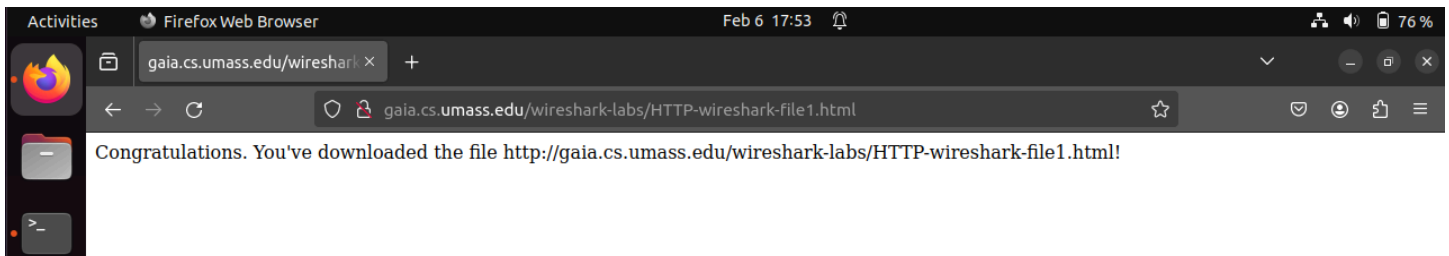
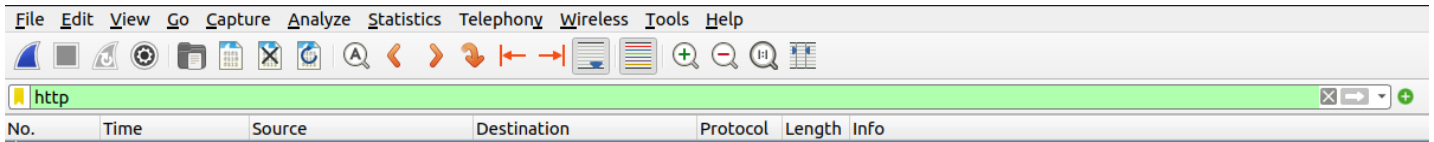
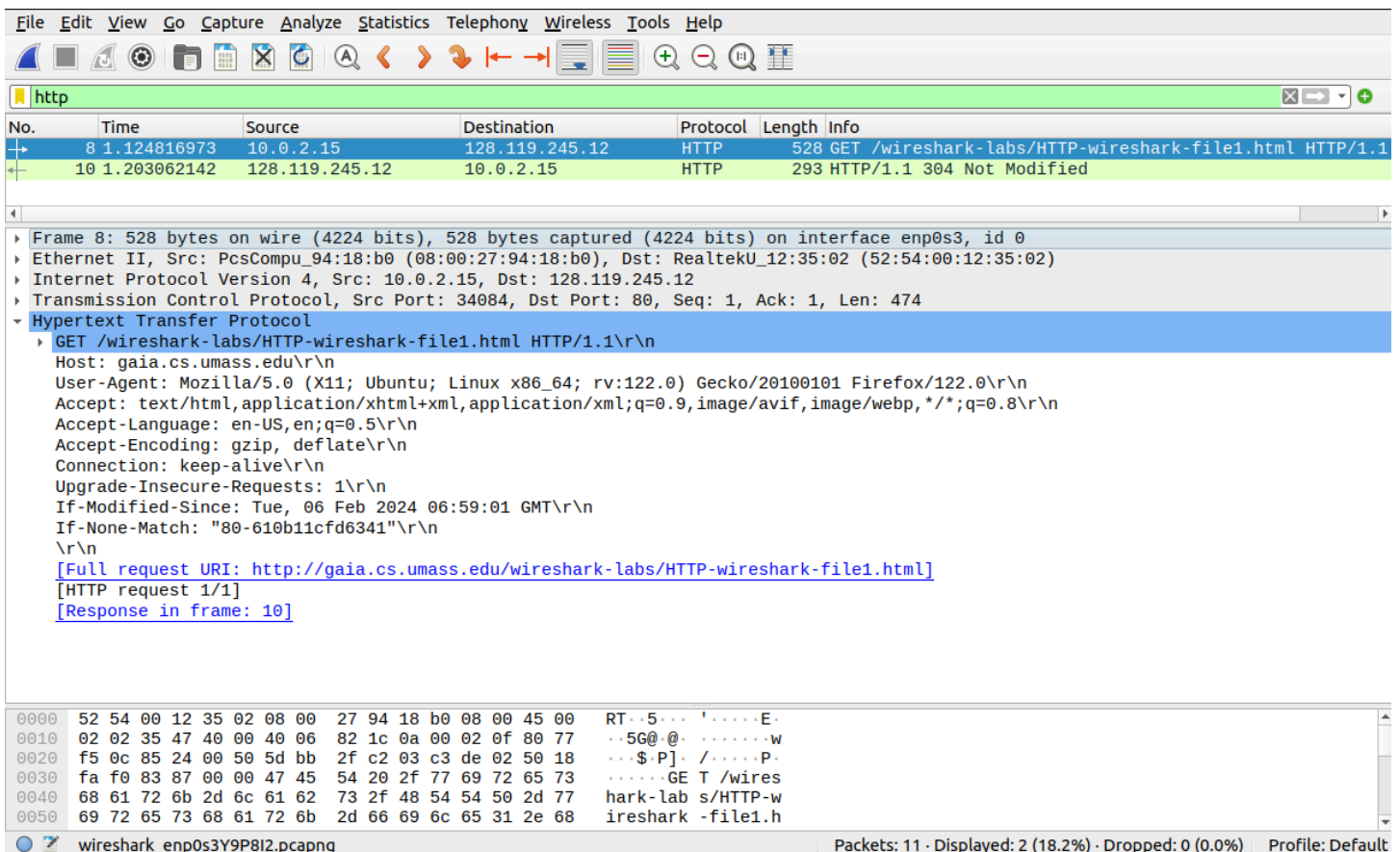


## PART I HTTP

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.



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
12	0.098717808	128.119.245.12	10.0.2.15	HTTP	486	HTTP/1.1 200 OK

Frame 12: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface enp0s3, id 0

Ethernet II, Src: RealtekU\_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu\_94:18:b0 (08:00:27:94:18:b0)

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.2.15

Transmission Control Protocol, Src Port: 80, Dst Port: 56174, Seq: 1, Ack: 390, Len: 486

Hypertext Transfer Protocol

HTTP/1.1 200 OK

Date: Wed, 07 Feb 2024 00:10:29 GMT

Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod\_perl/2.0.11 Perl/v5.16.3

Last-Modified: Tue, 06 Feb 2024 06:59:01 GMT

Etag: "80-610b11cfd6341"

Accept-Ranges: bytes

Content-Length: 128

Keep-Alive: timeout=5, max=100

Connection: Keep-Alive

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

[HTTP response 1/2]

[Time since request: 0.098717808 seconds]

[Request in frame: 10]

[Next request in frame: 14]

[Next response in frame: 16]

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

File Data: 128 bytes

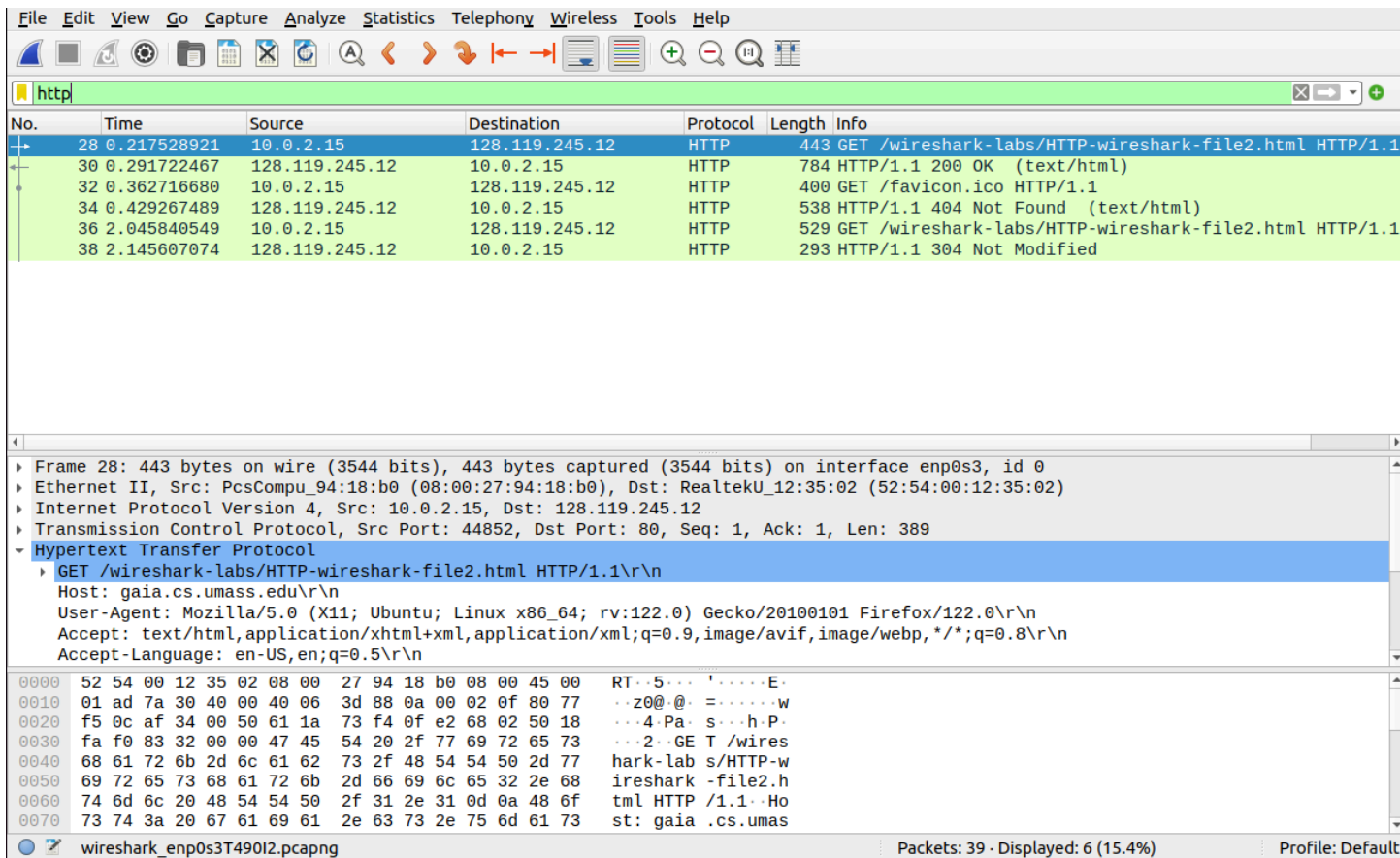
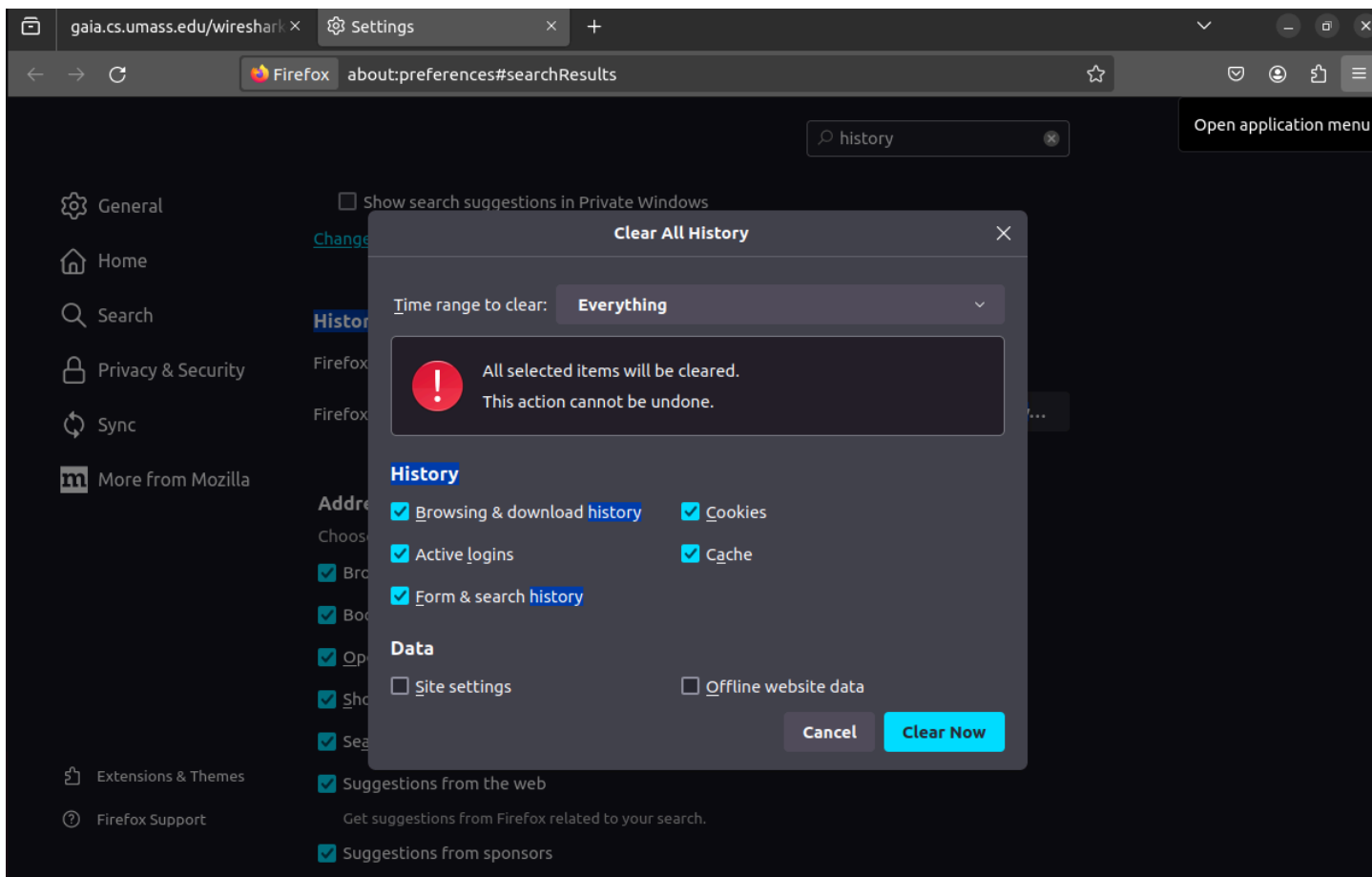
Line-based text data: text/html (4 lines)

Offset	Hex	ASCII
0000	08 00 27 94 18 b0 52 54 00 12 35 02 08 00 45 00	...RT...5..E..
0010	02 0e 2a 93 00 00 40 06 cc c4 80 77 f5 0c 0a 00	...*...@...w...
0020	02 0f 00 50 db 6e 0d 1d 6c 02 f4 82 87 f6 50 18	...P..n...l...P..
0030	ff ff ee 3d 00 00 48 54 54 50 2f 31 2e 31 20 32	...=...HT TP/1.1 2
0040	30 30 20 4f 4b 0d 0a 44 61 74 65 3a 20 57 65 64	00 OK..D ate: Wed
0050	2c 20 30 37 20 46 65 62 20 32 30 32 34 20 30 30	, 07 Feb 2024 00
0060	3a 31 30 3a 32 39 20 47 4d 54 0d 0a 53 65 72 76	:10:29 G MT..Serv
0070	65 72 3a 20 41 70 61 63 68 65 2f 32 2e 34 2e 36	er: Apac he/2.4.6

wireshark\_enp0s320UXI2.pcapng Packets: 43 · Displayed: 6 (14.0%) Profile: Default

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



- No, there is not a "If-Modified-Since" in the very first request packet.
- Yes, it is under "Line-based text data".
- Yes, there is an "If-Modified-Since" and it is followed by the day and time at which I had previously searched it.
- 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.

The image shows a Wireshark packet capture of an HTTP transaction. The packet list at the top shows four packets: a GET request (No. 10), a 200 OK response (No. 14), a GET request for a favicon (No. 100), and a 404 Not Found response (No. 148). The packet details pane for packet 14 shows the full HTTP response structure, including the status line (200 OK), headers (Date, Server, Last-Modified, ETag, Accept-Ranges, Content-Length, Keep-Alive, Connection, Content-Type), and the body (HTML content). The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
10	0.313903903	10.0.2.15	128.119.245.12	HTTP	443	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
14	0.391008829	128.119.245.12	10.0.2.15	HTTP	1995	HTTP/1.1 200 OK (text/html)
100	0.661740277	10.0.2.15	128.119.245.12	HTTP	400	GET /favicon.ico HTTP/1.1
148	0.748580235	128.119.245.12	10.0.2.15	HTTP	538	HTTP/1.1 404 Not Found (text/html)

Frame 14: 1995 bytes on wire (15960 bits), 1995 bytes captured (15960 bits) on interface enp0s3, id 0  
 Ethernet II, Src: RealtekU\_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu\_94:18:b0 (08:00:27:94:18:b0)  
 Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.2.15  
 Transmission Control Protocol, Src Port: 80, Dst Port: 50178, Seq: 2921, Ack: 390, Len: 1941  
 [2 Reassembled TCP Segments (4861 bytes): #12(2920), #14(1941)]  
 Hypertext Transfer Protocol  
 HTTP/1.1 200 OK\r\n  
 Date: Wed, 07 Feb 2024 00:22:21 GMT\r\n  
 Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod\_perl/2.0.11 Perl/v5.16.3\r\n  
 Last-Modified: Tue, 06 Feb 2024 06:59:01 GMT\r\n  
 ETag: "1194-610b11cfd20d9"\r\n  
 Accept-Ranges: bytes\r\n  
 Content-Length: 4500\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 1/2]  
 [Time since request: 0.077104926 seconds]

Frame (1995 bytes)   Reassembled TCP (4861 bytes)

0000 08 00 27 94 18 b0 52 54 00 12 35 02 08 00 45 00   ..'...RT..5...E.  
 0010 07 bd 2e e9 00 00 40 06 c2 bf 80 77 f5 0c 0a 00   .....@...w....  
 0020 02 0f 00 50 c4 02 12 93 e7 6a d7 4d 86 24 50 18   ..P....j.M.\$P..  
 0030 ff ff 89 42 00 00 74 69 61 2c 20 77 68 65 6e 20   ...B...ti a, when  
 0040 69 6e 20 61 63 74 75 61 6c 20 73 65 72 76 69 63   in actua l servic  
 0050 65 20 69 6e 20 74 69 6d 65 20 6f 66 20 77 61 72   e in tim e of war

Packets: 204 · Displayed: 4 (2.0%) · Dropped: 0 (0.0%)   Profile: Default

- My browser sent one packet, the first in the trace list above.
- The second packet in the trace above contains the response code and phrase of the request.
- 200 OK
- 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.

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
http						
No.	Time	Source	Destination	Protocol	Length	Info
30	0.432139637	10.0.2.15	128.119.245.12	HTTP	443	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
33	0.500353137	128.119.245.12	10.0.2.15	HTTP	1355	HTTP/1.1 200 OK (text/html)
35	0.713557470	10.0.2.15	128.119.245.12	HTTP	400	GET /pearson.png HTTP/1.1
57	0.780093610	128.119.245.12	10.0.2.15	HTTP	2233	HTTP/1.1 200 OK (PNG)
66	0.901628261	10.0.2.15	128.119.245.12	HTTP	400	GET /favicon.ico HTTP/1.1
68	0.967842805	128.119.245.12	10.0.2.15	HTTP	538	HTTP/1.1 404 Not Found (text/html)
72	1.124708179	10.0.2.15	178.79.137.164	HTTP	367	GET /8E_cover_small.jpg HTTP/1.1
74	1.692702407	178.79.137.164	10.0.2.15	HTTP	225	HTTP/1.1 301 Moved Permanently
116	2.142990182	10.0.2.15	104.93.21.33	OCSP	477	Request
118	2.193239255	104.93.21.33	10.0.2.15	OCSP	943	Response

Frame 33: 1355 bytes on wire (10840 bits), 1355 bytes captured (10840 bits) on interface enp0s3, id 0						
Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_94:18:b0 (08:00:27:94:18:b0)						
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.2.15						
Transmission Control Protocol, Src Port: 80, Dst Port: 47156, Seq: 1, Ack: 390, Len: 1301						
Hypertext Transfer Protocol						
HTTP/1.1 200 OK\r\n						
Date: Wed, 07 Feb 2024 00:28:39 GMT\r\n						
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n						
Last-Modified: Tue, 06 Feb 2024 06:59:01 GMT\r\n						
ETag: "3ae-610b11cfd53a1"\r\n						
Accept-Ranges: bytes\r\n						
Content-Length: 942\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 1/3]						
[Time since request: 0.068213500 seconds]						
[Request in frame: 30]						
[Next request in frame: 35]						

0000	08 00 27 94 18 b0 52 54	00 12 35 02 08 00 45 00	..!...RT ..5...E..
0010	05 3d 2f 8e 00 00 40 06	c4 9a 80 77 f5 0c 0a 00	./...@. ...w....

Frame (frame), 1,355 bytes      Packets: 237 · Displayed: 10 (4.2%) · Dropped: 0 (0.0%)      Profile: Default

- My browser sent 4 GET requests
- 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.

No.	Time	Source	Destination	Protocol	Length	Info
25	28.353174257	128.119.245.12	10.0.2.15	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
29	36.501649443	10.0.2.15	128.119.245.12	HTTP	518	GET /wireshark-labs/protected_pages/HTTP-wireshar
36	36.568026848	10.0.2.15	128.119.245.12	HTTP	518	GET /wireshark-labs/protected_pages/HTTP-wireshar
38	36.639289925	128.119.245.12	10.0.2.15	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
44	49.118444350	10.0.2.15	128.119.245.12	HTTP	518	GET /wireshark-labs/protected_pages/HTTP-wireshar
51	49.217370122	10.0.2.15	128.119.245.12	HTTP	518	GET /wireshark-labs/protected_pages/HTTP-wireshar
53	49.285529072	128.119.245.12	10.0.2.15	HTTP	544	HTTP/1.1 200 OK (text/html)
55	49.518746545	10.0.2.15	128.119.245.12	HTTP	416	GET /favicon.ico HTTP/1.1
57	49.586468923	128.119.245.12	10.0.2.15	HTTP	538	HTTP/1.1 404 Not Found (text/html)

Frame 53: 544 bytes on wire (4352 bits), 544 bytes captured (4352 bits) on interface enp0s3, id 0
Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_94:18:b0 (08:00:27:94:18:b0)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.2.15
Transmission Control Protocol, Src Port: 80, Dst Port: 42028, Seq: 1, Ack: 465, Len: 490
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
Date: Wed, 07 Feb 2024 00:35:12 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n
Last-Modified: Tue, 06 Feb 2024 06:59:01 GMT\r\n
ETag: "84-610b11cfd6ef9"\r\n
Accept-Ranges: bytes\r\n
Content-Length: 132\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 1/2]
[Time since request: 0.068158950 seconds]
[Request in frame: 51]
[Next request in frame: 55]

0000	08 00 27 94 18 b0 52 54	00 12 35 02 08 00 45 00	..'....RT..5...E..
0010	02 12 33 98 00 00 40 06	c3 bb 80 77 f5 0c 0a 00	..3...@...w....

wireshark\_enp0s3EKO4I2.pcapng      Packets: 61 · Displayed: 12 (19.7%) · Dropped: 0 (0.0%)      Profile: Default

- 401 Unauthorized
- Authorization, contains username and password

## PART II DNS

- 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
```

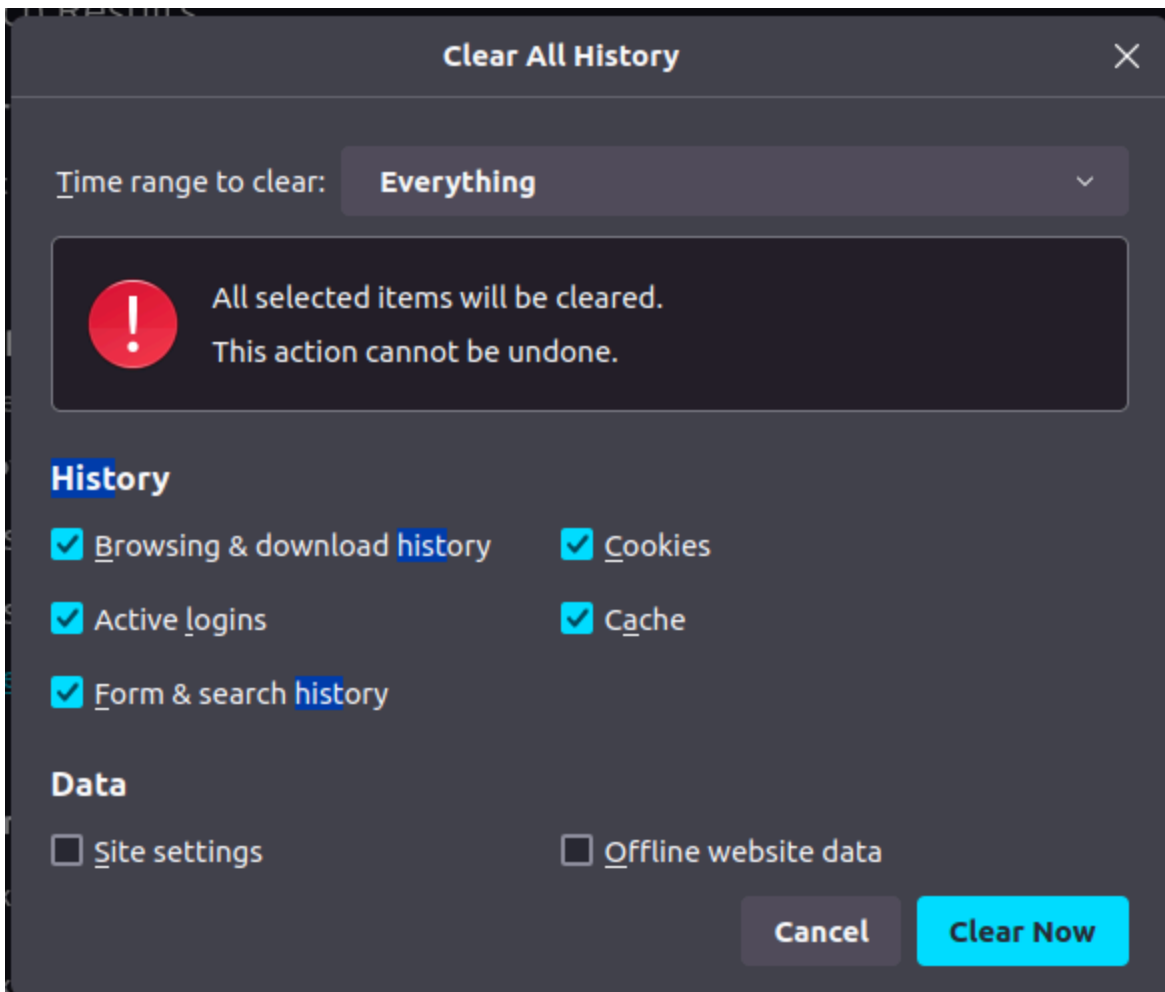
3. I first flush my DNS, then clear my browser cache, start capturing packets, navigate to the provided link, and then answer the questions.

```
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>
```





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
```

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
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	82	Standard query 0x8b8f A www.mit.edu OPT
2	0.061180343	192.168.1.254	10.0.2.15	DNS	206	Standard query response 0x8b8f A www.mit.edu CNAME www
3	0.063027869	10.0.2.15	192.168.1.254	DNS	117	Standard query 0xc4e3 AAAA user-att-104-55-56-0.e9566.
4	0.109012462	192.168.1.254	10.0.2.15	DNS	173	Standard query response 0xc4e3 AAAA user-att-104-55-56

- 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

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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	82	Standard query 0x01c4 NS www.mit.edu OPT
2	0.065643309	192.168.1.254	10.0.2.15	DNS	254	Standard query response 0x01c4 NS www.mit.edu CNAME ww
3	0.067001682	10.0.2.15	192.168.1.254	DNS	117	Standard query 0x0daa NS user-att-104-55-56-0.e9566.ds
4	0.081271888	192.168.1.254	10.0.2.15	DNS	181	Standard query response 0x0daa NS user-att-104-55-56-0

Frame 4: 181 bytes on wire (1448 bits), 181 bytes captured (1448 bits) on interface enp0s3, id 0

Ethernet II, Src: RealtekU\_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu\_94:18:b0 (08:00:27:94:18:b0)

Internet Protocol Version 4, Src: 192.168.1.254, Dst: 10.0.2.15

User Datagram Protocol, Src Port: 53, Dst Port: 53273

Domain Name System (response)

Transaction ID: 0x0daa

Flags: 0x8180 Standard query response, No error

Questions: 1

Answer RRs: 0

Authority RRs: 1

Additional RRs: 1

Queries

user-att-104-55-56-0.e9566.dscb.akamaiedge.net: type NS, class IN

Name: user-att-104-55-56-0.e9566.dscb.akamaiedge.net

[Name Length: 46]

[Label Count: 5]

0030 00 00 00 01 00 01 14 75 73 65 72 2d 61 74 74 2d ..u ser-att-

0040 31 30 34 2d 35 35 2d 35 36 2d 30 05 65 39 35 36 104-55-5 6-0.e956

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

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)

c.

Now for the command nslookup [www.aiit.or.kt](http://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.iiit.or.kr
4	5.053561401	10.0.2.15	18.0.72.3	DNS	74	Standard query 0x4746 A www.iiit.or.kr
7	10.062109536	10.0.2.15	18.0.72.3	DNS	74	Standard query 0x4746 A www.iiit.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)

```