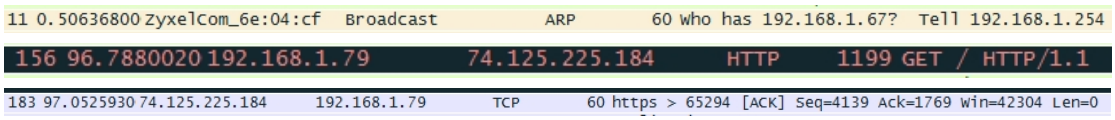
Answer 4:

A. Packet sniffer:

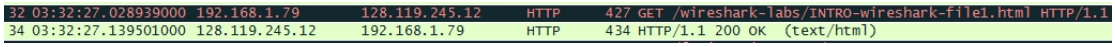
1.

Screenshot:



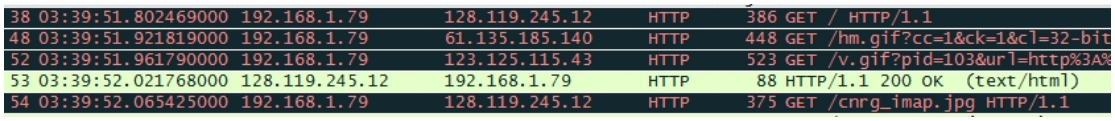
TCP HTTP ARP

2.



It takes 27.139501-27.028939=110.562msec.

3.



The address of the gaia.cs.umass.edu is 128.119.245.12.

And my computer's address is 192.168.1.79.

4.

No. Time Source Destination

Protocol Length Info

22 03:43:23.456825000 192.168.1.79 128.119.245.12

HTTP 513 GET /wireshark-labs/INTRO-wireshark-file1.html

HTTP/1.1

Frame 22: 513 bytes on wire (4104 bits), 513 bytes captured (4104 bits) on interface 0

Ethernet II, Src: Hewlett-_e7:83:ea (2c:27:d7:e7:83:ea), Dst: ZyxelCom_6e:04:cf (c8:6c:87:6e:04:cf)

Internet Protocol Version 4, Src: 192.168.1.79 (192.168.1.79), Dst: 128.119.245.12 (128.119.245.12)

Transmission Control Protocol, Src Port: 65323 (65323), Dst Port: http (80), Seq: 1, Ack: 1, Len: 459

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,*/*;q=0.8\r\n

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/27.0.1453.110 Safari/537.36\r\n

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

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

If-None-Match: "8734b-51-ad85ca40"\r\n

If-Modified-Since: Sun, 20 Oct 2013 10:32:01 GMT\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: 24]

[Next request in frame: 27]

No. Time Source Destination Protocol Length Info

24 03:43:23.569634000 128.119.245.12 192.168.1.79 HTTP 434 HTTP/1.1 200 OK (text/html)

Frame 24: 434 bytes on wire (3472 bits), 434 bytes captured (3472 bits) on interface 0

Ethernet II, Src: ZyxelCom_6e:04:cf (c8:6c:87:6e:04:cf), Dst: Hewlett-_e7:83:ea (2c:27:d7:e7:83:ea)

Internet Protocol Version 4, Src: 128.119.245.12 (128.119.245.12), Dst: 192.168.1.79 (192.168.1.79)

Transmission Control Protocol, Src Port: http (80), Dst Port: 65323 (65323), Seq: 1, Ack: 460, Len: 380

Hypertext Transfer Protocol

HTTP/1.1 200 OK\r\n

Date: Sun, 20 Oct 2013 10:43:23 GMT\r\n

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

Last-Modified: Sun, 20 Oct 2013 10:43:01 GMT\r\n

ETag: "8734b-51-d4dc9740"\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: 0.112809000 seconds]

[Request in frame: 22]

[Next request in frame: 27]

[Next response in frame: 28]

Line-based text data: text/html

B. HTTP:

Part 1.

GET and response messages:

No. Time Source Destination

Protocol Length Info

103 03:54:12.564883000 192.168.1.79 128.119.245.12 HTTP 426 GET /wireshark-labs/HTTP-wireshark-file1.html **HTTP/1.1 (Indicates the browser supports HTTP version 1.1)**

Frame 103: 426 bytes on wire (3408 bits), 426 bytes captured (3408 bits) on interface 0

Ethernet II, Src: Hewlett-_e7:83:ea (2c:27:d7:e7:83:ea), Dst: ZyxelCom_6e:04:cf (c8:6c:87:6e:04:cf)

Internet Protocol Version 4, Src: **192.168.1.79 (It's the address of my computer)** (192.168.1.79), Dst: **128.119.245.12 (It's the address of the server)** (128.119.245.12)

Transmission Control Protocol, Src Port: 65336 (65336), Dst Port: http (80), Seq: 1, Ack: 1, Len: 372

Hypertext Transfer Protocol

GET /wireshark-labs/HTTP-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,*/*;q=0.8\r\n

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/27.0.1453.110 Safari/537.36\r\n

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

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

\r\n (**Browser supports two languages: en-US and en.)**

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

[HTTP request 1/2]

[Response in frame: 109]

[Next request in frame: 118]

No. Time Source Destination Protocol Length Info

109 03:54:12.675089000 128.119.245.12 192.168.1.79 HTTP 482 **HTTP/1.1 (Indicates the server is running HTTP version 1.1**

) 200 OK (the status code returned) (text/html)

Frame 109: 482 bytes on wire (3856 bits), 482 bytes captured (3856 bits) on interface 0

Ethernet II, Src: ZyxelCom_6e:04:cf (c8:6c:87:6e:04:cf), Dst: Hewlett-_e7:83:ea (2c:27:d7:e7:83:ea)

Internet Protocol Version 4, Src: 128.119.245.12 (128.119.245.12), Dst: 192.168.1.79 (192.168.1.79)

Transmission Control Protocol, Src Port: http (80), Dst Port: 65336 (65336), Seq: 1, Ack: 373, Len: 428

Hypertext Transfer Protocol

HTTP/1.1 200 OK\r\n

Date: Sun, 20 Oct 2013 10:54:12 GMT\r\n

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

Last-Modified: Sun, 20 Oct 2013 10:54:01 GMT\r\n

(The HTML file was last modified at 20 Oct 2013 10:54:01 GMT)

ETag: "8734d-80-fc336440"\r\n

Accept-Ranges: bytes\r\n

Content-Length: 128\r\n

(The content length is 128 bytes)

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: 0.110206000 seconds]

[Request in frame: 103]

[Next request in frame: 118]

[Next response in frame: 119]

Line-based text data: text/html

There are some headers not displayed in the packet-listing window like Content-Type and Keep-Alive.

Part 2.

8. No.

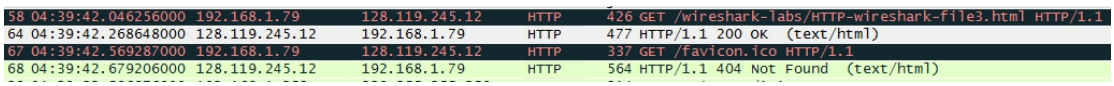
9. Yes. The status code return is “200 OK” not “304 Not Modified”, so the server has to send the whole HTML file to the client. On the other hand, the cache of browser is entirely deleted, so the browser has to get the html object from server.

10. Yes. The content of “IF-MODIFIED-SINCE:” header is “If-Modified-Since: Sun, 20 Oct 2013 11:22:01 GMT”.

11. The second status code returned is “304 Not Modified” and server didn’t return the content explicitly. That’s because the browser knows the cache is up-to-date from this status code and doesn’t need to ask the server to resend the html object.

Part 3.

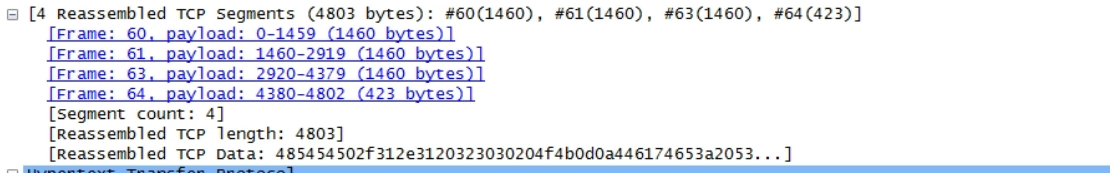
12. Two. Packet No.58 contains the GET message for the Bill of Rights.



13. Packet No.64.

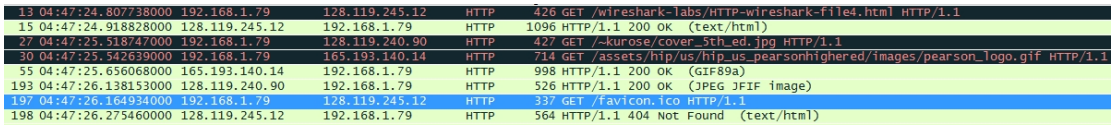
14. 200 OK.

15. Four.



Part 4.

16. Four. The address is 128.119.245.12, 128.119.240.90 and 165.193.140.14 respectively.



17. In parallel. Because the browser sends the second request before receiving the first response.

Part 5.

18. 401 Authorization Required

19.A new header called “Authorization” is included.

C. DNS

Part 3.

Packet content:

No. Time Source Destination Protocol Length Info

1 05:03:01.194590000 192.168.1.79 192.168.1.254 DNS 72 Standard query 0x8155 A www.ietf.org

Frame 1: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface 0

Ethernet II, Src: Hewlett-_e7:83:ea (2c:27:d7:e7:83:ea), Dst: ZyxelCom_6e:04:cf (c8:6c:87:6e:04:cf)

Internet Protocol Version 4, Src: 192.168.1.79 (192.168.1.79), Dst: 192.168.1.254 (192.168.1.254)

User Datagram Protocol, Src Port: 59065 (59065), Dst Port: domain (53)

Domain Name System (query)

No. Time Source Destination Protocol Length Info

2 05:03:01.246772000 192.168.1.254 192.168.1.79 DNS 88 Standard query response 0x8155 A 12.22.58.30

Frame 2: 88 bytes on wire (704 bits), 88 bytes captured (704 bits) on interface 0

Ethernet II, Src: ZyxelCom_6e:04:cf (c8:6c:87:6e:04:cf), Dst: Hewlett-_e7:83:ea (2c:27:d7:e7:83:ea)

Internet Protocol Version 4, Src: 192.168.1.254 (192.168.1.254), Dst: 192.168.1.79 (192.168.1.79)

User Datagram Protocol, Src Port: domain (53), Dst Port: 59065 (59065)

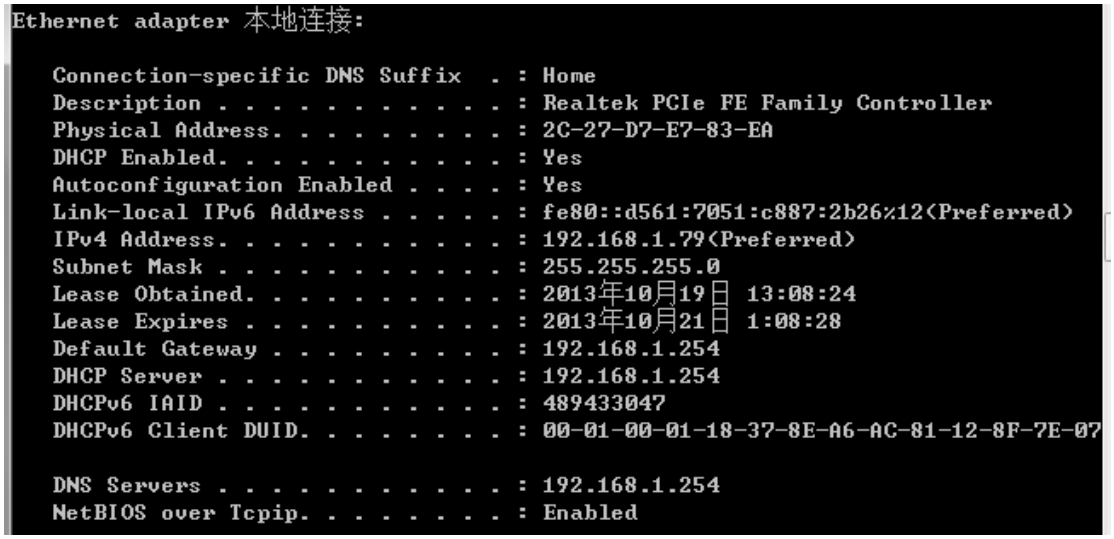
Domain Name System (response)

4. UDP.

```
⊞ Internet Protocol Version 4, Src: 192.168.1.79 (192.168.1.79), Dst: 192.168.1.254 (192.168.1.254)
⊟ User Datagram Protocol, Src Port: 59065 (59065), Dst Port: domain (53)
    Source port: 59065 (59065)
    Destination port: domain (53)
    Length: 38
  ⊞ Checksum: 0x84d5 [validation disabled]
⊟ Domain Name System (query)
    [Response In: 2]
    Transaction ID: 0x8155
```

5. The destination port is 53 and the source port is also 53.

6. 192.168.1.254. They are the same.



7. It's a type A Standard Query and it doesn't contain any answers.

8. There were 1 answers provided. The content is listed:

www.ietf.org: type A, class IN, addr 12.22.58.30

Name: www.ietf.org

Type: A (Host address)

Class: IN (0x0001)

Time to live: 30 minutes

Data length: 4

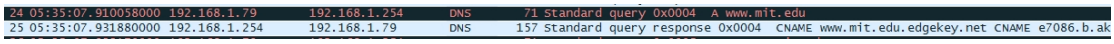
Addr: 12.22.58.30 (12.22.58.30)

9. The destination IP of SYN packet was just the IP address provided in the first DNS response message.

10. No.

11. The destination port for the DNS query message is 53. And the source port of DNS response message is also 53.

12. The DNS query message is sent to 192.168.1.254 which is the same IP address as my local DNS server.



13. It's a type A Standard Query and it doesn't contain any answers.

14. It provided 3 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)

Class: IN (0x0001)

Time to live: 26 minutes, 21 seconds

Data length: 25

Primaryname: www.mit.edu.edgekey.net

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

Name: www.mit.edu.edgekey.net

Type: CNAME (Canonical name for an alias)

Class: IN (0x0001)

Time to live: 4 minutes, 22 seconds

Data length: 21

Primaryname: e7086.b.akamaiedge.net

e7086.b.akamaiedge.net: type A, class IN, addr 23.6.166.151

Name: e7086.b.akamaiedge.net

Type: A (Host address)

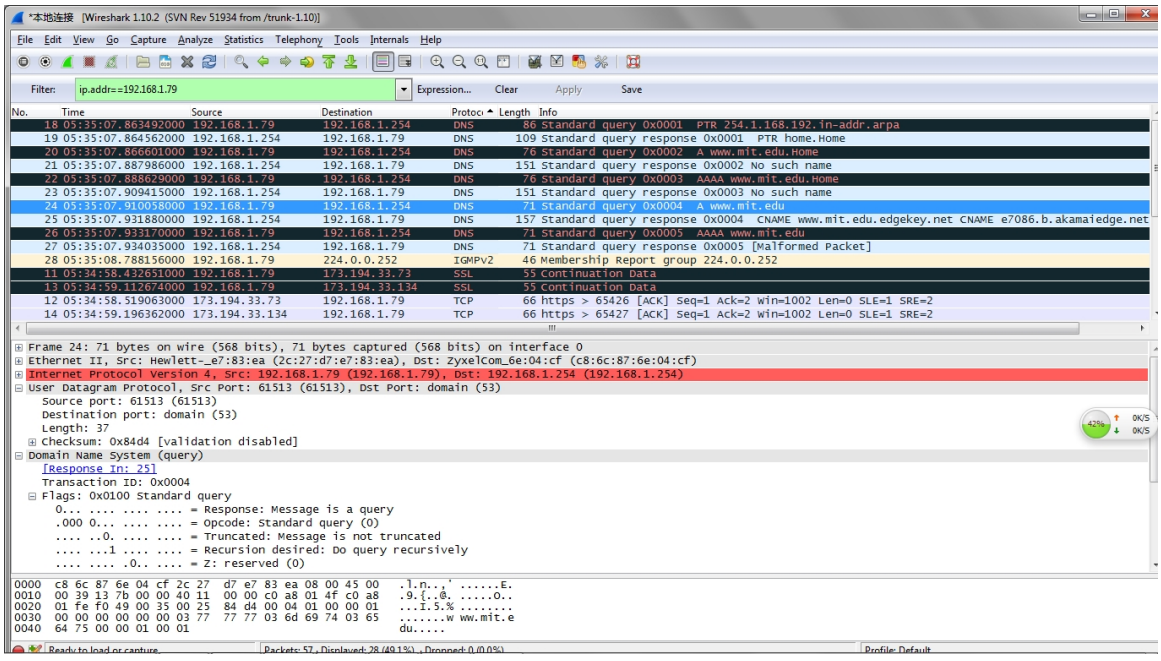
Class: IN (0x0001)

Time to live: 15 seconds

Data length: 4

Addr: 23.6.166.151 (23.6.166.151)

15.



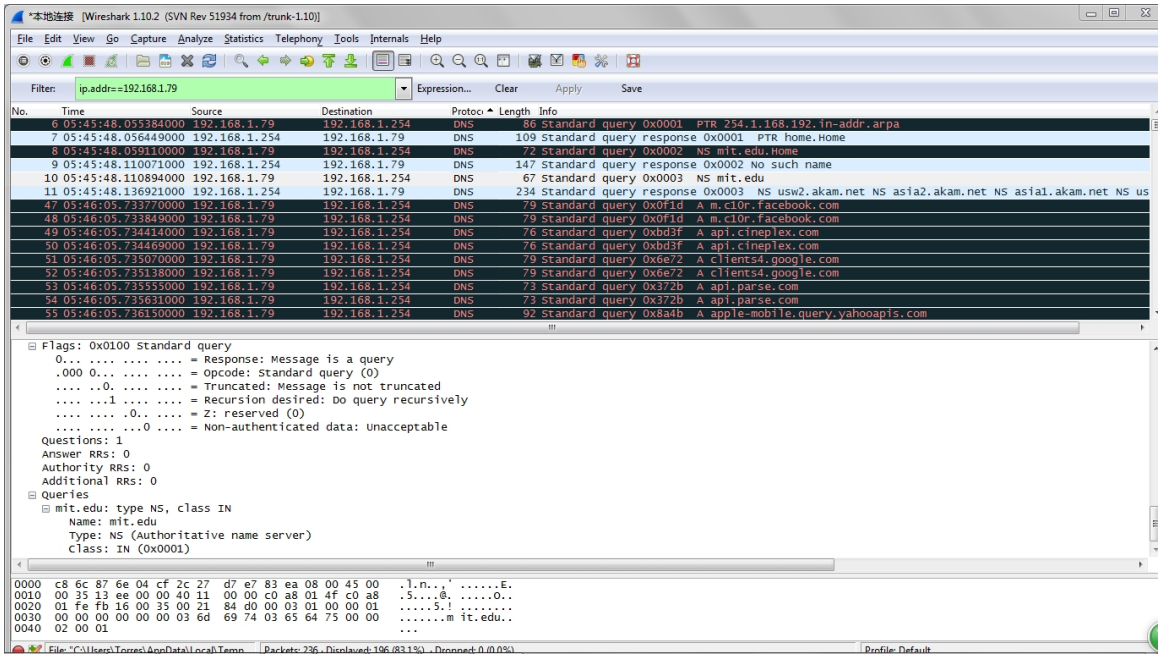
16. The DNS query message is sent to 192.168.1.254 which is my local DNS server.

17. It's a type NS Standard query and doesn't contain any answers.

18. Name servers of MIT are usw2.akam.net, asia2.akam.net,

asia1.akam.net, use5.akam.net, eur5.akam.net, ns1-173.akam.net, use2.akam.net, ns1-37.akam.net. It didn't provide the IP addresses of the name servers.

19.



20-23. It returns timeout notification.