Patrick Kevorkian
HW 6
Fall 2017

11/10/17

Lab 1: DNS

1) Site: https://www.baidu.com Popular asian search engine hosted in Hong Kong.

```
[Pat-Kevorkians-iMac:~ PatrickKevorkian$ nslookup https://www.baidu.com
Server:         2604:2000:1600:8007:8a1f:a1ff:fe29:6b45
Address:        2604:2000:1600:8007:8a1f:a1ff:fe29:6b45#53

Non-authoritative answer:
Name:   https://www.baidu.com
Address: 198.105.254.228
Name:   https://www.baidu.com
Address: 198.105.244.228
```

IP Address: 198.105.244.228

2) Site: www.ox.ac.uk Oxford University

```
Last login: Fri Nov 10 14:54:09 on ttys000
[Pat-Kevorkians-iMac:~ PatrickKevorkian$ nslookup
[> set query=ns
[> ox.ac.uk
Server:         2604:2000:1600:8007:8a1f:a1ff:fe29:6b45
Address:        2604:2000:1600:8007:8a1f:a1ff:fe29:6b45#53

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

Authoritative answers can be found from:
[> server ns2.ja.net
Default server: ns2.ja.net
Address: 2001:630:0:45::11#53
Default server: ns2.ja.net
Address: 193.63.105.17#53
[> set query = any
*** Invalid option: query
[> set query=any
[> ox.ac.uk
;; Truncated, retrying in TCP mode.
Server:         ns2.ja.net
Address:        2001:630:0:45::11#53

ox.ac.uk
        origin = nighthawk.dns.ox.ac.uk
        mail addr = hostmaster.ox.ac.uk
        serial = 2017111072
        refresh = 3600
        retry = 1800
        expire = 1209600
        minimum = 900
ox.ac.uk        naptr = 100 10 "s" "x-eduroam:radius.tls" "" _radsec._tcp.roaming.ja.net.
Name:   ox.ac.uk
Address: 129.67.242.154
Name:   ox.ac.uk
Address: 129.67.242.155
ox.ac.uk        afsdb = 1 db5.afs.ox.ac.uk.
ox.ac.uk        afsdb = 1 db2.afs.ox.ac.uk.
ox.ac.uk        afsdb = 1 db3.afs.ox.ac.uk.
ox.ac.uk        text = "v=spf1 redirect=_spf.ox.ac.uk"
ox.ac.uk        text = "google-site-verification=qb4BUD5Usjh0Nep0wKIkZIlLSR2rrXsD5PvYGIiKJtA"
ox.ac.uk        text = "MS=ms57844111"
ox.ac.uk        mail exchanger = 9 oxmail.ox.ac.uk.
ox.ac.uk        nameserver = dns2.ox.ac.uk.
ox.ac.uk        nameserver = ns2.ja.net.
ox.ac.uk        nameserver = dns0.ox.ac.uk.
ox.ac.uk        nameserver = dns1.ox.ac.uk.
>
```

There is more than one authoritative server: nighthawk.dns.ox.ac.uk and the others listed with “nameserver.”

3) Tried several of the authoritative servers above:

```
Authoritative answers can be found from:
> mail.yahoo.com ns2.ja.net
Server:         2604:2000:1600:8007:8a1f:a1ff:fe29:6b45
Address:        2604:2000:1600:8007:8a1f:a1ff:fe29:6b45#53

Non-authoritative answer:
mail.yahoo.com  canonical name = fd-geoycpi-uno.gycpi.b.yahoodns.net.

Authoritative answers can be found from:
> ns2.ja.net mail.yahoo.com
Server:         2604:2000:1600:8007:8a1f:a1ff:fe29:6b45
Address:        2604:2000:1600:8007:8a1f:a1ff:fe29:6b45#53

Non-authoritative answer:
Name:   ns2.ja.net
Address: 193.63.105.17

Authoritative answers can be found from:
> dns0.ox.ac.uk mail.yahoo.com
Server:         2604:2000:1600:8007:8a1f:a1ff:fe29:6b45
Address:        2604:2000:1600:8007:8a1f:a1ff:fe29:6b45#53

Non-authoritative answer:
Name:   dns0.ox.ac.uk
Address: 129.67.1.190

Authoritative answers can be found from:
> nighthawk.dns.ox.ac.uk mail.yahoo.com
Server:         2604:2000:1600:8007:8a1f:a1ff:fe29:6b45
Address:        2604:2000:1600:8007:8a1f:a1ff:fe29:6b45#53

Non-authoritative answer:
Name:   nighthawk.dns.ox.ac.uk
Address: 163.1.2.189

Authoritative answers can be found from:
> nighthawk.dns.ox.ac.uk hostmaster.yahoo-inc.com
Server:         2604:2000:1600:8007:8a1f:a1ff:fe29:6b45
Address:        2604:2000:1600:8007:8a1f:a1ff:fe29:6b45#53

Non-authoritative answer:
Name:   nighthawk.dns.ox.ac.uk
Address: 163.1.2.189
```

For nighthawk.dns.ox.uk the Ip is: 163.1.2.189

4) UDP

5)

```
▼ User Datagram Protocol, Src Port: 5353, Dst Port: 5353
    Source Port: 5353
    Destination Port: 5353
```

Source: 5353 , Destination: 5353

6) DNS servers 10.0.1.1

```
Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : si.rr.com
   Description . . . . . . . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
   Physical Address. . . . . . . . . : 08-00-27-7C-EE-10
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::787f:a684:988a:de4c%9(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.0.2.15(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Friday, November 10, 2017 4:04:24 PM
   Lease Expires . . . . . . . . . . : Saturday, November 11, 2017 5:35:39 PM
   Default Gateway . . . . . . . . . : 10.0.2.2
   DHCP Server . . . . . . . . . . . : 10.0.2.2
   DHCPv6 IAID . . . . . . . . . . . : 34078759
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-1D-E1-A8-D4-08-00-27-7C-EE-10
   DNS Servers . . . . . . . . . . . : 10.0.1.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

7) Standard queries such as this (Type A) do not contain any “answers.”

8)

```
5019 269.115510   2604:2000:1600:800… 2604:2000:1600:800… DNS   120 Standard query response 0xadea AAAA www.irtf.org AAAA 2001:1900:3001:11::2c
5020 269.119517   2604:2000:1600:800… 2604:2000:1600:800… DNS   107 Standard query response 0x8b3a A www.iab.org A 4.31.198.44
5021 269.119712   2604:2000:1600:800… 2604:2000:1600:800… DNS   135 Standard query response 0x711d A wiki.tools.ietf.org CNAME durif.tools.ietf.org
```

```
    [Stream index: 52]
▼ Domain Name System (response)
    [Request In: 4951]
    [Time: 0.479843000 seconds]
    Transaction ID: 0xadea
  ▶ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  ▼ Queries
    ▶ www.irtf.org: type AAAA, class IN
  ▼ Answers
    ▶ www.irtf.org: type AAAA, class IN, addr 2001:1900:3001:11::2c
```

One answer is provided:

```
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  ▼ Queries
    ▶ www.irtf.org: type AAAA, class IN
  ▼ Answers
    ▼ www.irtf.org: type AAAA, class IN, addr 2001:1900:3001:11::2c
        Name: www.irtf.org
        Type: AAAA (IPv6 Address) (28)
        Class: IN (0x0001)
        Time to live: 1800
        Data length: 16
        AAAA Address: 2001:1900:3001:11::2c
```

9) The first SYN packet sent was to 2001:1900:3001:11::2c witch is the same as the first ip address provided the DNS response message.

10) No. DNS and query messages are in the same format.

11)

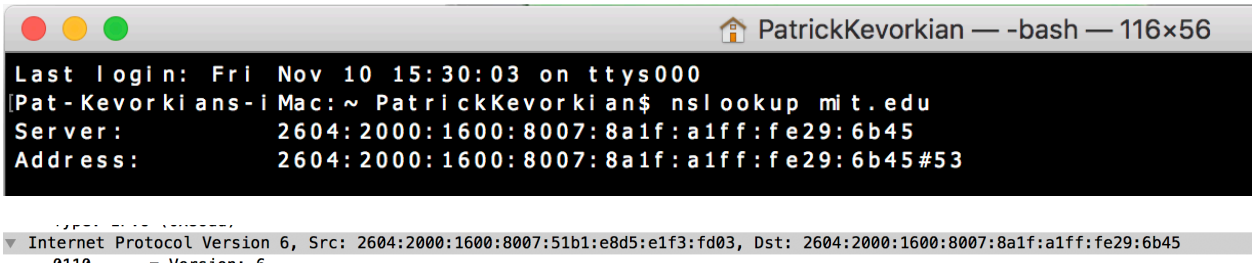
```
User Datagram Protocol, Src Port: 63176, Dst Port: 53
    Source Port: 63176
    Destination Port: 53
    Length: 33
    Checksum: 0x0274 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
```

Destination For Query port is: 53

```
User Datagram Protocol, Src Port: 53, Dst Port: 63176
    Source Port: 53
    Destination Port: 63176
    Length: 49
    Checksum: 0xa751 [unverified]
    [Checksum Status: Unverified]
```

Source port for Dns response is: 53

12)



The address the DNS query is sent to is: 2604:2000:1600:8007:8a1f:a1ff:fe29:6b45, which corresponds to the ifconfig command seen here.

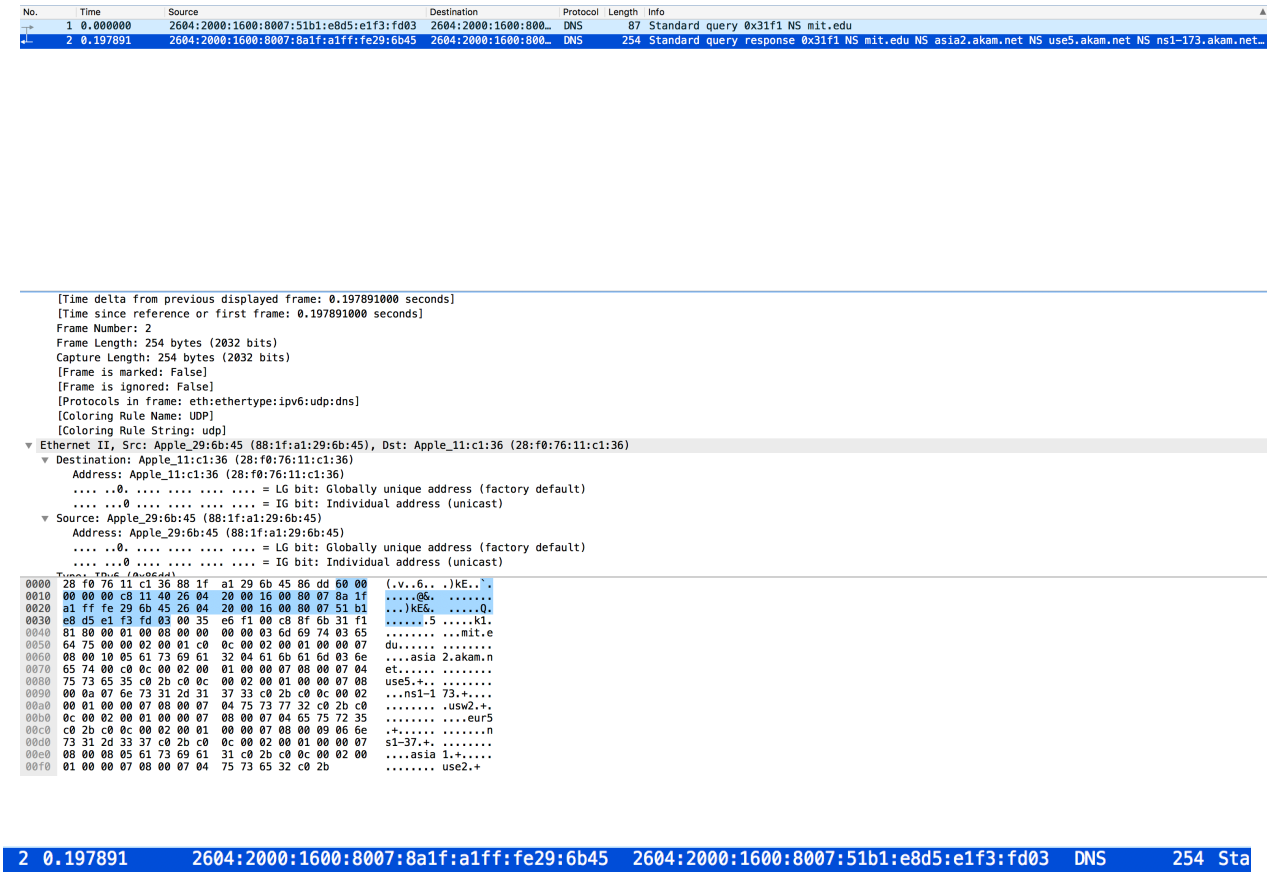
13) Type A, contains no answers:

```
Domain Name System (query)
    [Response In: 2]
    Transaction ID: 0xc758
  ▶ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▼ Queries
    ▼ mit.edu: type A, class IN
          Name: mit.edu
          [Name Length: 7]
          [Label Count: 2]
          Type: A (Host Address) (1)
          Class: IN (0x0001)
```

14/15) It contains one answer with the following information: Name, Type, Class, Tine to live, Data Length, and Address.

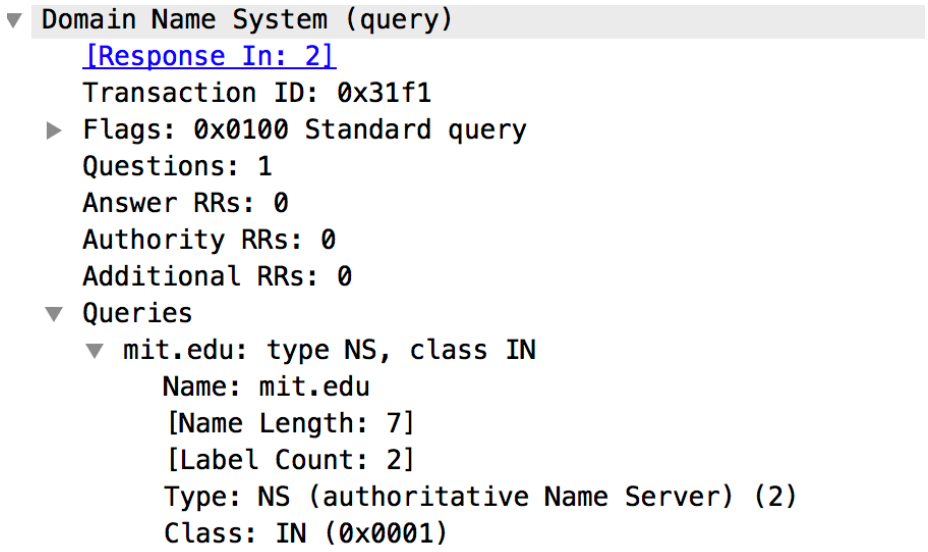
```
▼ Queries
  ▼ mit.edu: type A, class IN
      Name: mit.edu
      [Name Length: 7]
      [Label Count: 2]
      Type: A (Host Address) (1)
      Class: IN (0x0001)
▼ Answers
  ▼ mit.edu: type A, class IN, addr 23.217.168.218
      Name: mit.edu
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 20
      Data length: 4
      Address: 23.217.168.218
```

16)



The query message was sent to 2604:2000:1600:8007:8a1f:a1ff:fe29:6b45, which is my default DNS server.

17)



Its a type NS DNS query that contains no answers.

18/19)

```
▼ mit.edu: type NS, class IN, ns asia2.akam.net
    Name: mit.edu
    Type: NS (authoritative Name Server) (2)
    Class: IN (0x0001)
    Time to live: 1800
    Data length: 16
    Name Server: asia2.akam.net
▼ mit.edu: type NS, class IN, ns use5.akam.net
    Name: mit.edu
    Type: NS (authoritative Name Server) (2)
    Class: IN (0x0001)
    Time to live: 1800
    Data length: 7
    Name Server: use5.akam.net
▼ mit.edu: type NS, class IN, ns ns1-173.akam.net
    Name: mit.edu
    Type: NS (authoritative Name Server) (2)
    Class: IN (0x0001)
    Time to live: 1800
    Data length: 10
    Name Server: ns1-173.akam.net
▼ mit.edu: type NS, class IN, ns usw2.akam.net
    Name: mit.edu
    Type: NS (authoritative Name Server) (2)
    Class: IN (0x0001)
    Time to live: 1800
    Data length: 7
    Name Server: usw2.akam.net
    Name Server: usw2.akam.net
▼ mit.edu: type NS, class IN, ns eur5.akam.net
    Name: mit.edu
    Type: NS (authoritative Name Server) (2)
    Class: IN (0x0001)
    Time to live: 1800
    Data length: 7
    Name Server: eur5.akam.net
▼ mit.edu: type NS, class IN, ns ns1-37.akam.net
    Name: mit.edu
    Type: NS (authoritative Name Server) (2)
    Class: IN (0x0001)
    Time to live: 1800
    Data length: 9
    Name Server: ns1-37.akam.net
▼ mit.edu: type NS, class IN, ns asia1.akam.net
    Name: mit.edu
    Type: NS (authoritative Name Server) (2)
    Class: IN (0x0001)
    Time to live: 1800
    Data length: 8
    Name Server: asia1.akam.net
▼ mit.edu: type NS, class IN, ns use2.akam.net
    Name: mit.edu
    Type: NS (authoritative Name Server) (2)
    Class: IN (0x0001)
    Time to live: 1800
    Data length: 7
    Name Server: use2.akam.net
```

The names are: asia2.akam.net, use5.akam.net, ns1-173.akam.net, usw2.akam.net, eur5.akam.net, ns1-37.akam.net, asia1.akam.net, use2.akam.net

Does not provide their ip addresses.

20)

```
  4 0.462681      10.0.1.7                                18.72.0.3
```

Response sent to 18.72.0.3 which is bitty.mit.edu.

21) Standard Type A, no answers.

```
▼ Domain Name System (query)
    Transaction ID: 0x2f23
  ▼ Flags: 0x0100 Standard query
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Standard query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... .0.. .... = Z: reserved (0)
      .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▼ Queries
    ▼ 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)
```

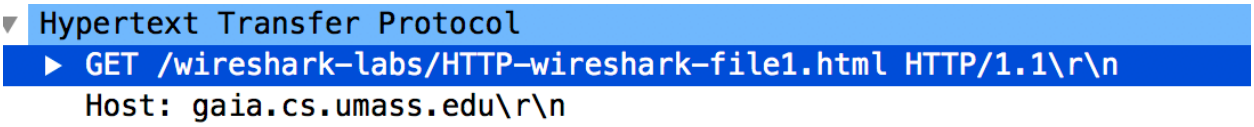
22/23) One answer provided in DNS response:

```
▼ Domain Name System (query)
    Transaction ID: 0x2f23
  ▼ Flags: 0x0100 Standard query
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Standard query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... .0.. .... = Z: reserved (0)
      .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▼ Queries
    ▼ 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)
```

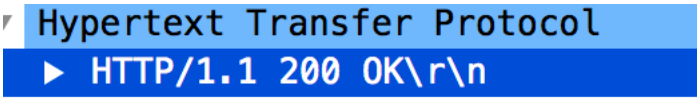
Lab 2: HTTP

1)

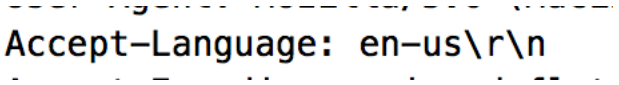
Client running HTTP 1.1



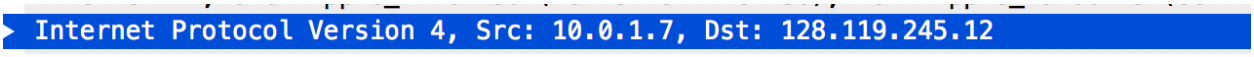
Server Running: HTTP 1.1



2) Browser indicates En-us

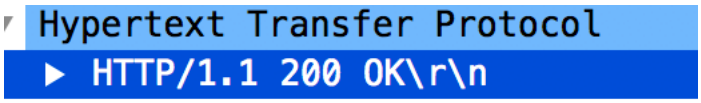


3)

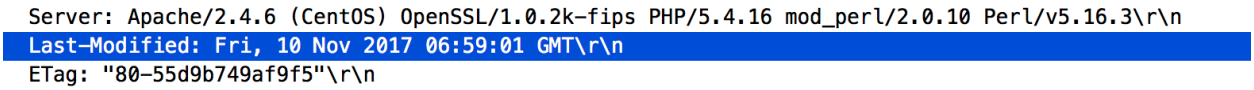


My ip: 10.0.1.7 gaia.cs.umass server: 128.119.245.12

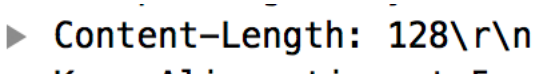
4) Status code: 200



5) Last modified: Friday, 10th November, 2017



6) 128 bytes of content

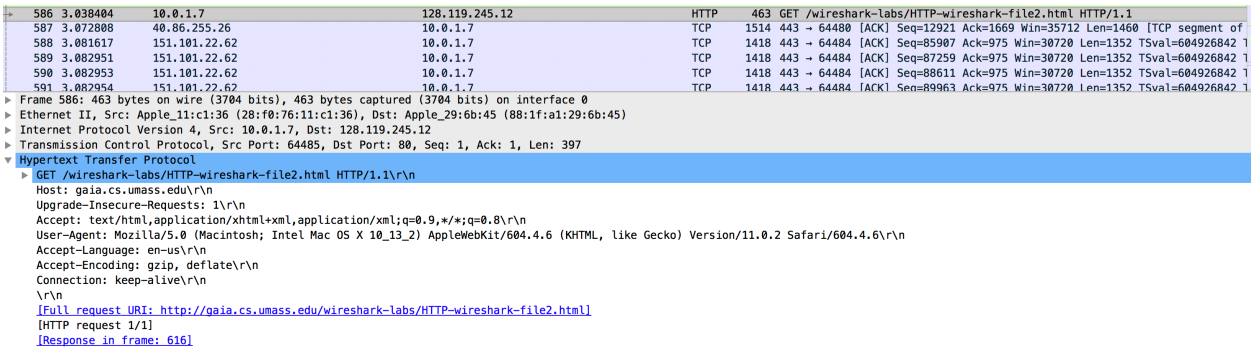


7) No

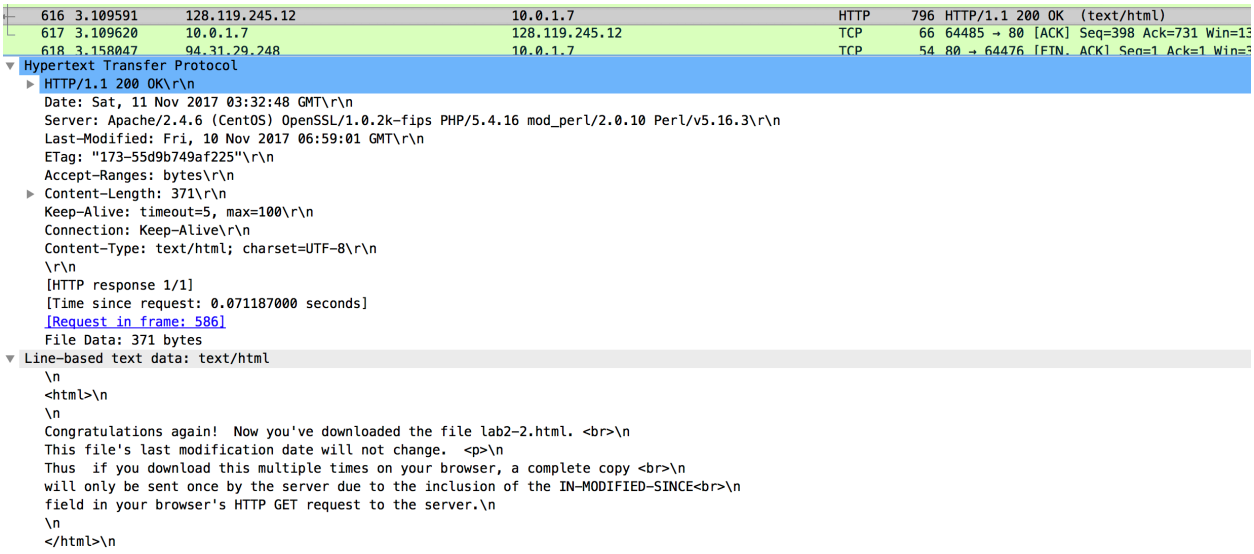
```
▸ Frame 8: 463 bytes on wire (3704 bits), 463 bytes captured (3704 bits) on interface 0
▸ Ethernet II, Src: Apple_11:c1:36 (28:f0:76:11:c1:36), Dst: Apple_29:6b:45 (88:1f:a1:29:6b:45)
▾ Internet Protocol Version 4, Src: 10.0.1.7, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 449
    Identification: 0x0000 (0)
  ▸ Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (6)
    Header checksum: 0xb8ac [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.0.1.7
    Destination: 128.119.245.12
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
▾ Transmission Control Protocol, Src Port: 62738, Dst Port: 80, Seq: 1, Ack: 1, Len: 397
    Source Port: 62738
    Destination Port: 80
    [Stream index: 0]
    [TCP Segment Len: 397]
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 398    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    1000 .... = Header Length: 32 bytes (8)
  ▸ Flags: 0x018 (PSH, ACK)
    Window size value: 4117
    [Calculated window size: 131744]
    [Window size scaling factor: 32]
    Checksum: 0x8d57 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  ▸ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  ▸ [SEQ/ACK analysis]
    TCP payload (397 bytes)
▾ Hypertext Transfer Protocol
  ▸ GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Upgrade-Insecure-Requests: 1\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_13_2) AppleWebKit/604.4.6 (KHTML, like Gecko) Version/11.0.2 Safari/604.4.6\r\n
    Accept-Language: en-us\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
    [HTTP request 1/1]
    [Response in frame: 10]
```

```
▸ Frame 10: 552 bytes on wire (4416 bits), 552 bytes captured (4416 bits) on interface 0
▸ Ethernet II, Src: Apple_29:6b:45 (88:1f:a1:29:6b:45), Dst: Apple_11:c1:36 (28:f0:76:11:c1:36)
▸ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.1.7
▸ Transmission Control Protocol, Src Port: 80, Dst Port: 62738, Seq: 1, Ack: 398, Len: 486
▾ Hypertext Transfer Protocol
  ▸ HTTP/1.1 200 OK\r\n
    Date: Sat, 11 Nov 2017 02:49:12 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
    Last-Modified: Fri, 10 Nov 2017 06:59:01 GMT\r\n
    ETag: "80-55d9b749af9f5"\r\n
    Accept-Ranges: bytes\r\n
  ▸ Content-Length: 128\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: 0.267271000 seconds]
    [Request in frame: 8]
    File Data: 128 bytes
▸ Line-based text data: text/html
```

8) The first Get does not contain “IF-MODIFIED-SINCE”



9) Yes the server returned the contents of the file:



10) The second Get has “IF-MODIFIED-SINCE” followed by the date and time.

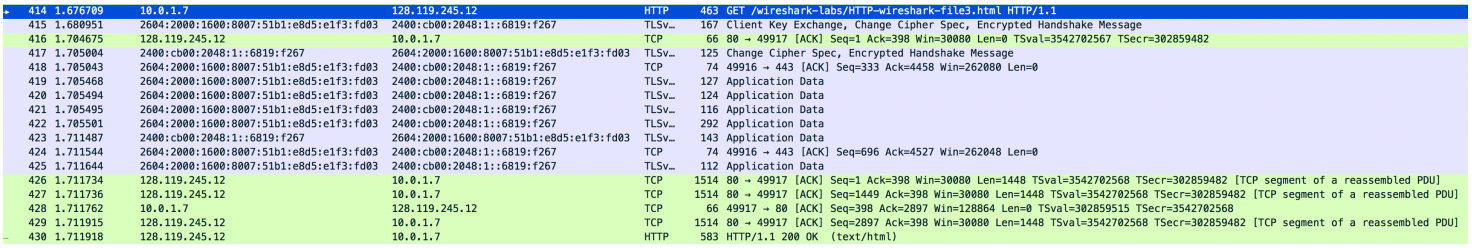
11) The second Get returns the status code 304 Not modified, and the text is not retuned.

12) Browser sent 1 HTTP GET request. Packet 414 contains the Get request:

13) Packet 430

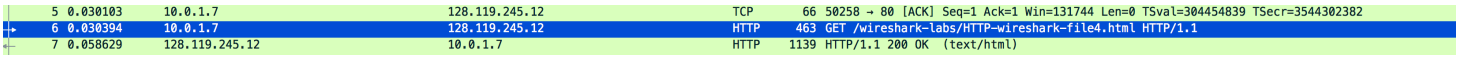
14) Status code and phrase: 200, OK

15) Three packets: 426,427, 429

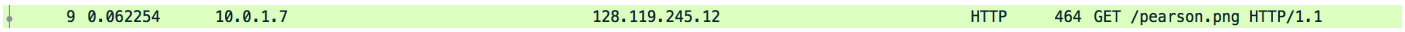


16) There were 3 GETS:

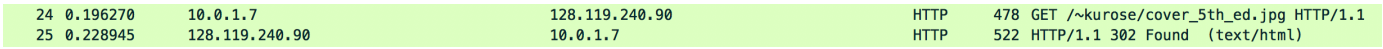
First for base file-



Second for Pearson Logo-

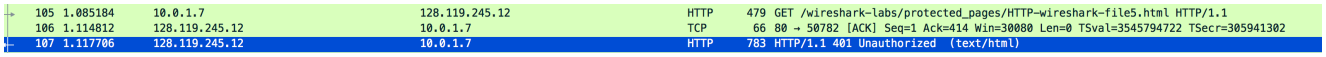


Third for 5th addition cover-



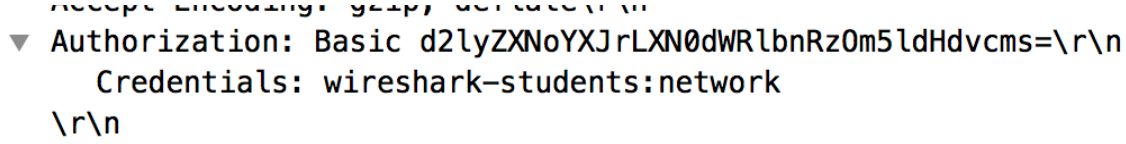
17) They happened in parallel. The 200 Ok response for both images happens before the first file was received. That and the TCP out of order delivery concluded this is the case.

18) The HTTP GET in packet 105 has a response of “401 Unauthorized” in packet 107.



→	105	1.085184	10.0.1.7	128.119.245.12	HTTP	479 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
	106	1.114812	128.119.245.12	10.0.1.7	TCP	66 80 → 50782 [ACK] Seq=1 Ack=414 Win=30080 Len=0 TSval=3545794722 TSecr=305941302
←	107	1.117706	128.119.245.12	10.0.1.7	HTTP	783 HTTP/1.1 401 Unauthorized (text/html)

19) The second Get ha the new field “Authorization: Basic.”



```
Accept-Encoding: gzip, deflate\r\n
▼ Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
    Credentials: wireshark-students:network
  \r\n
```