect
    status: inactive
awdl0: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1452
    ether 2e:c2:74:7d:eb:70
    inet6 fe80::2cc2:74ff:fe7d:eb70%awdl0 prefixlen 64 scopeid 0x9
        nd6 options=1<PERFORMNUD>

```

In my laptop I checked the /etc/resolv.conf to find my DNS cache:

```

XinyuYun:~ duoduo$ cat /etc/resolv.conf
#
# Mac OS X Notice
#
# This file is not used by the host name and address resolution
# or the DNS query routing mechanisms used by most processes on
# this Mac OS X system.
#
# This file is automatically generated.
#
domain lan
nameserver 192.168.199.1
XinyuYun:~ duoduo$ █

```

and scutil –dns to display all DNS configurations:

```
XinyuYun:~ duoduo$ scutil --dns
DNS configuration

resolver #1
    search domain[0] : lan
    nameserver[0] : 192.168.199.1
    if_index : 4 (en0)
    flags : Request A records
    reach : Reachable,Directly Reachable Address

resolver #2
    domain : local
    options : mdns
    timeout : 5
    flags : Request A records
    order : 300000

resolver #3
    domain : 254.169.in-addr.arpa
    options : mdns
    timeout : 5
    flags : Request A records
    order : 300200

resolver #4
    domain : 8.e.f.ip6.arpa
    options : mdns
    timeout : 5
    flags : Request A records
    order : 300400

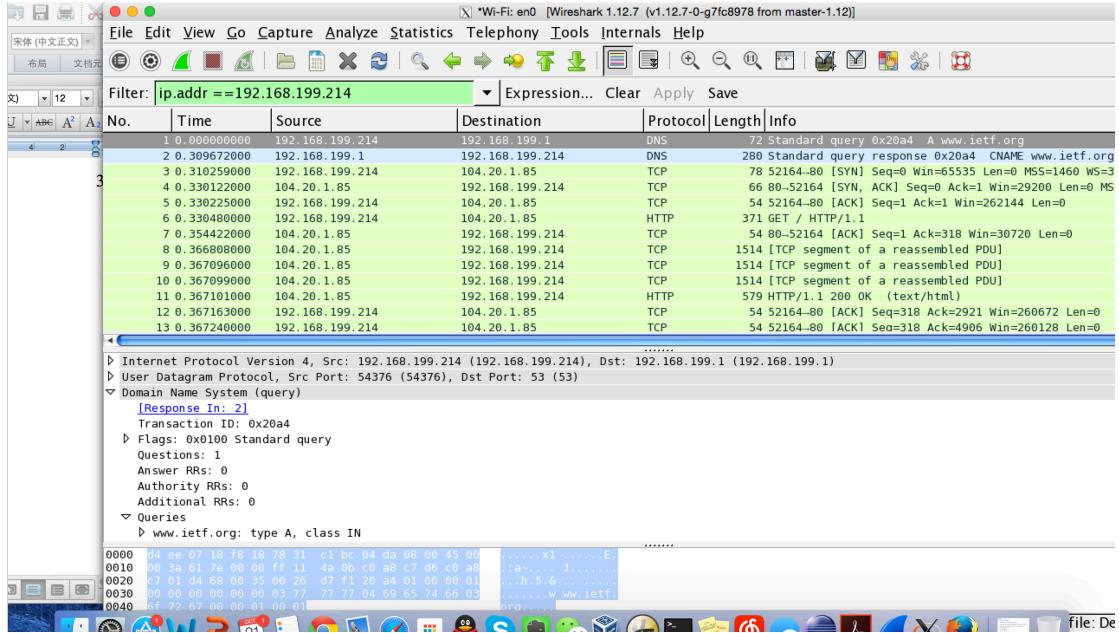
resolver #5
    domain : 9.e.f.ip6.arpa
    options : mdns
    timeout : 5
    flags : Request A records
    order : 300600

resolver #6
    domain : a.e.f.ip6.arpa
    options : mdns
    timeout : 5
    flags : Request A records
    order : 300800

resolver #7
```

In Mac OS 10.10, this command is used to flush DNS cache: sudo killall -HUP mDNSResponder

3. Tracing DNS with Wireshark

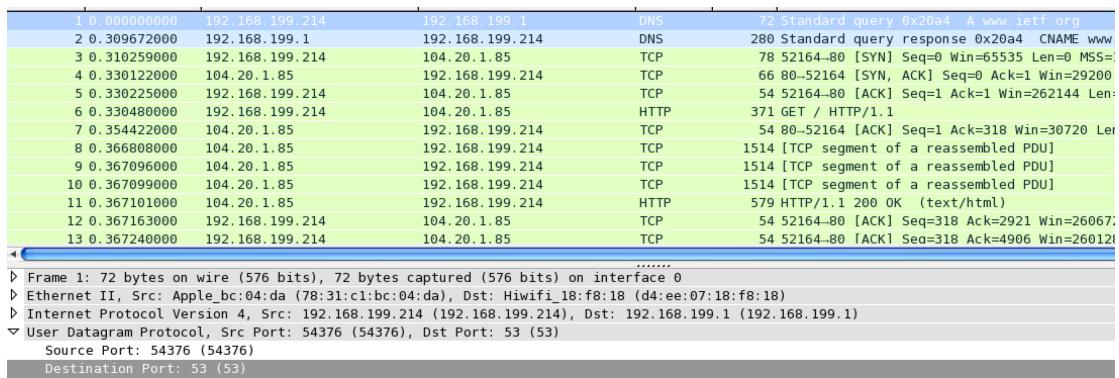


- Locate the DNS query and response messages. Are they sent over UDP or TCP?

Answer: after the DNS query response, the messages then sent over UDP.

- What is the destination port for the DNS query message? What is the source port of DNS response message?

Answer: the destination port for DNS query message is 53. So is the same port for DNS response message, 53.



2 0.309672000	192.168.199.1	192.168.199.214	DNS	280 Standard query response 0x20a4 CNAME www.ietf.org
3 0.310259000	192.168.199.214	104.20.1.85	TCP	78 52164-80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=3
4 0.330122000	104.20.1.85	192.168.199.214	TCP	66 80-52164 [SYN, ACK] Seq=1 Ack=1 Win=29200 Len=0 MS
5 0.330225000	192.168.199.214	104.20.1.85	TCP	54 52164-80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
6 0.330480000	192.168.199.214	104.20.1.85	HTTP	371 GET / HTTP/1.1
7 0.354422000	104.20.1.85	192.168.199.214	TCP	54 80-52164 [ACK] Seq=1 Ack=318 Win=30720 Len=0
8 0.366808000	104.20.1.85	192.168.199.214	TCP	1514 [TCP segment of a reassembled PDU]
9 0.367096000	104.20.1.85	192.168.199.214	TCP	1514 [TCP segment of a reassembled PDU]
10 0.367099000	104.20.1.85	192.168.199.214	TCP	1514 [TCP segment of a reassembled PDU]
11 0.367101000	104.20.1.85	192.168.199.214	HTTP	579 HTTP/1.1 200 OK (text/html)
12 0.367163000	192.168.199.214	104.20.1.85	TCP	54 52164-80 [ACK] Seq=318 Ack=2921 Win=260672 Len=0
13 0.367240000	192.168.199.214	104.20.1.85	TCP	54 52164-80 [ACK] Seq=318 Ack=4906 Win=260128 Len=0

Frame 2: 280 bytes on wire (2240 bits), 280 bytes captured (2240 bits) on interface 0
 Ethernet II, Src: Hiwifi_18:f8:18 (d4:ee:07:18:f8:18), Dst: Apple_bc:04:da (78:31:c1:bc:04:da)
 Internet Protocol Version 4, Src: 192.168.199.1 (192.168.199.1), Dst: 192.168.199.214 (192.168.199.214)
 User Datagram Protocol, Src Port: 53 (53), Dst Port: 54376 (54376)
 Source Port: 53 (53)
 Destination Port: 54376 (54376)
 Length: 246
 Checksum: 0x9bb9 [validation disabled]
 Stream index: 01

6. To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?

Answer: the destination IP is 192.168.199.1 in DNS query, which is as same as the IP in DNS resolver file saved in my Mac OS:

```
XinyuYun:~ duoduo$ cat /etc/resolv.conf
#
# Mac OS X Notice
#
# This file is not used by the host name and address resolution
# or the DNS query routing mechanisms used by most processes
# on
# this Mac OS X system.
#
# This file is automatically generated.
#
domain lan
nameserver 192.168.199.1
```

7. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

Answer: in query message, the type is A(host address)(1) meaning it will return a 32-bit IPv4 address, and the query does not contain answers.

```

▷ Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
▽ Queries
    ▽ www.ietf.org: type A, class IN
        Name: www.ietf.org
        [Name Length: 12]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)

```

8. Examine the DNS response message. How many “answers” are provided?

What does each of these answers contain?

Answer: In the response, 3 answers are provided, each of which contains Name, Type, Class, TTL, Data Length, and Address.

2 0.309672000	192.168.199.1	192.168.199.214	DNS	280 Standard query response 0x20a4
Answers				
▽ www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare-dnssec.net				
Name:	www.ietf.org	Type:	CNAME (Canonical NAME for an alias) (5)	Class: IN (0x0001)
Class:	IN (0x0001)	Time to live:	1800	Data length: 40
Data length:	40	CNAME:	www.ietf.org.cdn.cloudflare-dnssec.net	
▽ www.ietf.org.cdn.cloudflare-dnssec.net: type A, class IN, addr 104.20.1.85				
Name:	www.ietf.org.cdn.cloudflare-dnssec.net	Type:	A (Host Address) (1)	Class: IN (0x0001)
Class:	IN (0x0001)	Time to live:	300	Data length: 4
Data length:	4	Address:	104.20.1.85 (104.20.1.85)	
▽ www.ietf.org.cdn.cloudflare-dnssec.net: type A, class IN, addr 104.20.0.85				
Name:	www.ietf.org.cdn.cloudflare-dnssec.net	Type:	A (Host Address) (1)	Class: IN (0x0001)
Class:	IN (0x0001)	Time to live:	300	Data length: 4
Data length:	4	Address:	104.20.0.85 (104.20.0.85)	

9. Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?

Answer: the destination IP (104.20.0.85) in TCP [SYN] packet does correspond to the address in DNS query response answers.

3 0.310259000	192.168.199.214	104.20.1.85	TCP	78 52164-80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460
4 0.330122000	104.20.1.85	192.168.199.214	TCP	66 80-52164 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0
5 0.330225000	192.168.199.214	104.20.1.85	TCP	54 52164-80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
6 0.330480000	192.168.199.214	104.20.1.85	HTTP	371 GET / HTTP/1.1

10. This web page contains images. Before retrieving each image, does your host issue new DNS queries?

Answer: As checked the packets list, the image requests are all heading to the server 104.20.1.85, so there is no new DNS queries for GET these images.

50 0. 4407720000	192.168.199.214	104.20.1.85	HTTP	458 GET /images/jetfllogotrans.gif HTTP/1.1
51 0. 4409180000	192.168.199.214	104.20.1.85	HTTP	455 GET /images/chat-trans.png HTTP/1.1
52 0. 4410330000	192.168.199.214	104.20.1.85	HTTP	457 GET /images/openstand-md.png HTTP/1.1
53 0. 4411190000	192.168.199.214	104.20.1.85	HTTP	465 GET /meeting/94/images/yokohama2.jpg HTTP/1.1
54 0. 4411790000	192.168.199.214	104.20.1.85	HTTP	454 GET /images/isoc_logo.gif HTTP/1.1
55 0. 4415460000	192.168.199.214	104.20.1.85	HTTP	453 GET /images/ams_logo.png HTTP/1.1
80 0. 4689740000	104.20.1.85	192.168.199.214	HTTP	136 HTTP/1.1 200 OK (GIF89a) (GIF89a) (image/gif)
87 0. 4701120000	104.20.1.85	192.168.199.214	HTTP	914 HTTP/1.1 200 OK (PNG)
100 0. 4707680000	104.20.1.85	192.168.199.214	HTTP	1123 HTTP/1.1 200 OK (PNG)
130 0. 4907520000	104.20.1.85	192.168.199.214	HTTP	752 HTTP/1.1 200 OK (GIF89a) (GIF89a) (image/gif)
148 0. 4961410000	104.20.1.85	192.168.199.214	HTTP	1456 HTTP/1.1 200 OK (JPEG JFIF image)

- Start packet capture.

- Do an nslookup on www.mit.edu

- Stop packet capture.

11. What is the destination port for the DNS query message? What is the source port of DNS response message?

Answer: destination port for DNS query message is 53 and so is the source port of response message, being the port 53.

No.	Time	Source	Destination	Protocol	Length	Info
22 8. 1782740000	192.168.199.214	192.168.199.1		DNS	71	Standard query 0xf69a A www.mit.edu
23 8. 2011580000	192.168.199.1	192.168.199.214		DNS	456	Standard query response 0xf69a CNAME www.mit.edu.edgekey.net CN

Frame 22: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface 0
Ethernet II, Src: Apple_bc:04:da (78:31:c1:bc:04:da), Dst: Hiwifi_18:f8:18 (d4:ee:07:18:f8:18)
Internet Protocol Version 4, Src: 192.168.199.214 (192.168.199.214), Dst: 192.168.199.1 (192.168.199.1)
User Datagram Protocol, Src Port: 59516 (59516), Dst Port: 53 (53)
Source Port: 59516 (59516)
Destination Port: 53 (53)
Length: 37
Checksum: 0xbdb2 [validation disabled]
[Stream index: 1]
Domain Name System (query)

No.	Time	Source	Destination	Protocol	Length	Info
22 8. 1782740000	192.168.199.214	192.168.199.1		DNS	71	Standard query 0xf69a A www.mit.edu
23 8. 2011580000	192.168.199.1	192.168.199.214		DNS	456	Standard query response 0xf69a CNAME www.mit.edu.edgekey.net

Frame 23: 456 bytes on wire (3648 bits), 456 bytes captured (3648 bits) on interface 0
Ethernet II, Src: Hiwifi_18:f8:18 (d4:ee:07:18:f8:18), Dst: Apple_bc:04:da (78:31:c1:bc:04:da)
Internet Protocol Version 4, Src: 192.168.199.1 (192.168.199.1), Dst: 192.168.199.214 (192.168.199.214)
User Datagram Protocol, Src Port: 53 (53), Dst Port: 59516 (59516)
Source Port: 53 (53)
Destination Port: 59516 (59516)
Length: 422
Checksum: 0xeffb [validation disabled]
[Stream index: 1]
Domain Name System (response)

12. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

Answer: the destination IP is 192.168.199.1, which is the default DNS server.

13. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

Answer: the type of query message is also ‘A’, and the query does not contain any answers.

Filter: ip.addr == 192.168.199.214				▼ Expression...	Clear	Apply	Save
No.	Time	Source	Destination	Protocol	Length	Info	
22	8.178274000	192.168.199.214	192.168.199.1	DNS	71	Standard query	
23	8.201158000	192.168.199.1	192.168.199.214	DNS	456	Standard query response	


```

User Datagram Protocol, Src Port: 59516 (59516), Dst Port: 53 (53)
Source Port: 59516 (59516)
Destination Port: 53 (53)
Length: 37
▷ Checksum: 0xbd82 [validation disabled]
[Stream index: 1]
▽ Domain Name System (query)
  [Response In: 23]
    Transaction ID: 0xf69a
  ▷ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▷ Queries
    ▷ www.mit.edu: type A, class IN
      Name: www.mit.edu
      [Name Length: 11]
      [Label Count: 3]
      Type: A (Host Address) (1)
      Class: IN (0x0001)

```

14. Examine the DNS response message. How many “answers” are provided?

What does each of these answers contain?

Answer: There are 3 answers in response message; each of those contains name, type, class, TTL, data length, and address.

Filter: ip.addr == 192.168.199.214				▼ Expression...	Clear	Apply	Save
No.	Time	Source	Destination	Protocol	Length	Info	
22	8.178274000	192.168.199.214	192.168.199.1	DNS	71	Standard query 0xf69a A www.mit.edu	
23	8.201158000	192.168.199.1	192.168.199.214	DNS	456	Standard query response 0xf69a A www.mit.edu	

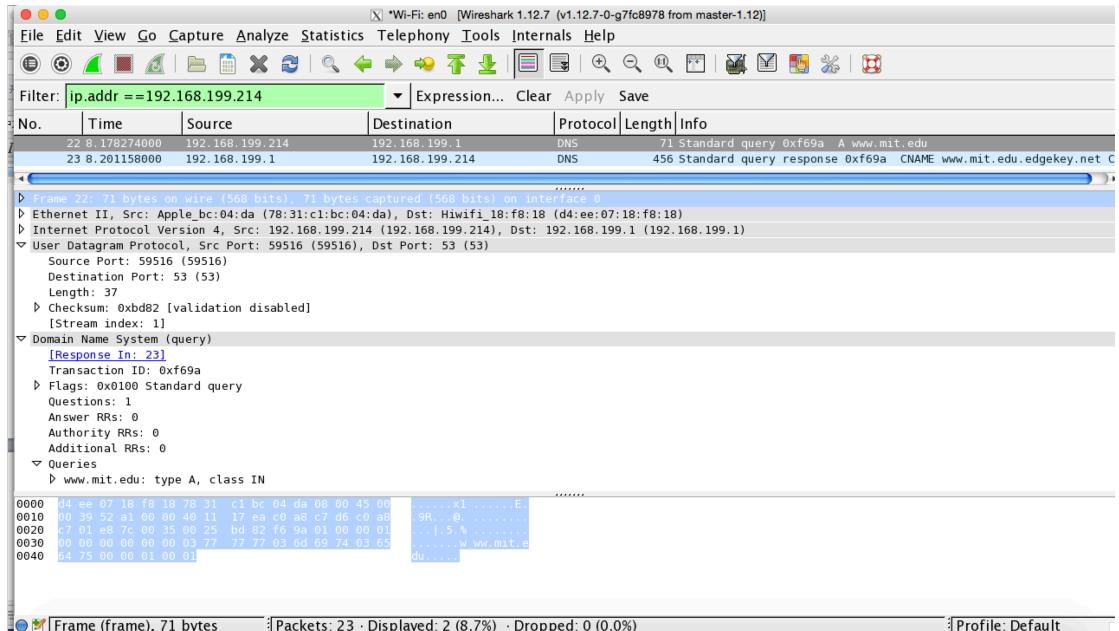

```

▽ 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: 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 A, class IN, addr 184.86.32.128
    Name: e9566.dscb.akamaiedge.net
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 20
    Data length: 4
    Address: 184.86.32.128 (184.86.32.128)

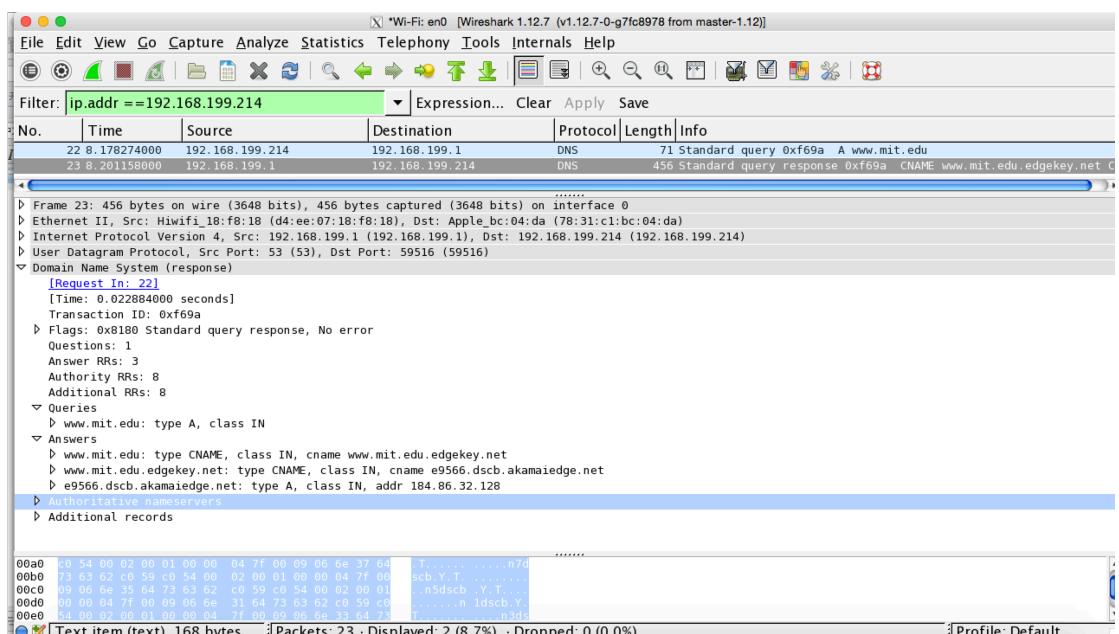
```

15. Provide a screenshot.

DNS query message:



DNS response message:



- nslookup -type=NS mit.edu**

- To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

Answer: the destination IP is also 192.168.199.1, which is my local default DNS server.

- Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

Answer: the type of query message is 'Type: NS (authoritative Name Server) (2)', and the query does not contain any answers either.

18. Examine the DNS response message. What MIT name servers does the response message provide? Does this response message also provide the IP addresses of the MIT namesers?

Answer: 8 name servers are provided as bellowed, and in the additional records section their IP addresses are provided.

▽ Answers

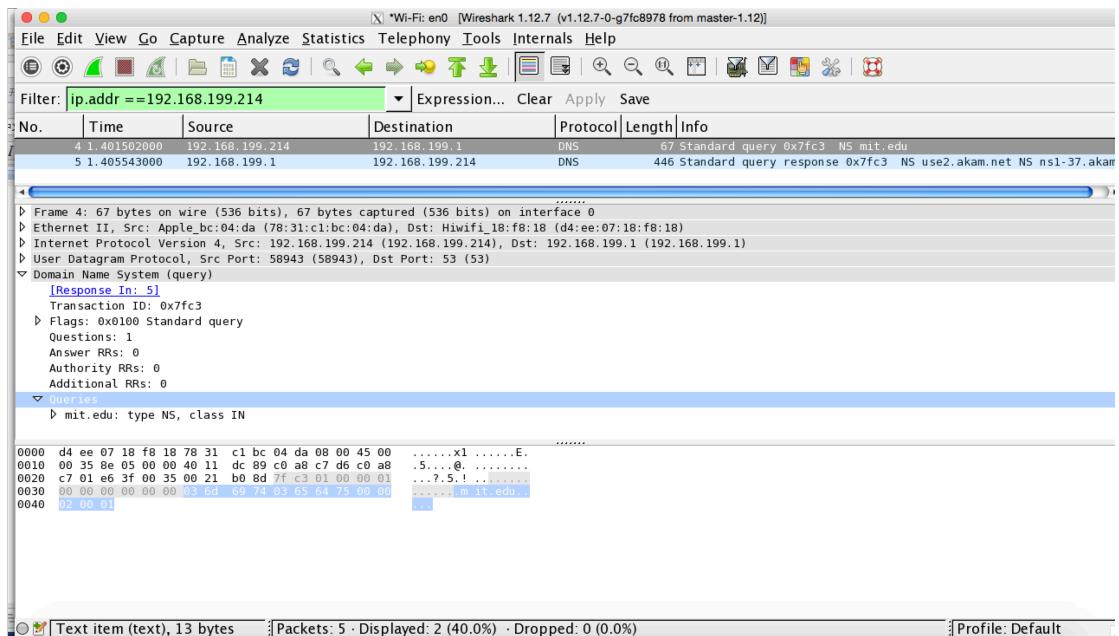
- ▷ mit.edu: type NS, class IN, ns use2.akam.net
- ▷ mit.edu: type NS, class IN, ns ns1-37.akam.net
- ▷ mit.edu: type NS, class IN, ns asia2.akam.net
- ▷ mit.edu: type NS, class IN, ns use5.akam.net
- ▷ mit.edu: type NS, class IN, ns usw2.akam.net
- ▷ mit.edu: type NS, class IN, ns asia1.akam.net
- ▷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

▽ Additional records

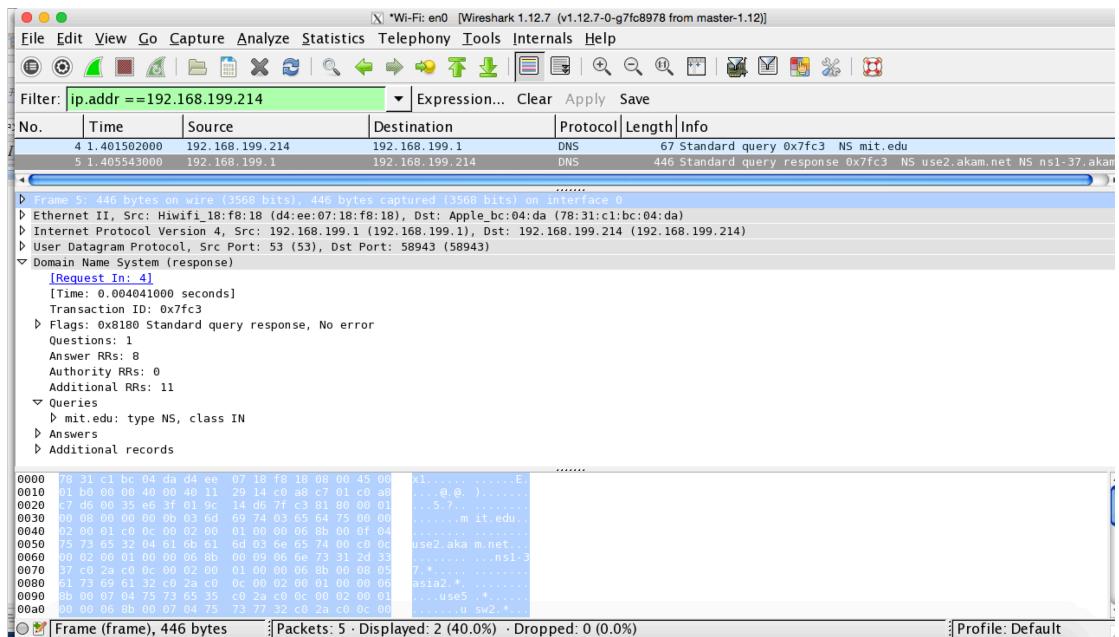
- ▷ eur5.akam.net: type A, class IN, addr 23.74.25.64
- ▷ use2.akam.net: type A, class IN, addr 96.7.49.64
- ▷ use5.akam.net: type A, class IN, addr 2.16.40.64
- ▷ use5.akam.net: type AAAA, class IN, addr 2600:1401:1::40
- ▷ usw2.akam.net: type A, class IN, addr 184.26.161.64
- ▷ asia1.akam.net: type A, class IN, addr 95.100.175.64
- ▷ asia2.akam.net: type A, class IN, addr 95.101.36.64
- ▷ ns1-37.akam.net: type A, class IN, addr 193.108.91.37
- ▷ ns1-37.akam.net: type AAAA, class IN, addr 2600:1401:2::25
- ▷ ns1-173.akam.net: type A, class IN, addr 193.108.91.173
- ▷ ns1-173.akam.net: type AAAA, class IN, addr 2600:1401:2::ad

19. Provide a screenshot.

DNS query:



DNS response:



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

Since neither the host ‘www.aiit.or.kr’ nor the name server ‘bitsy’ is available in my apartment Wifi with the Macbook.

Firstly as shown the name servers I found in previous question, the bitsy server is not included:

```
XinyuYun:~ duoduo$  
XinyuYun:~ duoduo$ nslookup -type=NS mit.edu  
Server:      192.168.199.1  
Address:     192.168.199.1#53  
  
Non-authoritative answer:  
mit.edu nameserver = use2.akam.net.  
mit.edu nameserver = ns1-37.akam.net.  
mit.edu nameserver = use5.akam.net.  
mit.edu nameserver = asia1.akam.net.  
mit.edu nameserver = eur5.akam.net.  
mit.edu nameserver = usw2.akam.net.  
mit.edu nameserver = ns1-173.akam.net.  
mit.edu nameserver = asia2.akam.net.  
  
Authoritative answers can be found from:  
eur5.akam.net  internet address = 23.74.25.64  
use2.akam.net  internet address = 96.7.49.64  
use5.akam.net  internet address = 2.16.40.64  
use5.akam.net  has AAAA address 2600:1401:1::40  
usw2.akam.net  internet address = 184.26.161.64  
asia1.akam.net  internet address = 95.100.175.64  
asia2.akam.net  internet address = 95.101.36.64  
ns1-37.akam.net  internet address = 193.108.91.37  
ns1-37.akam.net  has AAAA address 2600:1401:2::25  
ns1-173.akam.net  internet address = 193.108.91.173  
ns1-173.akam.net  has AAAA address 2600:1401:2::ad  
  
XinyuYun:~ duoduo$
```

Secondly, even I choose the found DNS servers to resolve ‘www.ait.or.kr’, the following message will returned to refuse the request.

```
XinyuYun:~ duoduo$ nslookup www.ait.or.eur5.akam.net  
Server:      eur5.akam.net  
Address:     23.74.25.64#53  
  
** server can't find www.ait.or.kr: REFUSED
```

As communicated with prof. and TA, I will use ‘www.ait.or.kr’ and another available server ‘ws-was.win-ip.dfn.de’ which I used in previous question to resolve the yahoo email server.

```
XinyuYun:~ duoduo$ nslookup www.ait.or.kr ws-was.win-ip.dfn.de  
Server:      ws-was.win-ip.dfn.de  
Address:     193.174.75.110#53  
  
Non-authoritative answer:  
Name:  www.ait.or.kr  
Address: 116.127.123.32
```

```
XinyuYun:~ duoduo$
```

20. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? If not, what does the IP address correspond to?

Answer: the IP where the query sent is 193.174.75.110, which is not my default local DNS server (192.168.199.1). The new IP corresponds to the DNS server I use in the nslookup command.

21. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

Answer: the type is A and the query does not contain any answers.

▽ Queries

▽ www.ait.or.kr: type A, class IN

Name: www.ait.or.kr

[Name Length: 13]

[Label Count: 4]

Type: A (Host Address) (1)

Class: IN (0x0001)

22. Examine the DNS response message. How many “answers” are provided?

What does each of these answers contain?

Answer: only one answer is provided in which there are name, type, class, TTL, data length, and address.

▽ Query Tree

▷ www.ait.or.kr: type A, class IN

▽ Answers

▽ www.ait.or.kr: type A, class IN, addr 116.127.123.32

Name: www.ait.or.kr

Type: A (Host Address) (1)

Class: IN (0x0001)

Time to live: 578

Data length: 4

Address: 116.127.123.32 (116.127.123.32)

23. Provide a screenshot.

DNS query:

Wi-Fi: en0 [Wireshark 1.12.7 (v1.12.7-0-g7fc8978 from master-1.12)]

Filter: ip.addr == 192.168.199.214

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.199.214	193.174.75.110	DNS	73	Standard query 0x5118 A www.ait.or.kr
2	0.112992000	193.174.75.110	192.168.199.214	DNS	180	Standard query response 0x5118 A 116.127

Frame 1: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0

Ethernet II, Src: Apple_bc:04:da (78:31:c1:bc:04:da), Dst: Hiwifi_18:f8:18 (d4:ee:07:18:f8:18)

Internet Protocol Version 4, Src: 192.168.199.214 (192.168.199.214), Dst: 193.174.75.110 (193.174.75.110)

User Datagram Protocol, Src Port: 55635 (55635), Dst Port: 53 (53)

Domain Name System (query)

[Response In: 2]

Transaction ID: 0x5118

Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

Queries

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

Name: www.ait.or.kr
[Name Length: 13]
[Label Count: 4]
Type: A (Host Address) (1)
Class: IN (0x0001)

0000 d4 ee 07 18 f8 18 78 31 c1 bc 04 da 08 00 45 00x1 ...E.
0010 00 3b 85 c2 00 40 11 5f 54 c0 a8 c7 d6 c1 ae@.T.
0020 4b 6b d9 53 00 35 00 27 74 ba 51 18 01 00 00 01 Kn.5.5.1.10.w ww.ait.o
0030 00 00 00 00 00 03 77 77 77 03 61 69 74 02 6fr.kr....
0040 72 02 6b 72 00 00 01 00 01

3. Provide a screenshot.

Frame (frame), 73 bytes | Packets: 2 · Displayed: 2 (100.0%) · Dropped: 0 (0.0%)

DNS response:

Wi-Fi: en0 [Wireshark 1.12.7 (v1.12.7-0-g7fc8978 from master-1.12)]

Filter: ip.addr == 192.168.199.214

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.199.214	193.174.75.110	DNS	73	Standard query 0x5118 A www.ait.or.kr
2	0.112992000	193.174.75.110	192.168.199.214	DNS	180	Standard query response 0x5118 A 116.127

Frame 2: 180 bytes on wire (1440 bits), 180 bytes captured (1440 bits) on interface 0

Ethernet II, Src: Hiwifi_18:f8:18 (d4:ee:07:18:f8:18), Dst: Apple_bc:04:da (78:31:c1:bc:04:da)

Internet Protocol Version 4, Src: 193.174.75.110 (193.174.75.110), Dst: 192.168.199.214 (192.168.199.214)

User Datagram Protocol, Src Port: 53 (53), Dst Port: 55635 (55635)

Domain Name System (response)

[Request In: 1]

[Time: 0.112992000 seconds]

Transaction ID: 0x5118

Flags: 0x8180 Standard query response, No error

Questions: 1

Answer RRs: 1

Authority RRs: 2

Additional RRs: 2

Queries

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

Answers

www.ait.or.kr: type A, class IN, addr 116.127.123.32

Authoritative nameservers

ait.or.kr: type NS, class IN, ns ns1.whoisweb.net

ait.or.kr: type NS, class IN, ns ns1.whois.co.kr

Additional records

ns1.whois.co.kr: type A, class IN, addr 218.232.110.171

ns1.whoisweb.net: type A, class IN, addr 218.232.110.172

0000 78 31 c1 bc 04 da d4 ee 07 18 f8 18 08 00 45 00x1 ...E.
0010 00 a6 f4 5d 40 00 f2 11 fe 4c c1 aa 4b 6e cd a8@.L.Kn.
0020 c7 d6 00 3d d9 53 00 92 68 3f 51 18 81 80 00 01S.S.170.
0030 00 01 00 02 00 02 03 77 77 77 03 61 69 74 02 6fw ww.ait.o
0040 72 02 6b 72 00 00 01 00 01 e0 00 00 01 00 00 01 r.kr....
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

3. Provide a screenshot.

Frame (frame), 180 bytes | Packets: 2 · Displayed: 2 (100.0%) · Dropped: 0 (0.0%)