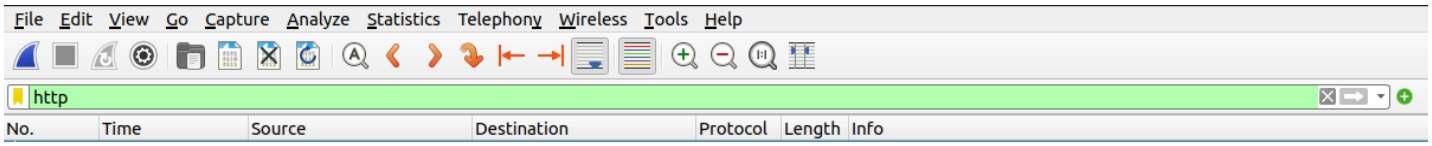
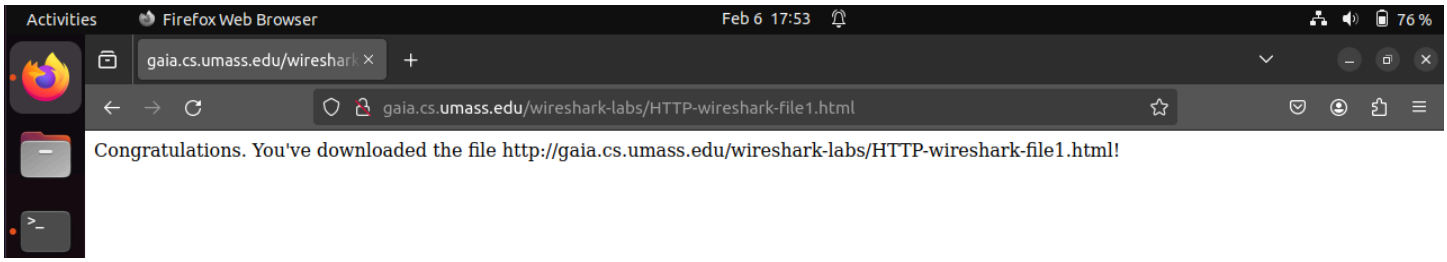
Lab 02 - CS 6330
Lauren Escobedo

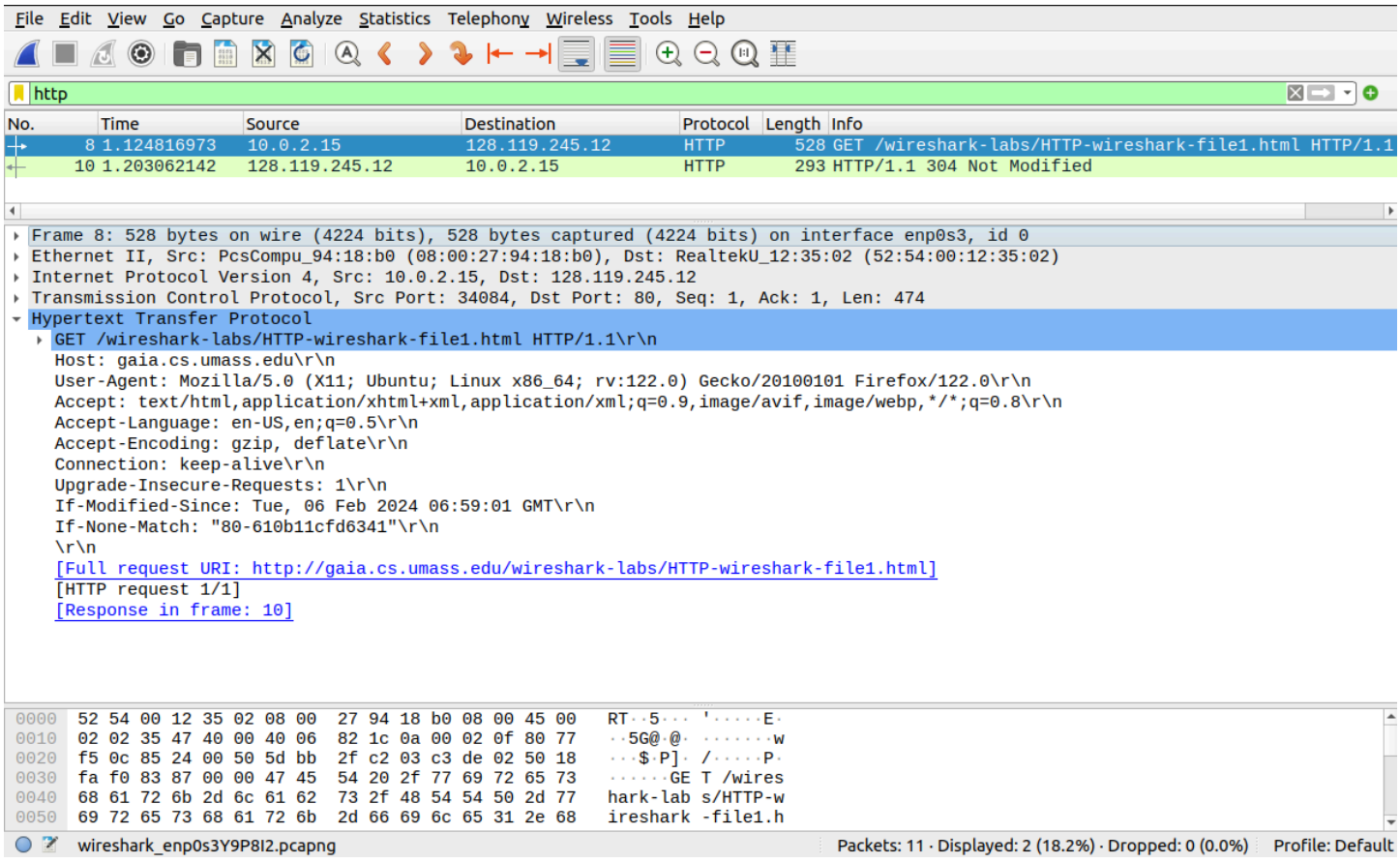
PART I HTTP

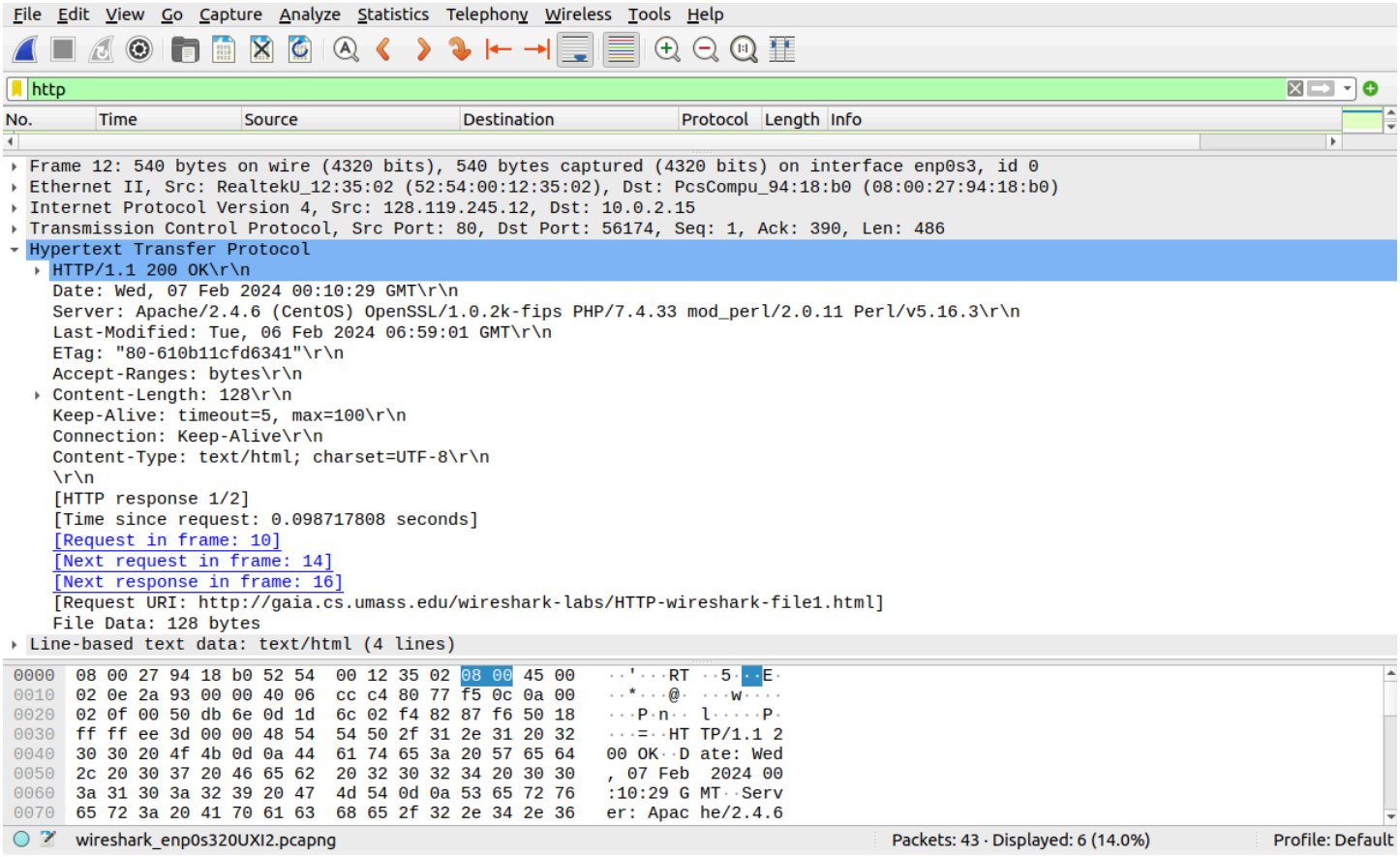
1. I started Wireshark, and opened up my browser. After setting the Wireshark capture filter to only display HTTP protocol packets and waiting about a minute, I searched the URL found in the lab document.





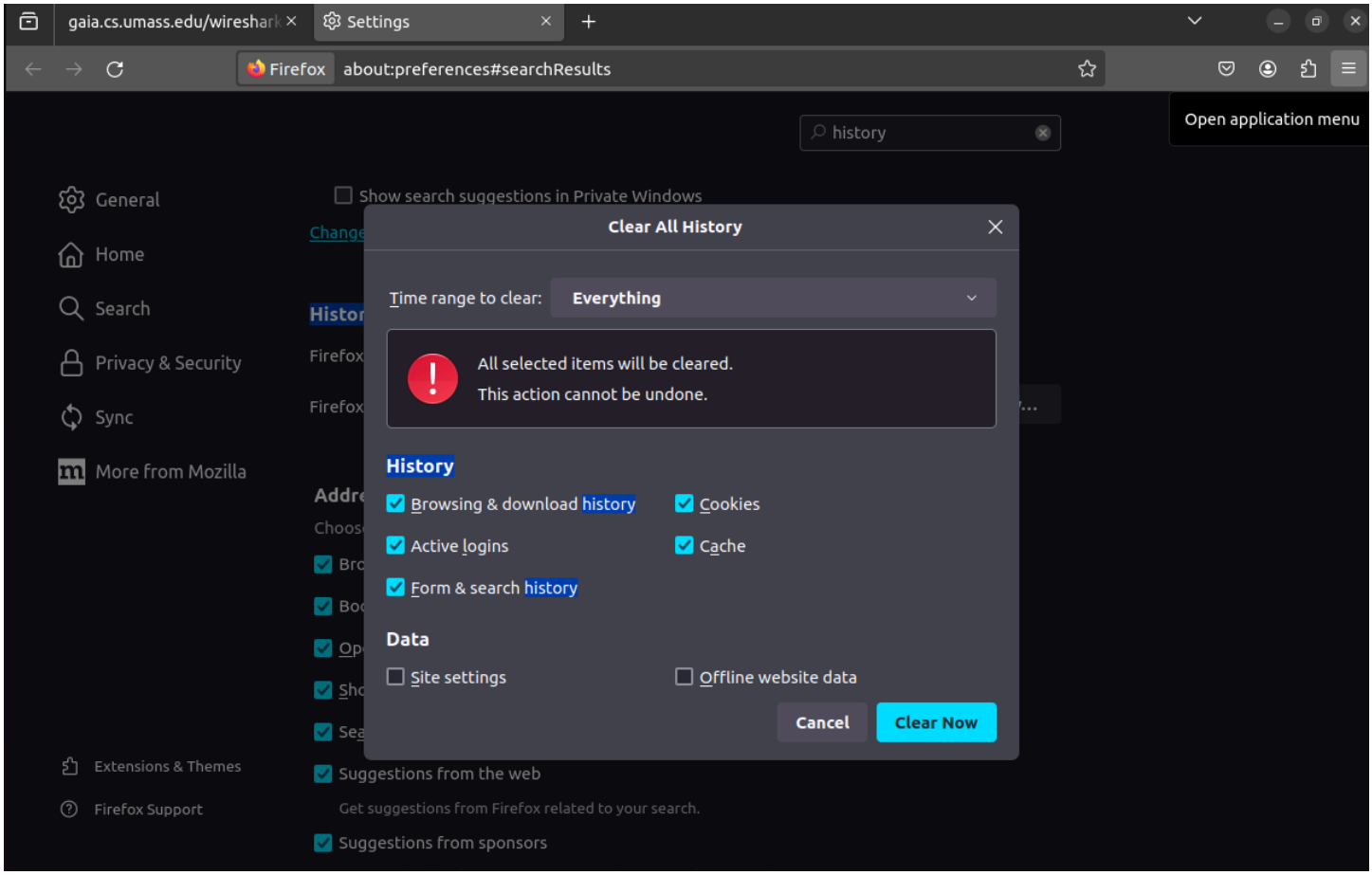
This is the information associated with the packets sent from my machine and received by my machine respectively. I will now answer the questions listed in the lab below.

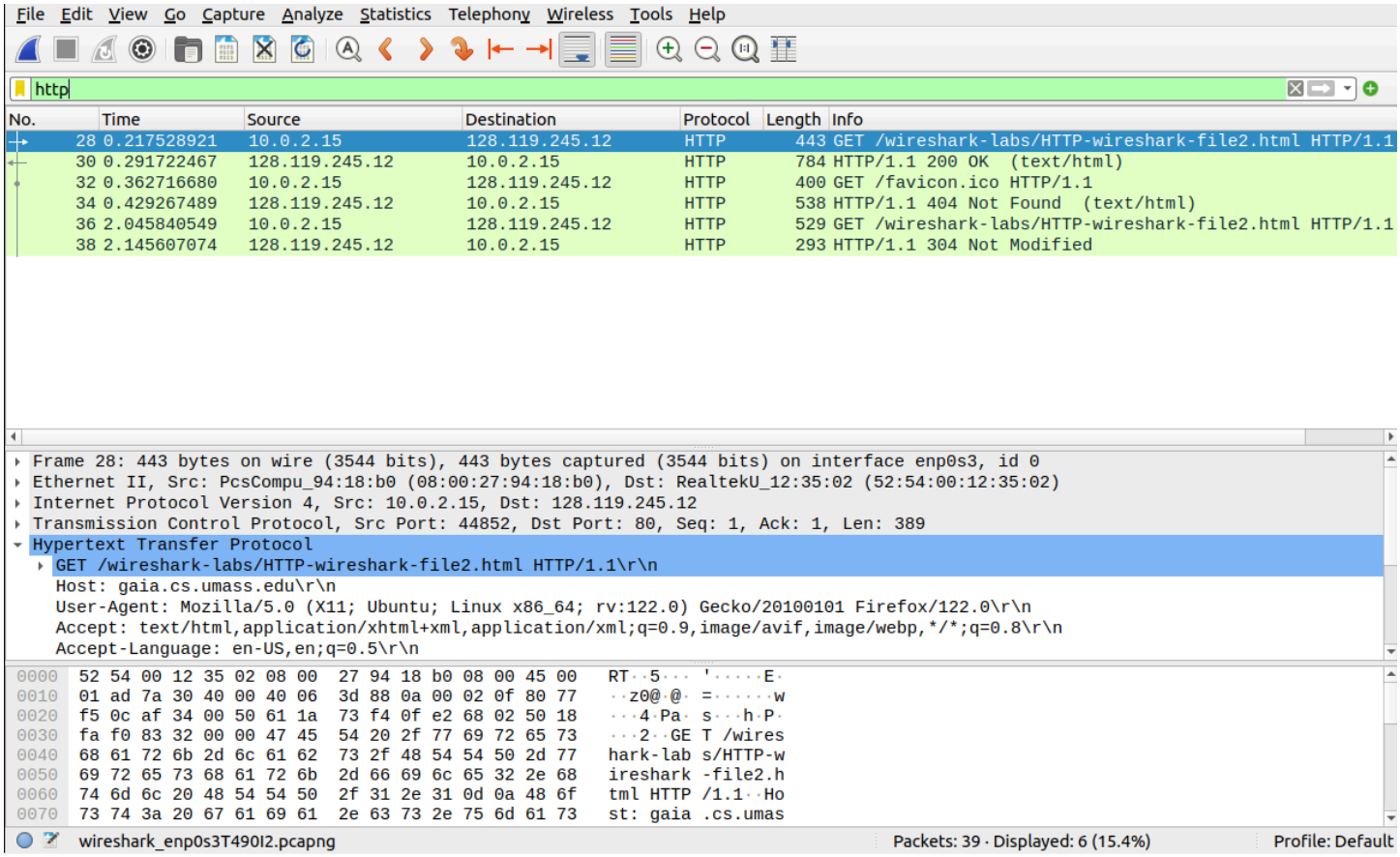




a. My browser is running HTTP 1.1, and the server is running HTTP 1.1.
b. My browser specifies that it accepts “en-US, en”, presumably US English or English.
c. My IP address is 10.0.2.12, and the IP address of the server is 128.119.245.12.
d. The status code I received was 200, OK.
e. The Last Modified date of the message received from the server was 02/06/2024 (today).
f. The Content Length of the message received from the server is 128 bytes.
g. Date

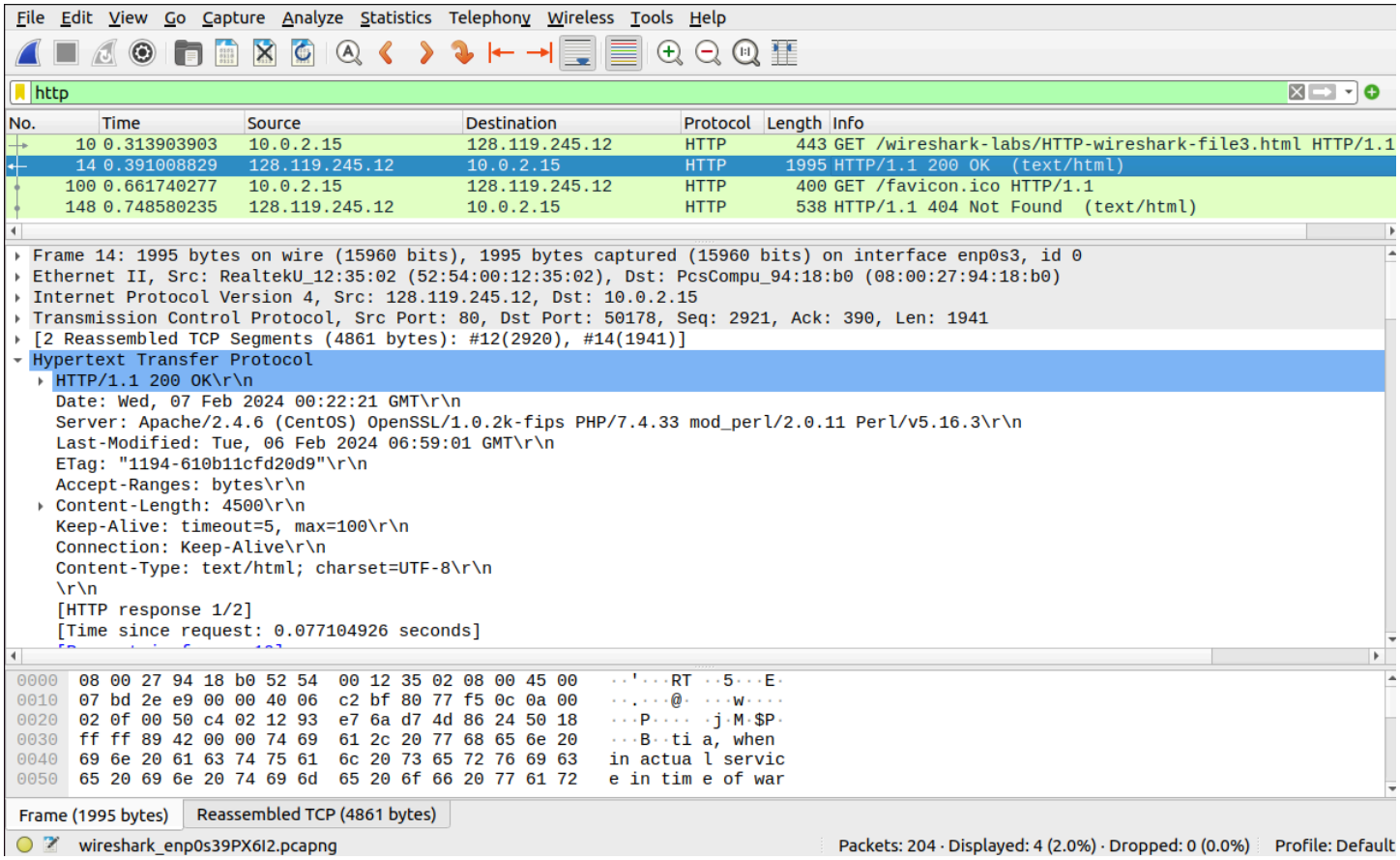
2. I now clear my history before loading the next webpage. I receive 4 packets in Wireshark. One for the request, one for the .ico, one for the response, and one for an object that was not found. I quickly refresh the page to capture the Not Modified packet as well. I will now answer the questions listed in the lab below.


gaia.cs.umass.edu/wireshark
Settings
Firefox
about:preferences#searchResults
Open application menu
history
General
Home
Search
Privacy & Security
Sync
More from Mozilla
Extensions & Themes
Firefox Support
Show search suggestions in Private Windows
Clear All History
Time range to clear:
Everything
All selected items will be cleared.
This action cannot be undone.
History
Browsing & download history
Cookies
Active logins
Cache
Form & search history
Data
Site settings
Offline website data
Cancel
Clear Now
Suggestions from the web
Get suggestions from Firefox related to your search.
Suggestions from sponsors


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
28 0.217528921 10.0.2.15 128.119.245.12 HTTP 443 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
30 0.291722467 128.119.245.12 10.0.2.15 HTTP 784 HTTP/1.1 200 OK (text/html)
32 0.362716680 10.0.2.15 128.119.245.12 HTTP 400 GET /favicon.ico HTTP/1.1
34 0.429267489 128.119.245.12 10.0.2.15 HTTP 538 HTTP/1.1 404 Not Found (text/html)
36 2.045840549 10.0.2.15 128.119.245.12 HTTP 529 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
38 2.145607074 128.119.245.12 10.0.2.15 HTTP 293 HTTP/1.1 304 Not Modified
Frame 28: 443 bytes on wire (3544 bits), 443 bytes captured (3544 bits) on interface enp0s3, id 0
Ethernet II, Src: PcsCompu_94:18:b0 (08:00:27:94:18:b0), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 44852, Dst Port: 80, Seq: 1, Ack: 1, Len: 389
Hypertext Transfer Protocol
GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
Host: gaia.cs.umass.edu\r\n
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:122.0) Gecko/20100101 Firefox/122.0\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n
Accept-Language: en-US,en;q=0.5\r\n
0000 52 54 00 12 35 02 08 00 27 94 18 b0 08 00 45 00
0010 01 ad 7a 30 40 00 40 06 3d 88 0a 00 02 0f 80 77
0020 f5 0c af 34 00 50 61 1a 73 f4 0f e2 68 02 50 18
0030 fa f0 83 32 00 00 47 45 54 20 2f 77 69 72 65 73
0040 68 61 72 6b 2d 6c 61 62 73 2f 48 54 54 50 2d 77
0050 69 72 65 73 68 61 72 6b 2d 66 69 6c 65 32 2e 68
0060 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f
0070 73 74 3a 20 67 61 69 61 2e 63 73 2e 75 6d 61 73
wireshark_enp0s3T490I2.pcapng
Packets: 39 · Displayed: 6 (15.4%)
Profile: Default

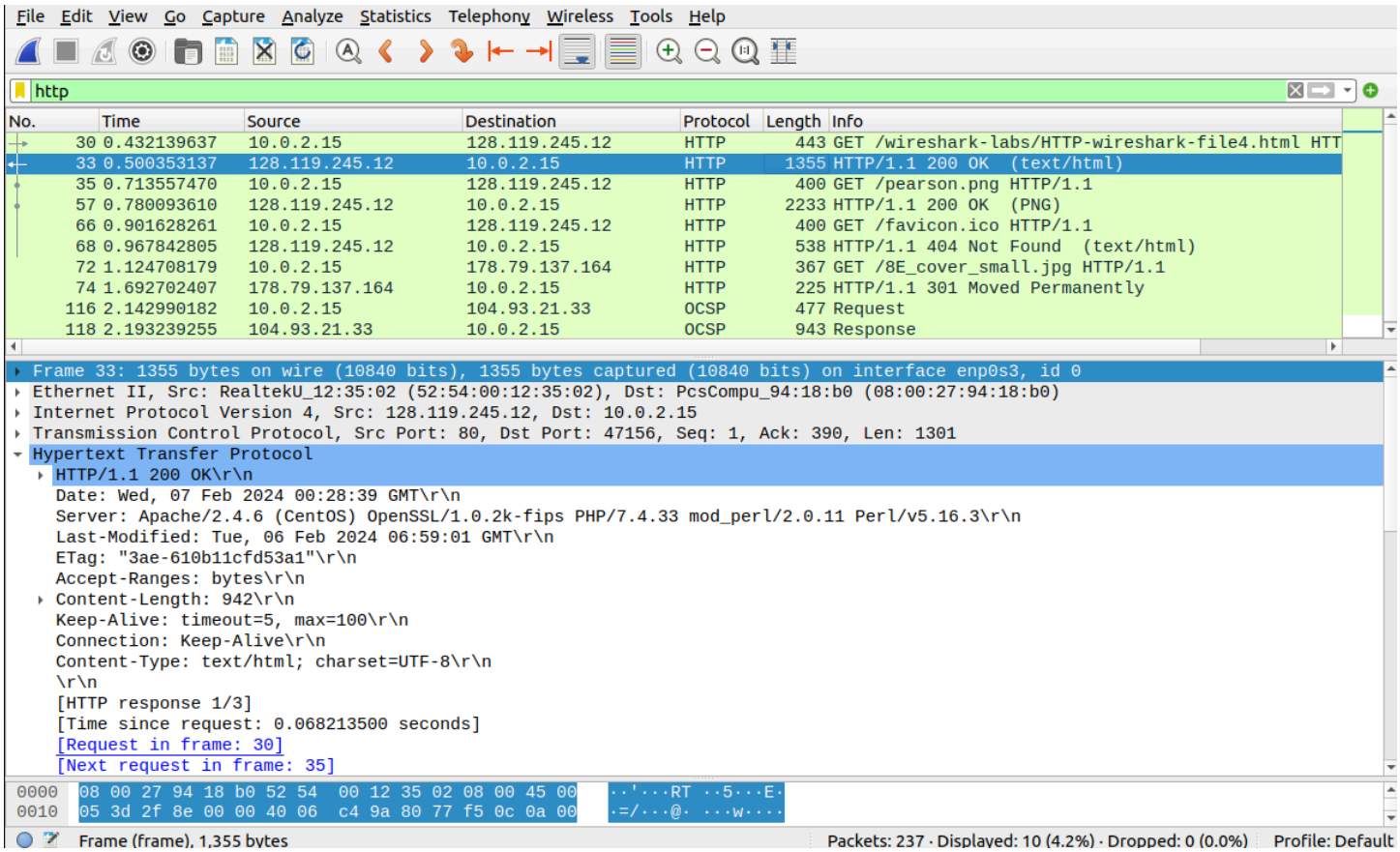
a. No, there is not a “If-Modified-Since” in the very first request packet.
b. Yes, it is under “Line-based text data”.
c. Yes, there is an “If-Modified-Since” and it is followed by the day and time at which I had previously searched it.
d. 304 Not Modified, no the file contents were not passed it simply points to the packet in which they were previously passed.

3. I have now done the same steps as above, clearing the history and cache of my browser, and loaded the new link. Here are the captured packets. I will now answer the questions listed in the lab below.



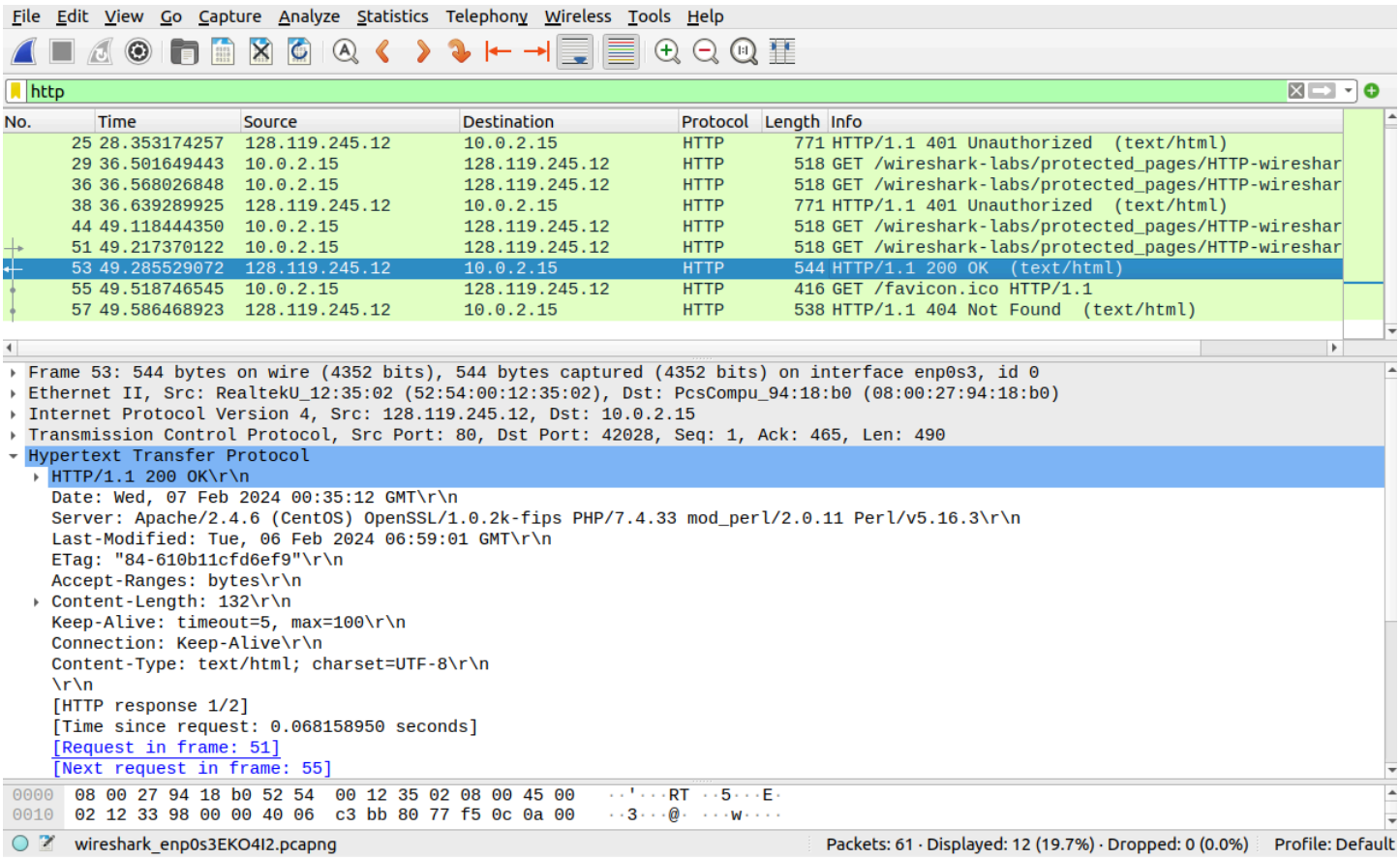
a. My browser sent one packet, the first in the trace list above.
b. The second packet in the trace above contains the response code and phrase of the request.
c. 200 OK
d. 2 segments

4. I have now done the same steps as above, clearing the history and cache of my browser, and loaded the new link. Here are the captured packets. I will now answer the questions listed in the lab below.



a. My browser sent 4 GET requests
b. They were requested sequentially as shown by the frame numbers.

5. I have now done the same steps as above, clearing the history and cache of my browser, and loaded the new link. Here are the captured packets. I entered the password wrong several times so there are extra packets for the unauthorized responses. I will now answer the questions listed in the lab below.



a. 401 Unauthorized
b. Authorization, contains username and password

PART II DNS

1. First I used nslookup to query a web server in Asia, raumen.co.jp, then I queried a web server for a university in Europe, then queried from the previous server to the mail servers of yahoo and google. This part was unsuccessful.

```
(base) lauren@lauren-vm:~/Desktop/adv-computer-networks/Lab 2$ nslookup raumen.co.jp
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   raumen.co.jp
Address: 49.212.215.136

(base) lauren@lauren-vm:~/Desktop/adv-computer-networks/Lab 2$ nslookup -type=NS raumen.co.jp
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
raumen.co.jp    nameserver = ns2.dns.ne.jp.
raumen.co.jp    nameserver = ns1.dns.ne.jp.

Authoritative answers can be found from:
ns1.dns.ne.jp   internet address = 61.211.236.1
ns2.dns.ne.jp   internet address = 133.167.21.1

(base) lauren@lauren-vm:~/Desktop/adv-computer-networks/Lab 2$
```

```
(base) lauren@lauren-vm:~/Desktop/adv-computer-networks/Lab 2$ nslookup lmu.de
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   lmu.de
Address: 141.84.44.56
Name:   lmu.de
Address: 2001:4ca0:4f06:1:141:84:44:56

(base) lauren@lauren-vm:~/Desktop/adv-computer-networks/Lab 2$ nslookup -type=NS lmu.de
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
lmu.de  nameserver = dns3.lrz.eu.
lmu.de  nameserver = dns2.lrz.bayern.
lmu.de  nameserver = dns1.lrz.de.

Authoritative answers can be found from:
dns2.lrz.bayern internet address = 141.40.9.211
dns1.lrz.de     internet address = 129.187.19.183
dns3.lrz.eu     internet address = 78.128.211.180
dns2.lrz.bayern has AAAA address 2001:4ca0:0:100:0:53:1:2
dns1.lrz.de     has AAAA address 2001:4ca0:0:100:0:53:1:1
dns3.lrz.eu     has AAAA address 2001:718:1:1f:50:56ff:feee:180

(base) lauren@lauren-vm:~/Desktop/adv-computer-networks/Lab 2$
```

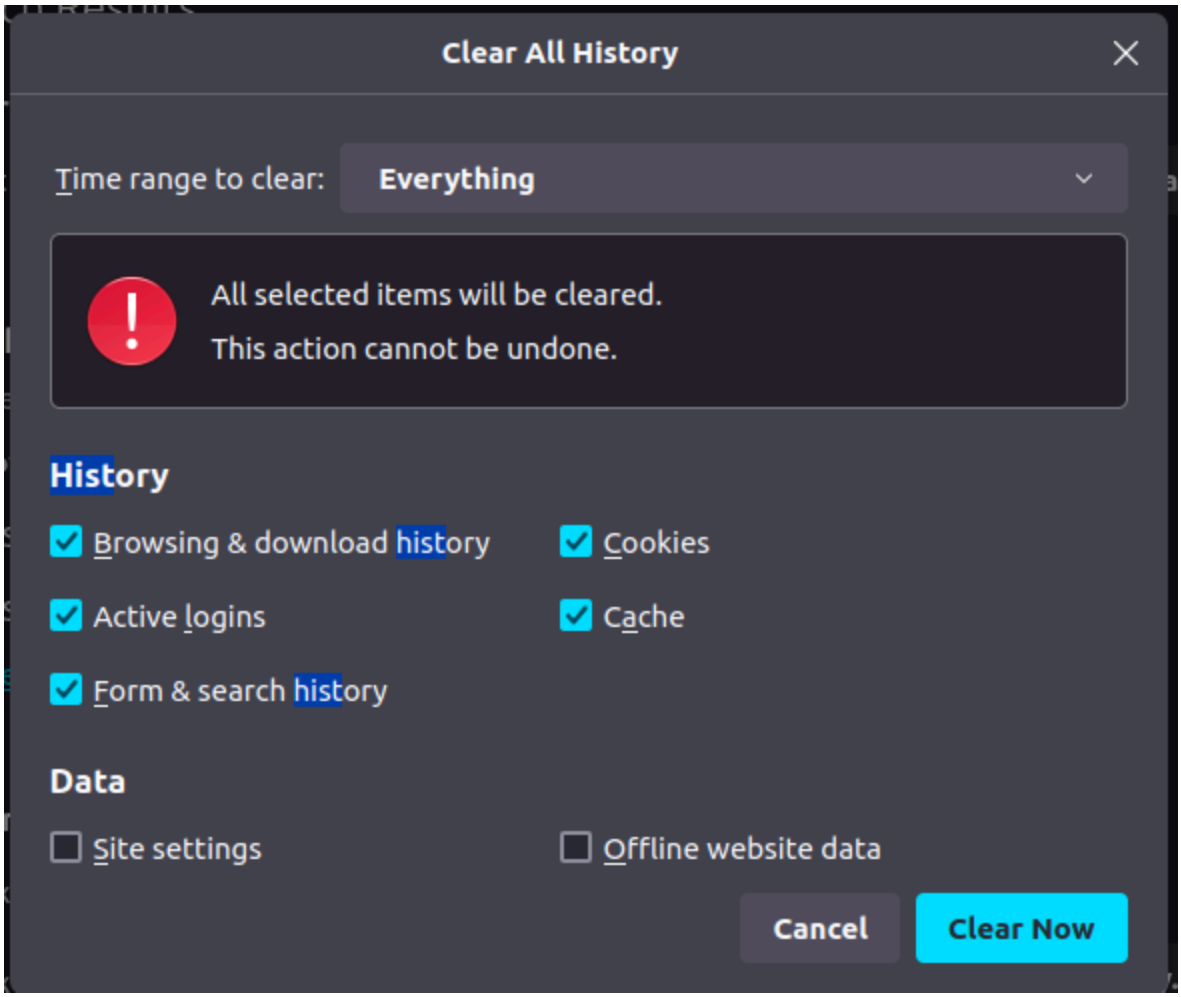
```
(base) lauren@lauren-vm:~/Desktop/adv-computer-networks/Lab 2$ nslookup lmu.de smtp.mail.yahoo.com
;; communications error to 66.163.170.52#53: timed out
;; communications error to 66.163.170.52#53: timed out
;; communications error to 66.163.170.52#53: timed out
;; no servers could be reached


(base) lauren@lauren-vm:~/Desktop/adv-computer-networks/Lab 2$ nslookup lmu.de mail.yahoo.com
;; communications error to 69.147.87.251#53: timed out
;; communications error to 69.147.87.251#53: timed out
;; communications error to 69.147.87.251#53: timed out
;; communications error to 69.147.87.252#53: timed out
;; UDP setup with 2001:4998:20:807::2#53(2001:4998:20:807::2) for lmu.de failed: network unreachable.
;; UDP setup with 2001:4998:20:807::1#53(2001:4998:20:807::1) for lmu.de failed: network unreachable.

(base) lauren@lauren-vm:~/Desktop/adv-computer-networks/Lab 2$ nslookup lmu.de mail.google.com
;; communications error to 142.250.190.133#53: timed out
;; communications error to 142.250.190.133#53: timed out
;; communications error to 142.250.190.133#53: timed out
;; UDP setup with 2607:f8b0:4002:c05::53#53(2607:f8b0:4002:c05::53) for lmu.de failed: network unreachable.
;; UDP setup with 2607:f8b0:4002:c05::11#53(2607:f8b0:4002:c05::11) for lmu.de failed: network unreachable.
;; UDP setup with 2607:f8b0:4002:c05::13#53(2607:f8b0:4002:c05::13) for lmu.de failed: network unreachable.
;; UDP setup with 2607:f8b0:4002:c05::12#53(2607:f8b0:4002:c05::12) for lmu.de failed: network unreachable.

(base) lauren@lauren-vm:~/Desktop/adv-computer-networks/Lab 2$
```

2. Then, I ran ifconfig (Linux platform)

```
(base) lauren@lauren-vm:~/Desktop/adv-computer-networks/Lab 2$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::ac32:5c4b:7a66:6235  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:94:18:b0  txqueuelen 1000  (Ethernet)
        RX packets 23324  bytes 24226851 (24.2 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 10012  bytes 1833912 (1.8 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 538  bytes 49489 (49.4 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 538  bytes 49489 (49.4 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

3. I first flush my DNS, then clear my browser cache, start capturing packets, navigate to the provided link, and then answer the questions.

```
PS C:\Users\laesc\OneDrive\Desktop\repos\adv-computer-networks\Lab 2> ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.
PS C:\Users\laesc\OneDrive\Desktop\repos\adv-computer-networks\Lab 2>
```



ip.addr==10.0.2.15

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.15	192.168.1.254	DNS	97	Standard query 0x3bb3 A mozilla.cloudflare-dns.co
2	0.005624684	10.0.2.15	172.64.41.4	TCP	74	51544 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
3	0.007425343	10.0.2.15	172.64.41.4	TCP	74	51548 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
4	0.019895447	192.168.1.254	10.0.2.15	DNS	129	Standard query response 0x3bb3 A mozilla.cloudfla
5	0.025108094	172.64.41.4	10.0.2.15	TCP	60	443 → 51544 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=
6	0.025155585	10.0.2.15	172.64.41.4	TCP	54	51544 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
7	0.027678123	10.0.2.15	172.64.41.4	TLSv1.3	728	Client Hello
8	0.028181425	172.64.41.4	10.0.2.15	TCP	60	443 → 51544 [ACK] Seq=1 Ack=675 Win=65535 Len=0
9	0.030049774	172.64.41.4	10.0.2.15	TCP	60	443 → 51548 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=
10	0.030134953	10.0.2.15	172.64.41.4	TCP	54	51548 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
11	0.032445163	10.0.2.15	172.64.41.4	TLSv1.3	728	Client Hello
12	0.032885020	172.64.41.4	10.0.2.15	TCP	60	443 → 51548 [ACK] Seq=1 Ack=675 Win=65535 Len=0
13	0.034095794	10.0.2.15	172.64.41.4	TCP	74	51550 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
14	0.056892305	172.64.41.4	10.0.2.15	TCP	60	443 → 51550 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=

```
▸ Frame 1: 97 bytes on wire (776 bits), 97 bytes captured (776 bits) on interface enp0s3, id 0
▸ Ethernet II, Src: PcsCompu_94:18:b0 (08:00:27:94:18:b0), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 192.168.1.254
▸ User Datagram Protocol, Src Port: 53778, Dst Port: 53
▸ Domain Name System (query)
```

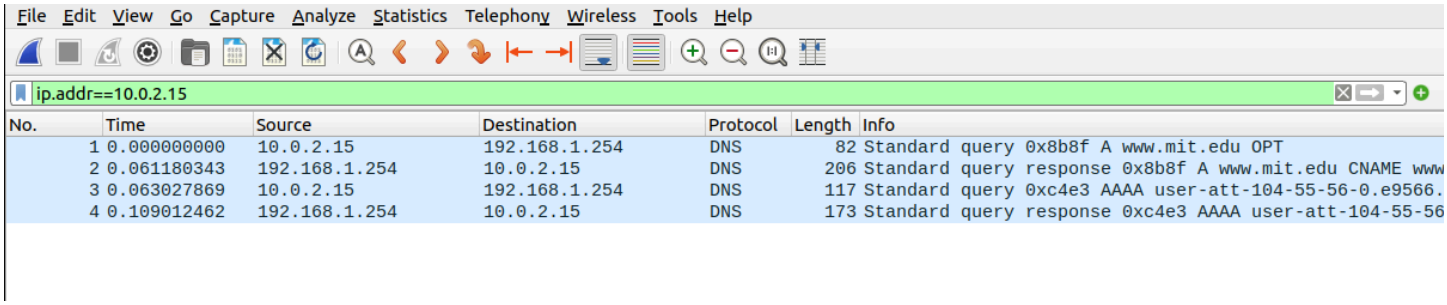
```
0000  52 54 00 12 35 02 08 00  27 94 18 b0 08 00 45 00   RT··5··· '·····E·
0010  00 53 94 1f 00 00 40 11  17 c6 0a 00 02 0f c0 a8   ·S····@· ········
```

wireshark_enp0s3BWRUI2.pcapng Packets: 1121 · Displayed: 1121 (100.0%) · Dropped: 0 (0.0%) Profile: Default

a. The DNS packets are using UDP.
b. 53, 53
c. 192.168.1.254, yes it is my DNS server from ipconfig
d. A, it does have the answer
e. It has two answers to the query
f. Yes it does
g. No it does not issue new DNS queries

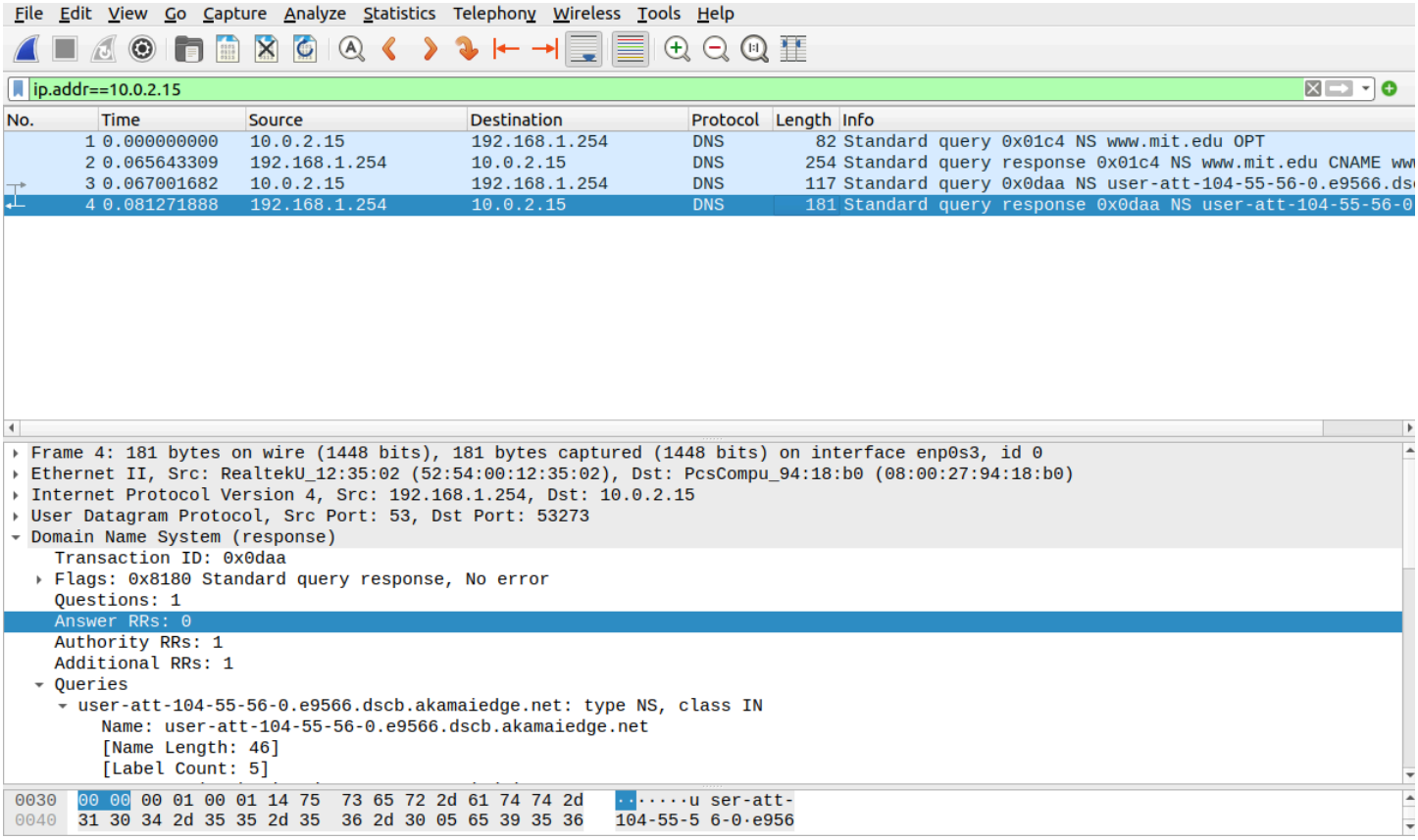
4. Now I do the packet capturing with nslookup.

```
(base) lauren@lauren-vm:~/Desktop/adv-computer-networks/Lab 2$ nslookup www.mit.edu
Server:         127.0.0.53
Address:        127.0.0.53#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.
e9566.dscb.akamaiedge.net       canonical name = user-att-104-55-56-0.e9566.dscb.akamaiedge.net.
Name:   user-att-104-55-56-0.e9566.dscb.akamaiedge.net
Address: 104.118.239.203
Name:   user-att-104-55-56-0.e9566.dscb.akamaiedge.net
Address: 2600:1404:6400:380::255e
Name:   user-att-104-55-56-0.e9566.dscb.akamaiedge.net
Address: 2600:1404:6400:389::255e
```



a. 53, 53
b. 192.168.1.254, yes this is my default DNS server
c. AAAA, no the query itself does not contain answers only the response
d. It has two answers in the response

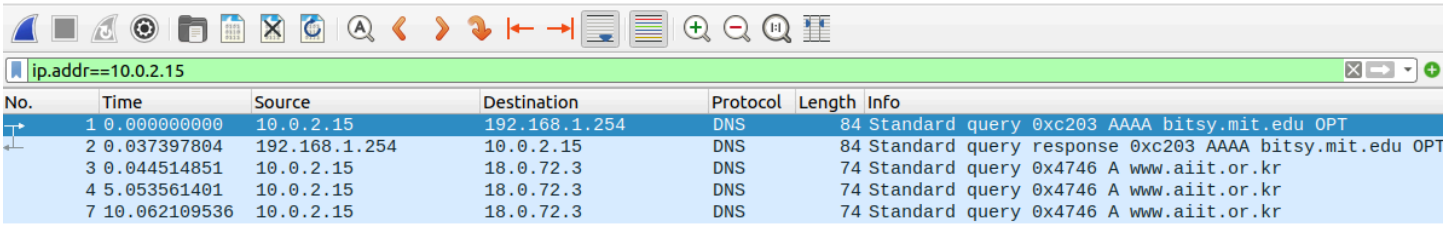
Now with the -type=NS

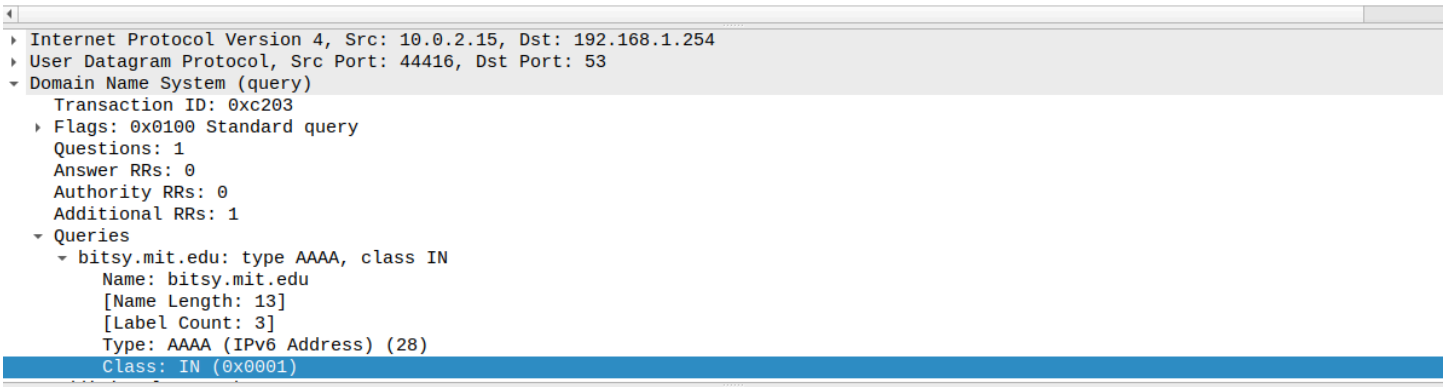


a. 192.168.1.254, yes this is my default DNS server
b. NS, no the query itself does not contain answers only the response
c.

```
Authoritative nameservers
  dscb.akamaiedge.net: type SOA, class IN, mname n0dscb.akamaiedge.net
      Name: dscb.akamaiedge.net
      Type: SOA (Start Of a zone of Authority) (6)
      Class: IN (0x0001)
      Time to live: 1000 (16 minutes, 40 seconds)
      Data length: 52
      Primary name server: n0dscb.akamaiedge.net
      Responsible authority's mailbox: hostmaster.akamai.com
      Serial Number: 1707278495
      Refresh Interval: 1000 (16 minutes, 40 seconds)
      Retry Interval: 1000 (16 minutes, 40 seconds)
      Expire limit: 1000 (16 minutes, 40 seconds)
      Minimum TTL: 1800 (30 minutes)
```

Now for the command nslookup www.aiit.or.kt bitsy.mit.edu. It was not successful


ip.addr==10.0.2.15
No. Time Source Destination Protocol Length Info
1 0.000000000 10.0.2.15 192.168.1.254 DNS 84 Standard query 0xc203 AAAA bitsy.mit.edu OPT
2 0.037397804 192.168.1.254 10.0.2.15 DNS 84 Standard query response 0xc203 AAAA bitsy.mit.edu OPT
3 0.044514851 10.0.2.15 18.0.72.3 DNS 74 Standard query 0x4746 A www.aiit.or.kr
4 5.053561401 10.0.2.15 18.0.72.3 DNS 74 Standard query 0x4746 A www.aiit.or.kr
7 10.062109536 10.0.2.15 18.0.72.3 DNS 74 Standard query 0x4746 A www.aiit.or.kr


Internet Protocol Version 4, Src: 10.0.2.15, Dst: 192.168.1.254
User Datagram Protocol, Src Port: 44416, Dst Port: 53
Domain Name System (query)
Transaction ID: 0xc203
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 1
Queries
bitsy.mit.edu: type AAAA, class IN
Name: bitsy.mit.edu
[Name Length: 13]
[Label Count: 3]
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)