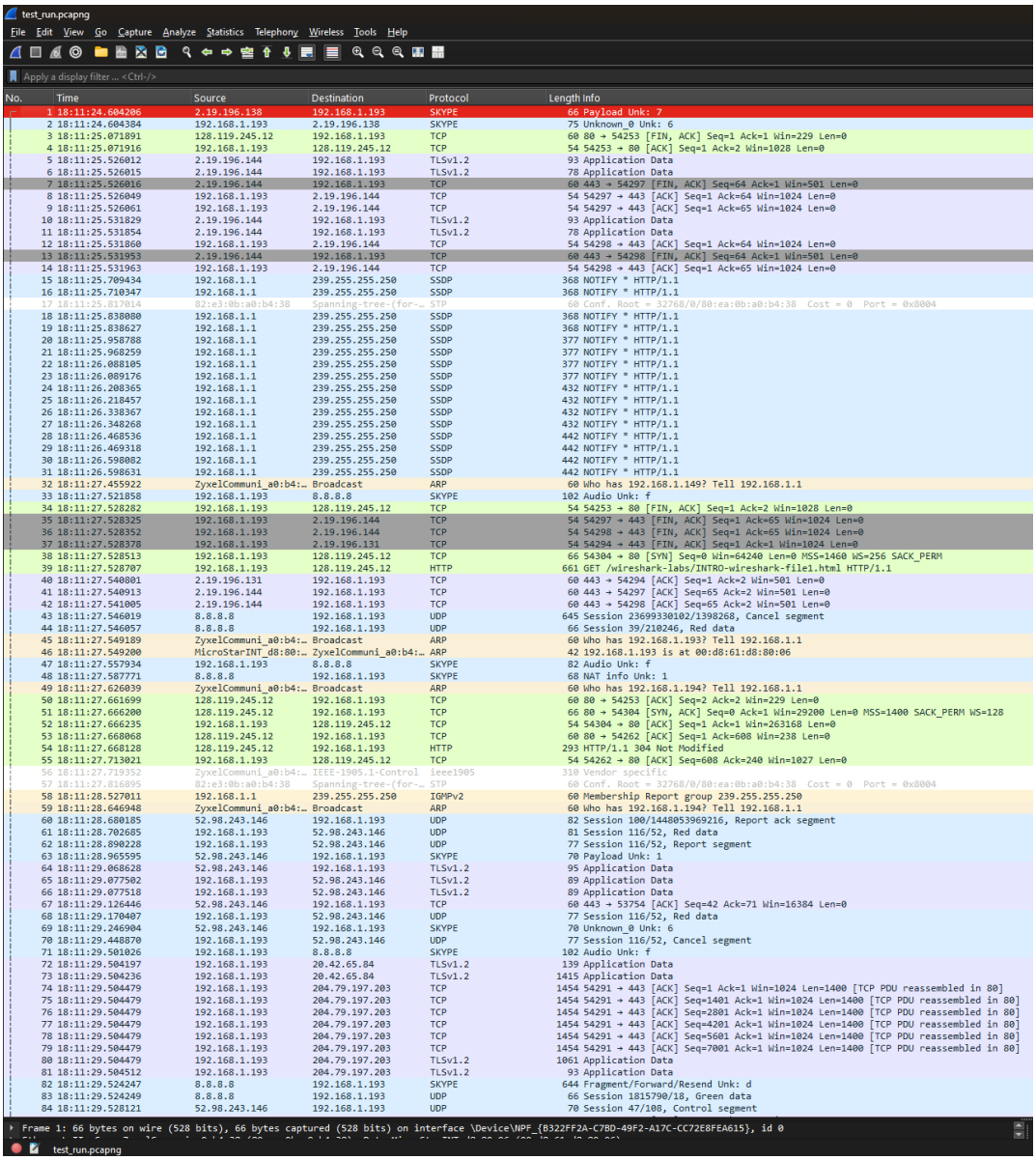
CS 421 Wireshark Assignment
Görkem Kadir Solun 22003214
Taking Wireshark for a Test Run

What to hand in

1. List up to 10 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.

ieee1905, UDP, TLSv1.3, TLSv1.2, TCP, STP, SKYPE, HTTP, DNS, BFCP, ARP



No.	Time	Source	Destination	Protocol	Length	Info
1	18:11:24.604206	2.19.196.138	192.168.1.193	SKYPE	66	Payload Unk: 7
2	18:11:24.604384	192.168.1.193	2.19.196.138	SKYPE	75	Unknown_0 Unk: 6
3	18:11:25.071891	128.119.245.12	192.168.1.193	TCP	60	80 → 54253 [FIN, ACK] Seq=1 Ack=1 Win=229 Len=0
4	18:11:25.071916	192.168.1.193	128.119.245.12	TCP	54	54253 → 80 [ACK] Seq=1 Ack=2 Win=1028 Len=0
5	18:11:25.526012	2.19.196.144	192.168.1.193	TLSv1.2	93	Application Data
6	18:11:25.526015	2.19.196.144	192.168.1.193	TLSv1.2	78	Application Data
7	18:11:25.526016	2.19.196.144	192.168.1.193	TCP	60	443 → 54297 [FIN, ACK] Seq=64 Ack=1 Win=501 Len=0
8	18:11:25.526049	192.168.1.193	2.19.196.144	TCP	54	54297 → 443 [ACK] Seq=1 Ack=64 Win=1024 Len=0
9	18:11:25.526061	192.168.1.193	2.19.196.144	TCP	54	54297 → 443 [ACK] Seq=1 Ack=65 Win=1024 Len=0
10	18:11:25.531829	2.19.196.144	192.168.1.193	TLSv1.2	93	Application Data
11	18:11:25.531854	2.19.196.144	192.168.1.193	TLSv1.2	78	Application Data
12	18:11:25.531860	192.168.1.193	2.19.196.144	TCP	54	54298 → 443 [ACK] Seq=1 Ack=64 Win=1024 Len=0
13	18:11:25.531953	2.19.196.144	192.168.1.193	TCP	60	443 → 54298 [FIN, ACK] Seq=64 Ack=1 Win=501 Len=0
14	18:11:25.531963	192.168.1.193	2.19.196.144	TCP	54	54298 → 443 [ACK] Seq=1 Ack=65 Win=1024 Len=0
15	18:11:25.709434	192.168.1.1	239.255.255.250	SSDP	368	NOTIFY * HTTP/1.1
16	18:11:25.710347	192.168.1.1	239.255.255.250	SSDP	368	NOTIFY * HTTP/1.1
17	18:11:25.817014	82:e3:0b:a0:b4:38	Spanning-tree-(for-…	STP	60	Conf. Root = 32768/0/80:ea:0b:a0:b4:38 Cost = 0 Port = 0x8004
18	18:11:25.838080	192.168.1.1	239.255.255.250	SSDP	368	NOTIFY * HTTP/1.1
19	18:11:25.838627	192.168.1.1	239.255.255.250	SSDP	368	NOTIFY * HTTP/1.1
20	18:11:25.958788	192.168.1.1	239.255.255.250	SSDP	377	NOTIFY * HTTP/1.1
21	18:11:25.968259	192.168.1.1	239.255.255.250	SSDP	377	NOTIFY * HTTP/1.1
22	18:11:26.088105	192.168.1.1	239.255.255.250	SSDP	377	NOTIFY * HTTP/1.1
23	18:11:26.089176	192.168.1.1	239.255.255.250	SSDP	377	NOTIFY * HTTP/1.1
24	18:11:26.208365	192.168.1.1	239.255.255.250	SSDP	432	NOTIFY * HTTP/1.1
25	18:11:26.218457	192.168.1.1	239.255.255.250	SSDP	432	NOTIFY * HTTP/1.1
26	18:11:26.338367	192.168.1.1	239.255.255.250	SSDP	432	NOTIFY * HTTP/1.1
27	18:11:26.348268	192.168.1.1	239.255.255.250	SSDP	432	NOTIFY * HTTP/1.1
28	18:11:26.468536	192.168.1.1	239.255.255.250	SSDP	442	NOTIFY * HTTP/1.1
29	18:11:26.469318	192.168.1.1	239.255.255.250	SSDP	442	NOTIFY * HTTP/1.1
30	18:11:26.598082	192.168.1.1	239.255.255.250	SSDP	442	NOTIFY * HTTP/1.1
31	18:11:26.598631	192.168.1.1	239.255.255.250	SSDP	442	NOTIFY * HTTP/1.1
32	18:11:27.455922	ZyxelCommuni_a0:b4:…	Broadcast	ARP	60	Who has 192.168.1.149? Tell 192.168.1.1
33	18:11:27.521858	192.168.1.193	8.8.8.8	SKYPE	102	Audio Unk: f
34	18:11:27.528282	192.168.1.193	128.119.245.12	TCP	54	54253 → 80 [FIN, ACK] Seq=1 Ack=2 Win=1028 Len=0
35	18:11:27.528325	192.168.1.193	2.19.196.144	TCP	54	54297 → 443 [FIN, ACK] Seq=1 Ack=65 Win=1024 Len=0
36	18:11:27.528352	192.168.1.193	2.19.196.144	TCP	54	54298 → 443 [FIN, ACK] Seq=1 Ack=65 Win=1024 Len=0
37	18:11:27.528378	192.168.1.193	2.19.196.131	TCP	54	54294 → 443 [FIN, ACK] Seq=1 Ack=1 Win=1024 Len=0
38	18:11:27.528513	192.168.1.193	128.119.245.12	TCP	66	54304 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
39	18:11:27.528707	192.168.1.193	128.119.245.12	HTTP	661	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
40	18:11:27.540801	2.19.196.131	192.168.1.193	TCP	60	443 → 54294 [ACK] Seq=1 Ack=2 Win=501 Len=0
41	18:11:27.540913	2.19.196.144	192.168.1.193	TCP	60	443 → 54297 [ACK] Seq=65 Ack=2 Win=501 Len=0
42	18:11:27.541005	2.19.196.144	192.168.1.193	TCP	60	443 → 54298 [ACK] Seq=65 Ack=2 Win=501 Len=0
43	18:11:27.546019	8.8.8.8	192.168.1.193	UDP	645	Session 23699330102/1398268, Cancel segment
44	18:11:27.546057	8.8.8.8	192.168.1.193	UDP	66	Session 39/210246, Red data
45	18:11:27.549189	ZyxelCommuni_a0:b4:…	Broadcast	ARP	60	Who has 192.168.1.193? Tell 192.168.1.1
46	18:11:27.549200	MicroStarINT_d8:80:…	ZyxelCommuni_a0:b4:…	ARP	42	192.168.1.193 is at 00:d8:61:d8:80:06
47	18:11:27.557934	192.168.1.193	8.8.8.8	SKYPE	82	Audio Unk: f
48	18:11:27.587771	8.8.8.8	192.168.1.193	SKYPE	68	NAT info Unk: 1
49	18:11:27.626039	ZyxelCommuni_a0:b4:…	Broadcast	ARP	60	Who has 192.168.1.194? Tell 192.168.1.1
50	18:11:27.661699	128.119.245.12	192.168.1.193	TCP	60	80 → 54253 [ACK] Seq=2 Ack=2 Win=229 Len=0
51	18:11:27.666200	128.119.245.12	192.168.1.193	TCP	66	80 → 54304 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400 SACK_PERM WS=128
52	18:11:27.666235	192.168.1.193	128.119.245.12	TCP	54	54304 → 80 [ACK] Seq=1 Ack=1 Win=263168 Len=0
53	18:11:27.668068	128.119.245.12	192.168.1.193	TCP	60	80 → 54262 [ACK] Seq=1 Ack=608 Win=238 Len=0
54	18:11:27.668128	128.119.245.12	192.168.1.193	HTTP	293	HTTP/1.1 304 Not Modified
55	18:11:27.713021	192.168.1.193	128.119.245.12	TCP	54	54262 → 80 [ACK] Seq=608 Ack=240 Win=1027 Len=0
56	18:11:27.719352	ZyxelCommuni_a0:b4:…	IEEE-1905.1-Control	ieee1905	310	Vendor specific
57	18:11:27.816895	82:e3:0b:a0:b4:38	Spanning-tree-(for-…	STP	60	Conf. Root = 32768/0/80:ea:0b:a0:b4:38 Cost = 0 Port = 0x8004
58	18:11:28.527011	192.168.1.1	239.255.255.250	IGMPv2	60	Membership Report group 239.255.255.250
59	18:11:28.646948	ZyxelCommuni_a0:b4:…	Broadcast	ARP	60	Who has 192.168.1.194? Tell 192.168.1.1
60	18:11:28.680185	52.98.243.146	192.168.1.193	UDP	82	Session 100/1448053969216, Report ack segment
61	18:11:28.702685	192.168.1.193	52.98.243.146	UDP	81	Session 116/52, Red data
62	18:11:28.890228	192.168.1.193	52.98.243.146	UDP	77	Session 116/52, Report segment
63	18:11:28.965595	52.98.243.146	192.168.1.193	SKYPE	70	Payload Unk: 1
64	18:11:29.068628	52.98.243.146	192.168.1.193	TLSv1.2	95	Application Data
65	18:11:29.077502	192.168.1.193	52.98.243.146	TLSv1.2	89	Application Data
66	18:11:29.077518	192.168.1.193	52.98.243.146	TLSv1.2	89	Application Data
67	18:11:29.126446	52.98.243.146	192.168.1.193	TCP	60	443 → 53754 [ACK] Seq=42 Ack=71 Win=16384 Len=0
68	18:11:29.170407	192.168.1.193	52.98.243.146	UDP	77	Session 116/52, Red data
69	18:11:29.246904	52.98.243.146	192.168.1.193	SKYPE	70	Unknown_0 Unk: 6
70	18:11:29.448870	192.168.1.193	52.98.243.146	UDP	77	Session 116/52, Cancel segment
71	18:11:29.501026	192.168.1.193	8.8.8.8	SKYPE	102	Audio Unk: f
72	18:11:29.504197	192.168.1.193	20.42.65.84	TLSv1.2	139	Application Data
73	18:11:29.504236	192.168.1.193	20.42.65.84	TLSv1.2	1415	Application Data
74	18:11:29.504479	192.168.1.193	204.79.197.203	TCP	1454	54291 → 443 [ACK] Seq=1 Ack=1 Win=1024 Len=1400 [TCP PDU reassembled in 80]
75	18:11:29.504479	192.168.1.193	204.79.197.203	TCP	1454	54291 → 443 [ACK] Seq=1401 Ack=1 Win=1024 Len=1400 [TCP PDU reassembled in 80]
76	18:11:29.504479	192.168.1.193	204.79.197.203	TCP	1454	54291 → 443 [ACK] Seq=2801 Ack=1 Win=1024 Len=1400 [TCP PDU reassembled in 80]
77	18:11:29.504479	192.168.1.193	204.79.197.203	TCP	1454	54291 → 443 [ACK] Seq=4201 Ack=1 Win=1024 Len=1400 [TCP PDU reassembled in 80]
78	18:11:29.504479	192.168.1.193	204.79.197.203	TCP	1454	54291 → 443 [ACK] Seq=5601 Ack=1 Win=1024 Len=1400 [TCP PDU reassembled in 80]
79	18:11:29.504479	192.168.1.193	204.79.197.203	TCP	1454	54291 → 443 [ACK] Seq=7001 Ack=1 Win=1024 Len=1400 [TCP PDU reassembled in 80]
80	18:11:29.504479	192.168.1.193	204.79.197.203	TLSv1.2	1061	Application Data
81	18:11:29.504512	192.168.1.193	204.79.197.203	TLSv1.2	93	Application Data
82	18:11:29.524247	8.8.8.8	192.168.1.193	SKYPE	644	Fragment/Forward/Resend Unk: d
83	18:11:29.524249	8.8.8.8	192.168.1.193	UDP	66	Session 1815790/18, Green data
84	18:11:29.528121	52.98.243.146	192.168.1.193	UDP	70	Session 47/108, Control segment

Figure 1: Some of the protocols from the first task

2. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packet listing window is the amount of time, in seconds, since Wireshark tracing began. To display the Time field in time-of-day format, select the Wireshark View pull down menu, then select Time Display Format, then select Time-of-day.)

10652	18:12:56.757061	192.168.1.193	128.119.245.12	HTTP	541 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
10657	18:12:56.895935	128.119.245.12	192.168.1.193	HTTP	492 HTTP/1.1 200 OK (text/html)

~0.12 seconds

3. What is the Internet address of gaia.cs.umass.edu (also known as www.net.cs.umass.edu)? What is the Internet address of your computer?

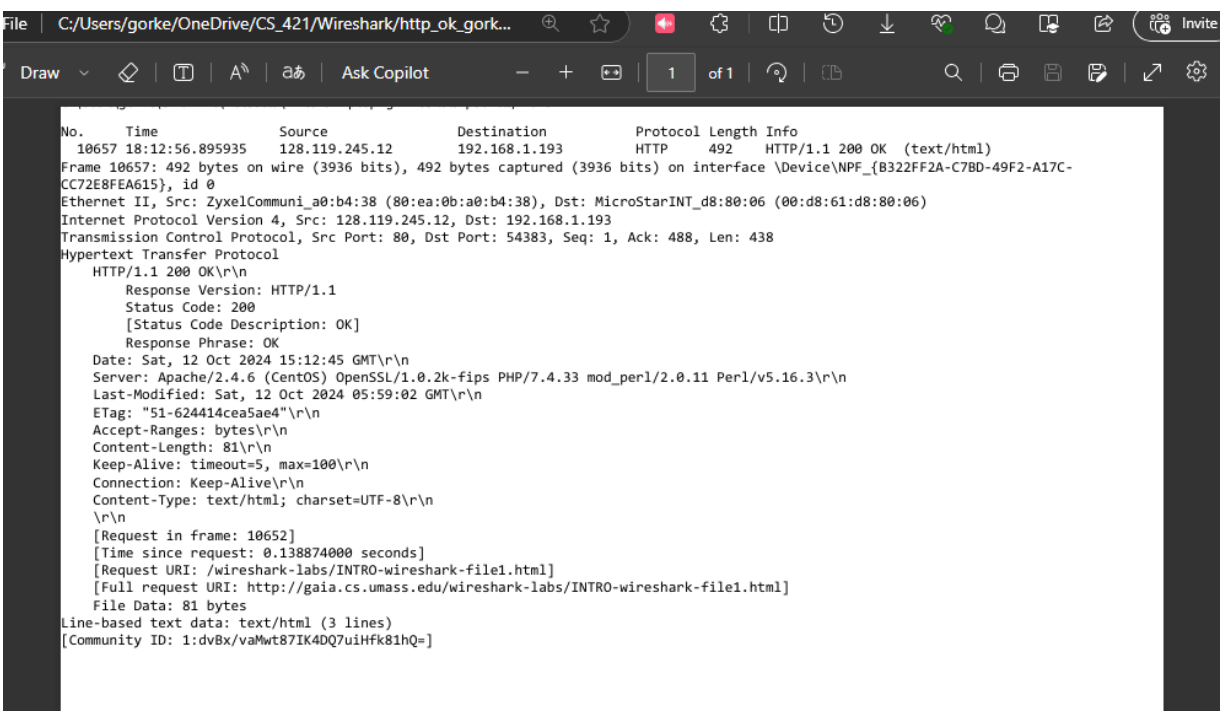
```
PS C:\Users\gorke> nslookup gaia.cs.umass.edu
Server:  dns.google
Address:  8.8.4.4

Non-authoritative answer:
Name:    gaia.cs.umass.edu
Address:  128.119.245.12
```

My computer: 192.169.1.193

gaia.cs.umass.edu: 128.119.245.12

4. Print the two HTTP messages displayed in step 9 above. To do so, select Print from the Wireshark File command menu, and select “Selected Packet Only” and “Print as displayed” and then click OK.




```
No.     Time               Source                Destination           Protocol Length Info
  10657 18:12:56.895935    128.119.245.12        192.168.1.193         HTTP     492    HTTP/1.1 200 OK  (text/html)
Frame 10657: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface \Device\NPF_{B322FF2A-C7BD-49F2-A17C-
CC72E8FEA615}, id 0
Ethernet II, Src: ZyxelCommuni_a0:b4:38 (80:ea:0b:a0:b4:38), Dst: MicroStarINT_d8:80:06 (00:d8:61:d8:80:06)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.193
Transmission Control Protocol, Src Port: 80, Dst Port: 54383, Seq: 1, Ack: 488, Len: 438
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
        Response Version: HTTP/1.1
        Status Code: 200
        [Status Code Description: OK]
        Response Phrase: OK
    Date: Sat, 12 Oct 2024 15:12:45 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: Sat, 12 Oct 2024 05:59:02 GMT\r\n
    ETag: "51-624414cea5ae4"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 81\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
    [Request in frame: 10652]
    [Time since request: 0.138874000 seconds]
    [Request URI: /wireshark-labs/INTRO-wireshark-file1.html]
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
    File Data: 81 bytes
Line-based text data: text/html (3 lines)
[Community ID: 1:dvBx/vaMwt87IK4DQ7uiHfk81hQ=]
```

Figure 2: Print of HTTP OK

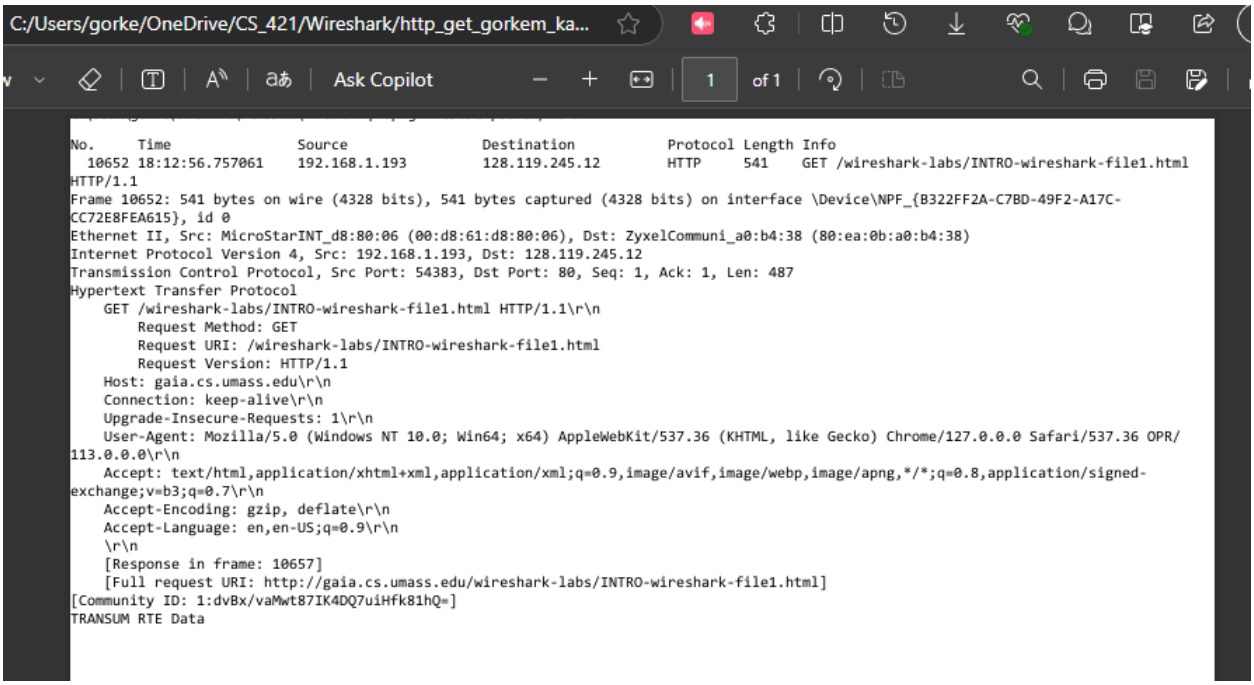


Figure 3: Print of HTTP OK

Wireshark Lab: HTTP

1. The Basic HTTP GET/response interaction

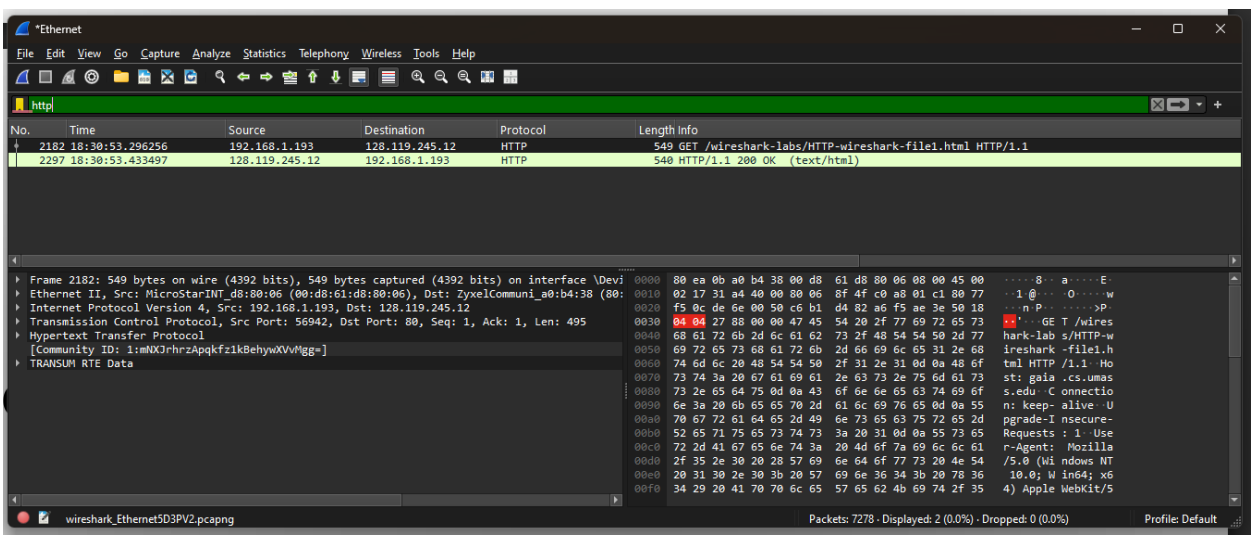
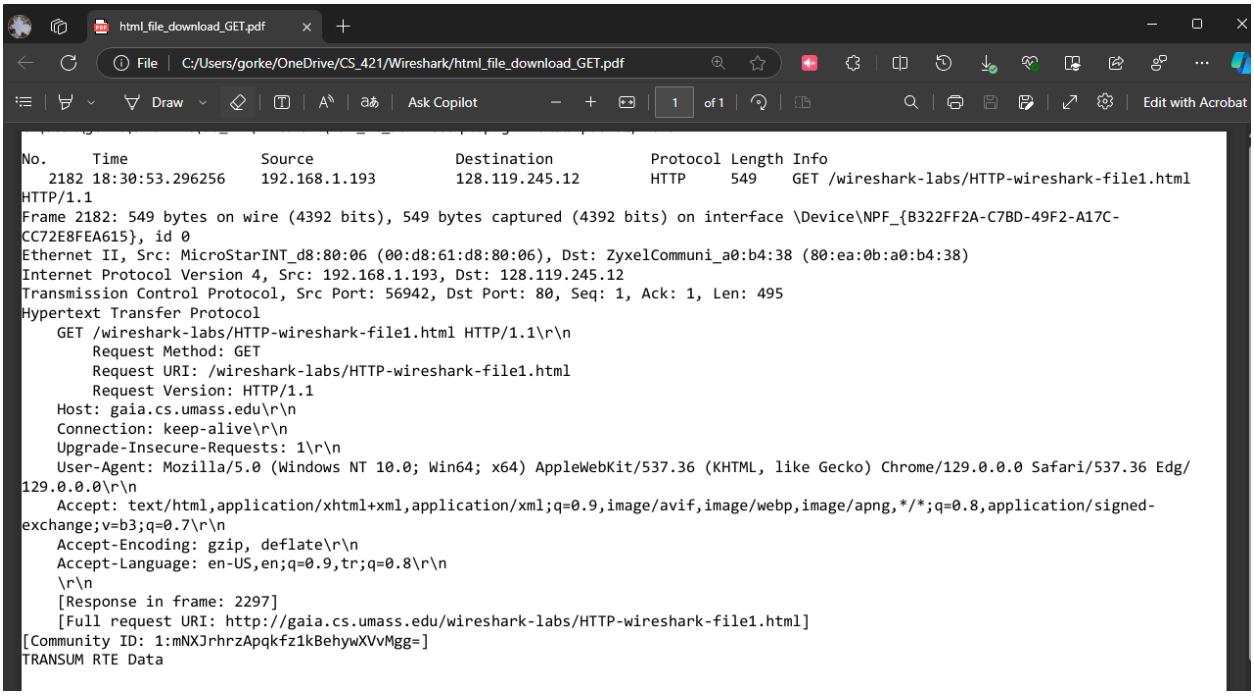
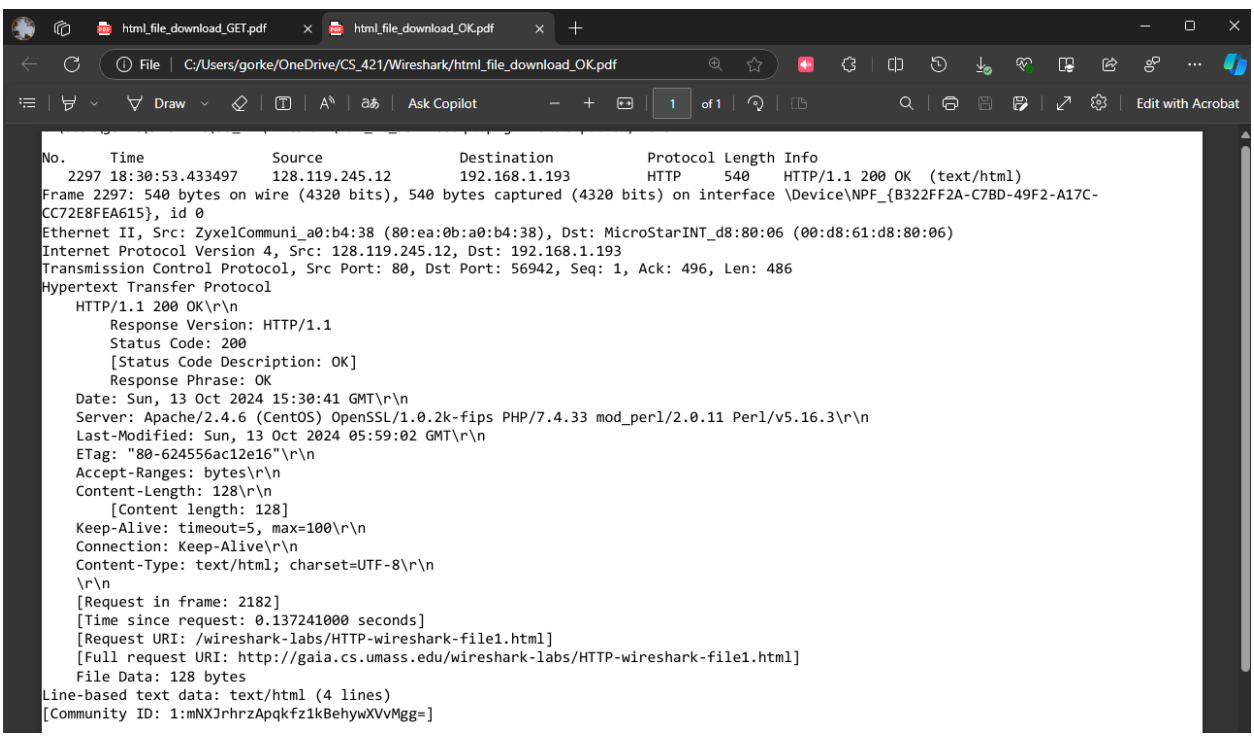


Figure 4: Downloaded the first HTML file



```
No.     Time               Source                Destination           Protocol Length Info
   2182 18:30:53.296256    192.168.1.193         128.119.245.12        HTTP     549    GET /wireshark-labs/HTTP-wireshark-file1.html
HTTP/1.1
Frame 2182: 549 bytes on wire (4392 bits), 549 bytes captured (4392 bits) on interface \Device\NPF_{B322FF2A-C7BD-49F2-A17C-
CC72E8FEA615}, id 0
Ethernet II, Src: MicroStarINT_d8:80:06 (00:d8:61:d8:80:06), Dst: ZyxelCommuni_a0:b4:38 (80:ea:0b:a0:b4:38)
Internet Protocol Version 4, Src: 192.168.1.193, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 56942, Dst Port: 80, Seq: 1, Ack: 1, Len: 495
Hypertext Transfer Protocol
    GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
        Request Method: GET
        Request URI: /wireshark-labs/HTTP-wireshark-file1.html
        Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.0.0 Safari/537.36 Edg/
129.0.0.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.7\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9,tr;q=0.8\r\n
    \r\n
    [Response in frame: 2297]
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
[Community ID: 1:mNXJrhrzApqkfz1kBehywXVvMgg=]
TRANSUM RTE Data
```

Figure 5: HTML file download GET



```
No.     Time               Source                Destination           Protocol Length Info
   2297 18:30:53.433497    128.119.245.12        192.168.1.193         HTTP     540    HTTP/1.1 200 OK  (text/html)
Frame 2297: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_{B322FF2A-C7BD-49F2-A17C-
CC72E8FEA615}, id 0
Ethernet II, Src: ZyxelCommuni_a0:b4:38 (80:ea:0b:a0:b4:38), Dst: MicroStarINT_d8:80:06 (00:d8:61:d8:80:06)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.193
Transmission Control Protocol, Src Port: 80, Dst Port: 56942, Seq: 1, Ack: 496, Len: 486
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
        Response Version: HTTP/1.1
        Status Code: 200
        [Status Code Description: OK]
        Response Phrase: OK
    Date: Sun, 13 Oct 2024 15:30:41 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: Sun, 13 Oct 2024 05:59:02 GMT\r\n
    ETag: "80-624556ac12e16"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 128\r\n
        [Content length: 128]
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [Request in frame: 2182]
    [Time since request: 0.137241000 seconds]
    [Request URI: /wireshark-labs/HTTP-wireshark-file1.html]
    [Full 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)
[Community ID: 1:mNXJrhrzApqkfz1kBehywXVvMgg=]
```

Figure 6: HTML file download OK

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

Both use HTTP 1.1 as we can see the response and request versions in the header.

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

“Accept-Language: en-US,en;q=0.9,tr;q=0.8\r\n” at GET request implies US English and TR Turkish.

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

```
Source              Destination
192.168.1.193       128.119.245.12
```

In the GET request, it says my IP is 192.168.1.193, and gaia.cs.umass.edu’s IP is 128.119.245.12.

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

```
Status Code: 200
[Status Code Description: OK]
Response Phrase: OK
```

It is “200” as written in the OK response.

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

```
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips
Last-Modified: Sun, 13 Oct 2024 05:59:02 GMT\r\n
ETag: "80-624556ac12e16"\r\n
```

It is “Sun, 13 Oct 2024 05:59:02” as written in the OK response.

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

This value is in the "Content-Length: 128" line of the HTTP OK response header.

```
Accept-Ranges: bytes\r\n
Content-Length: 128\r\n
    [Content length: 128]
Keep-Alive: timeout=5, max
```

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.

No additional headers are visible within the raw data not already displayed in the packet-listing window. All the key HTTP headers, such as Date, Server, Last-Modified, ETag, Content-Length, Keep-Alive, Connection, and Content-Type, appear fully displayed in the packet-listing window. Please check Figure 6 above.

2. The HTTP CONDITIONAL GET/response interaction

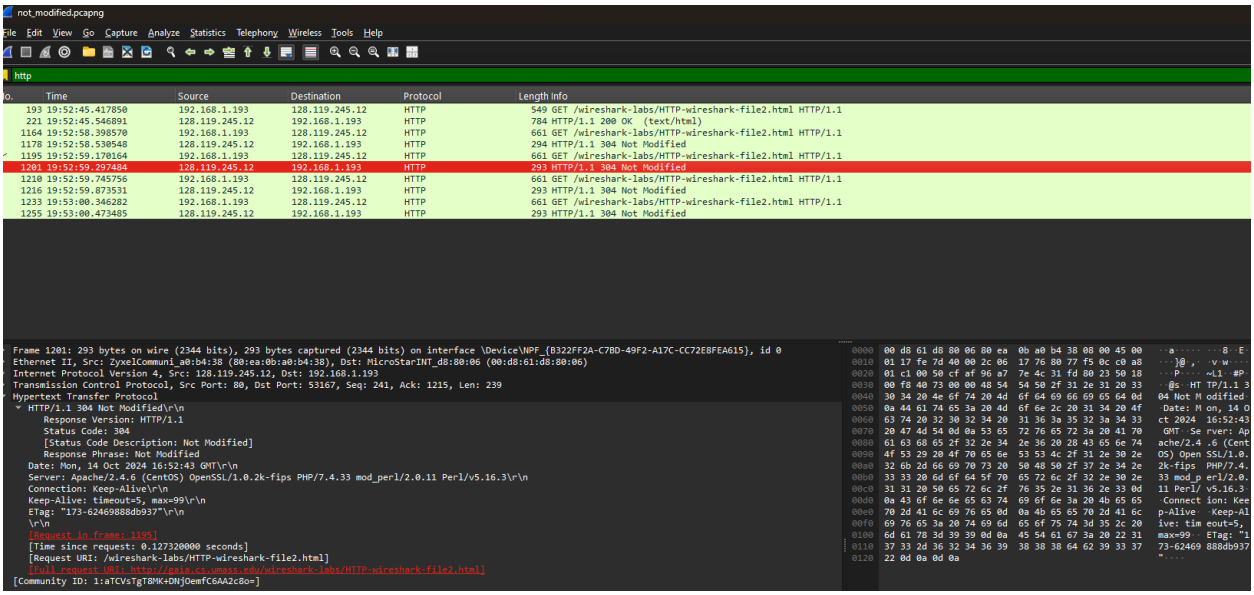


Figure 7: Not modified

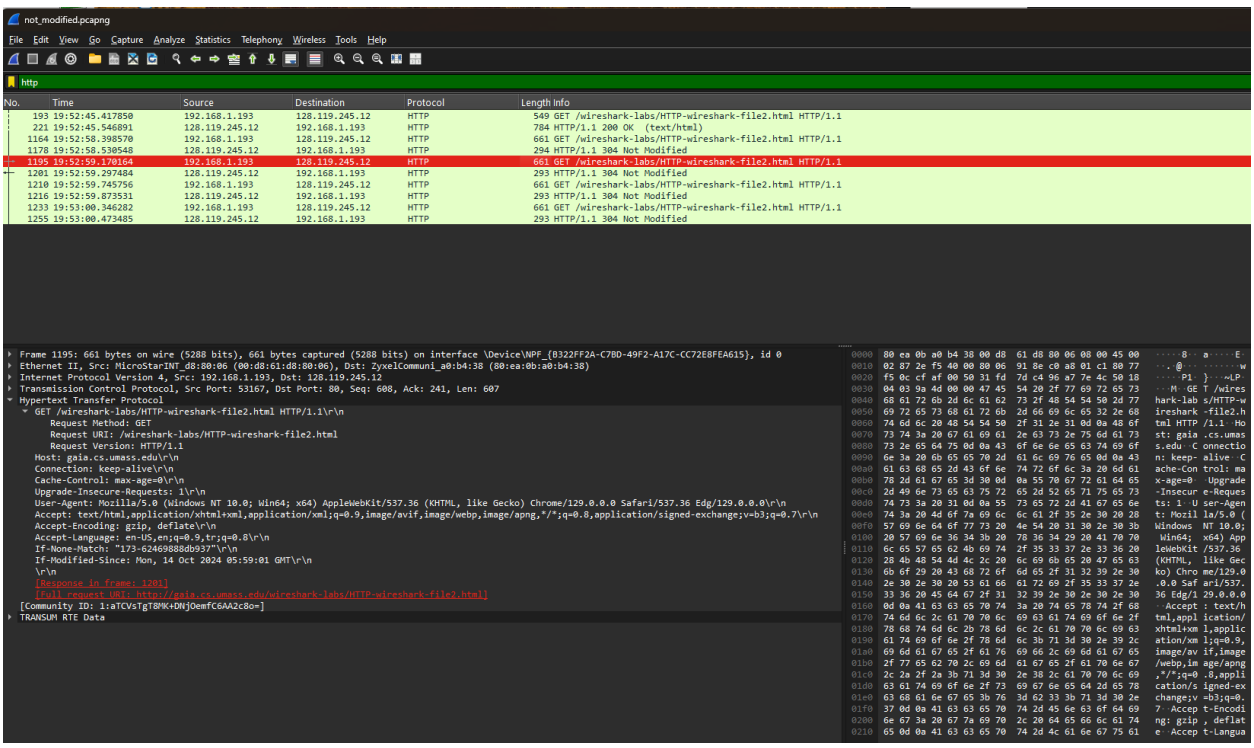


Figure 8: The third GET request of the cached file.

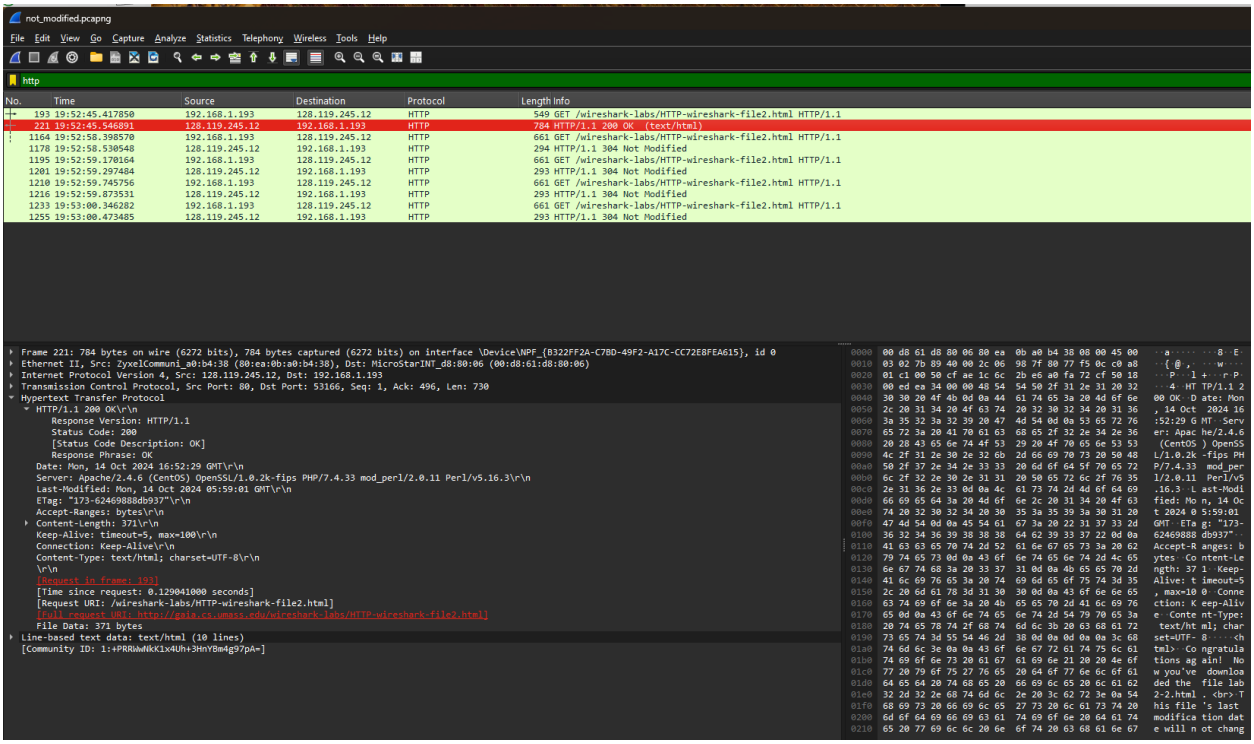


Figure 9: Successful file retrieval with an OK response.

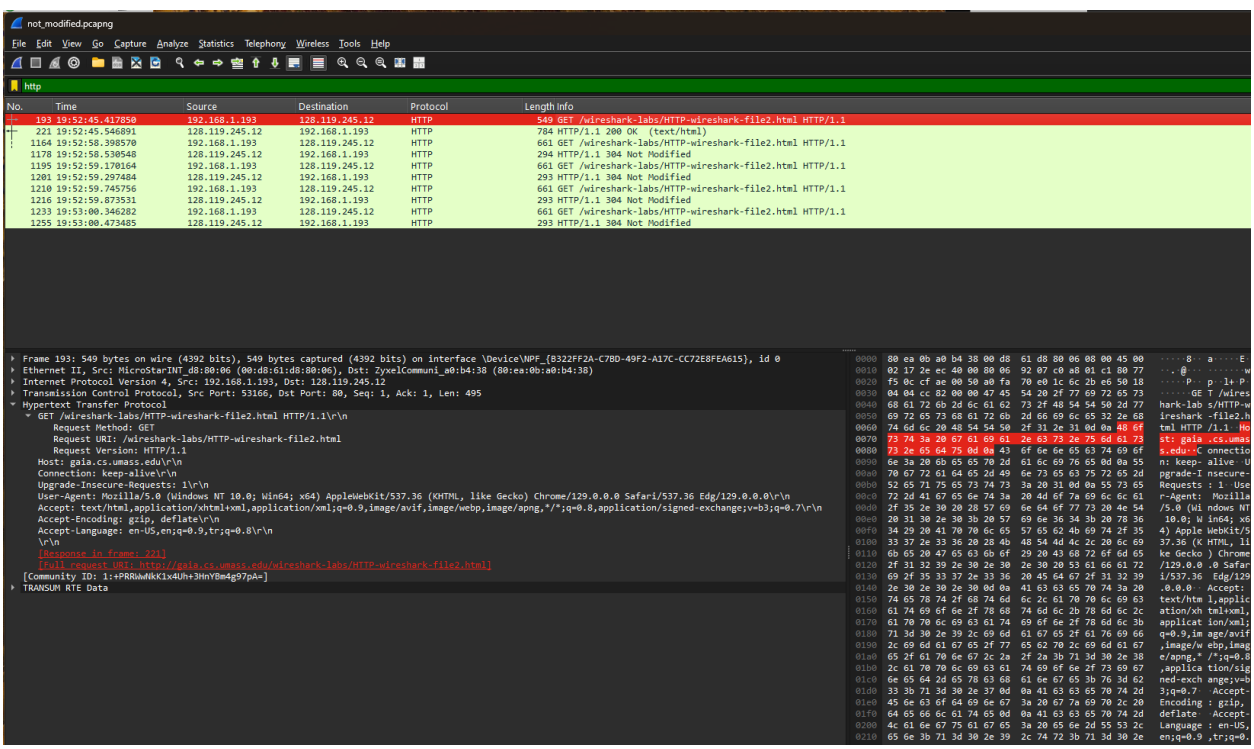


Figure 10: The first GET request of the file.

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?

```
Hypertext Transfer Protocol
  GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
      Request Method: GET
      Request URI: /wireshark-labs/HTTP-wireshark-file2.html
      Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) Apple
    Accept: text/html,application/xhtml+xml,application/xml;q=0
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9,tr;q=0.8\r\n
    \r\n
    [Response in frame: 221]
```

No.

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

```
    [Full request URI: http://gaia.cs.umass.
    File Data: 371 bytes
  Line-based text data: text/html (10 lines)
```

By comparing Figure 9 with 7, we can see that the OK response has the file data. With this, we can tell that the file was retrieved in the OK response and not in the Not modified response.

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?

```
If-None-Match: "173-62469888db937"\r\n
If-Modified-Since: Mon, 14 Oct 2024 05:59:01 GMT\r\n
\r\n
```

Yes. When we first got our file.

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.

```
HTTP/1.1 304 Not Modified\r\n
    Response Version: HTTP/1.1
    Status Code: 304
    [Status Code Description: Not Modified]
    Response Phrase: Not Modified
Date: Mon, 14 Oct 2024 16:52:42 GMT\r\n
```

No. The server did not return the file's contents requested as the file was not modified.

3. Retrieving Long Documents

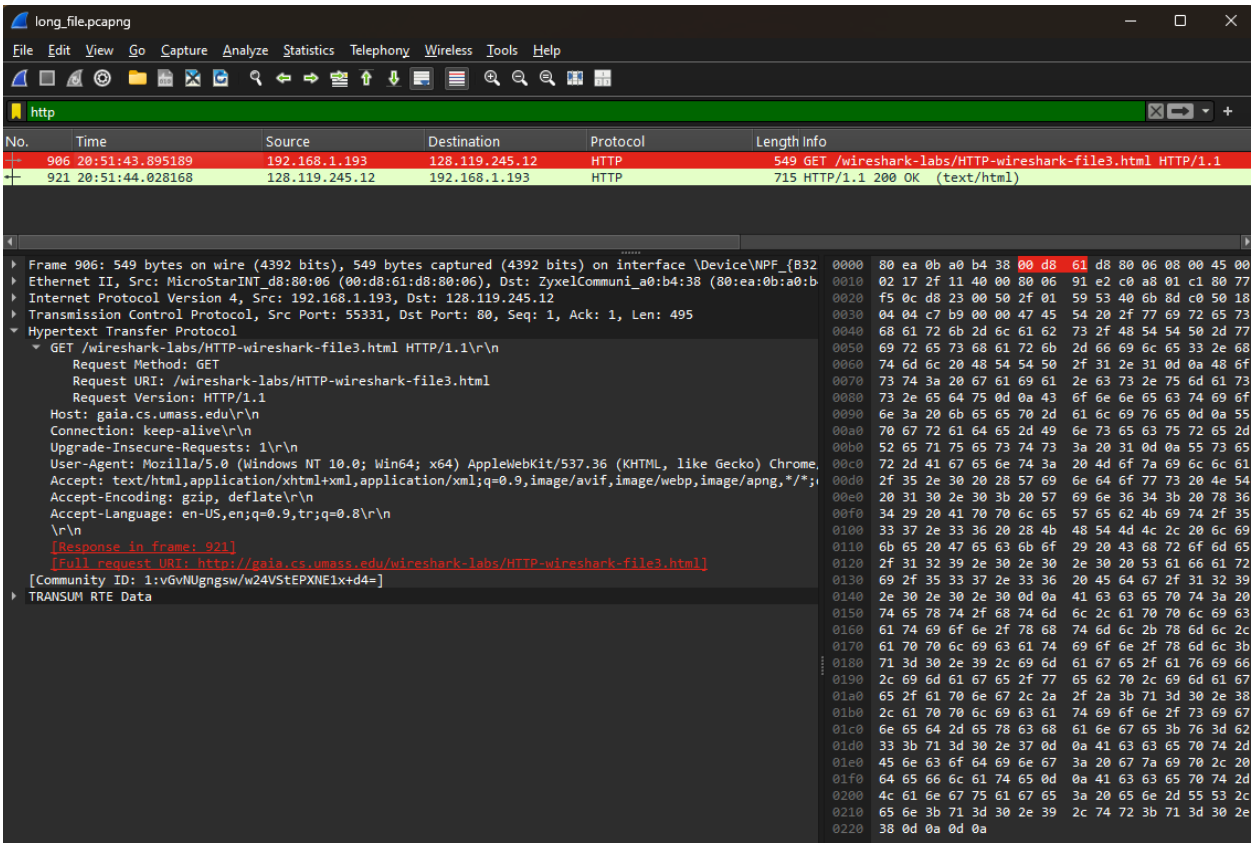


Figure 11: GET request for the long file.

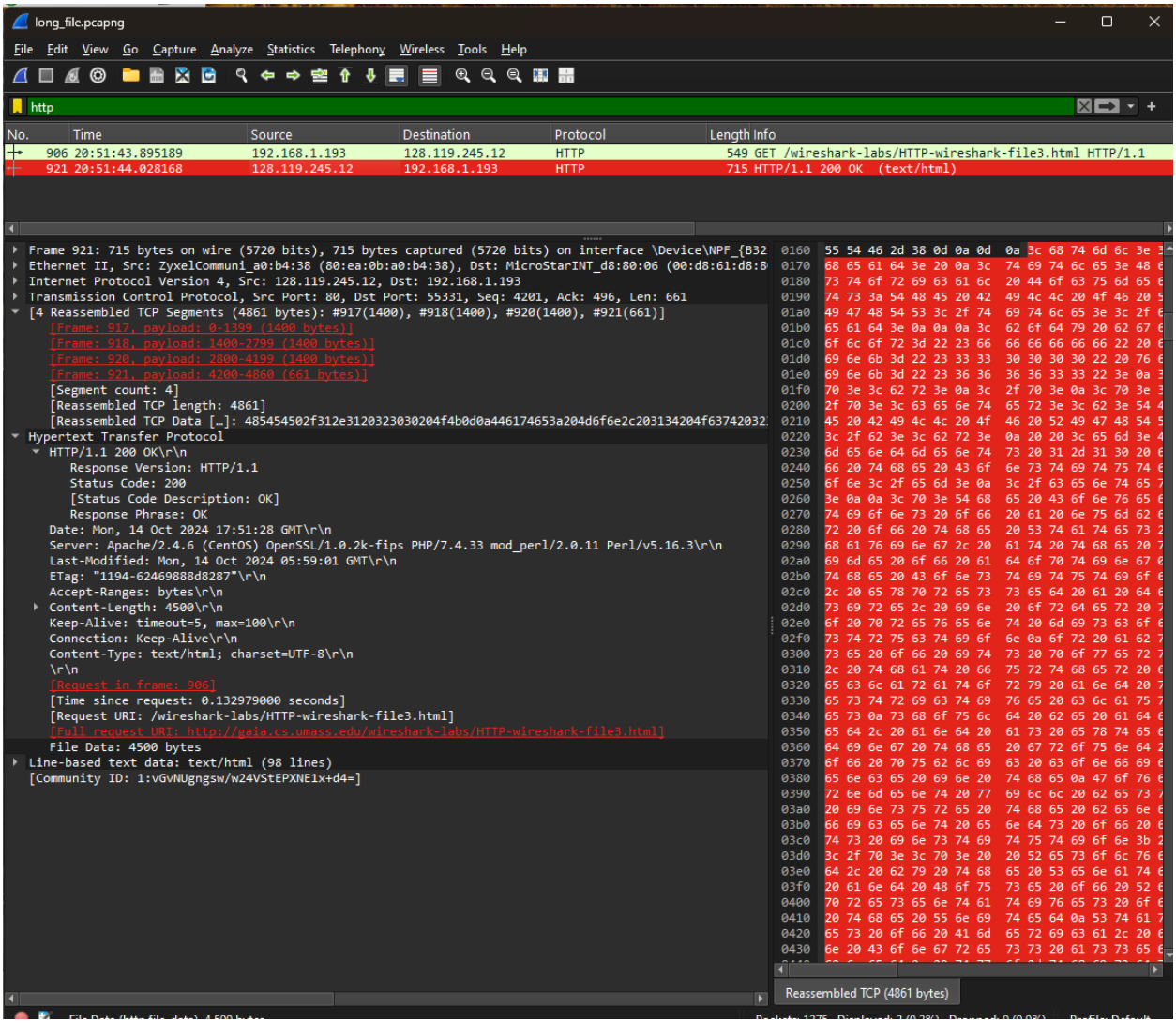
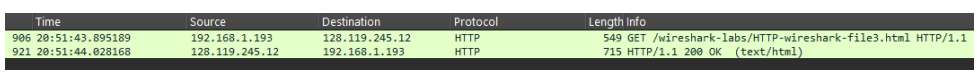


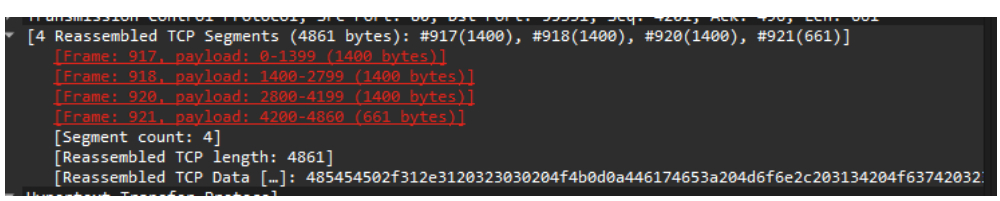
Figure 12: Retrieved long file

12. How many HTTP GET request messages were sent by your browser?



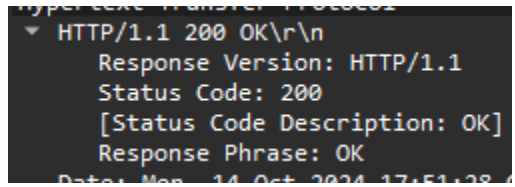
One.

13. How many data-containing TCP segments were needed to carry the single HTTP response?



Four.

14. What is the status code and phrase associated with the response to the HTTP GET request?



200 OK.

15. Are there any HTTP status lines in the transmitted data associated with a TCP induced “Continuation”?

There is no additional HTTP status line in these continuation packets—just the payload's continuation.

4. HTML Documents with Embedded Objects

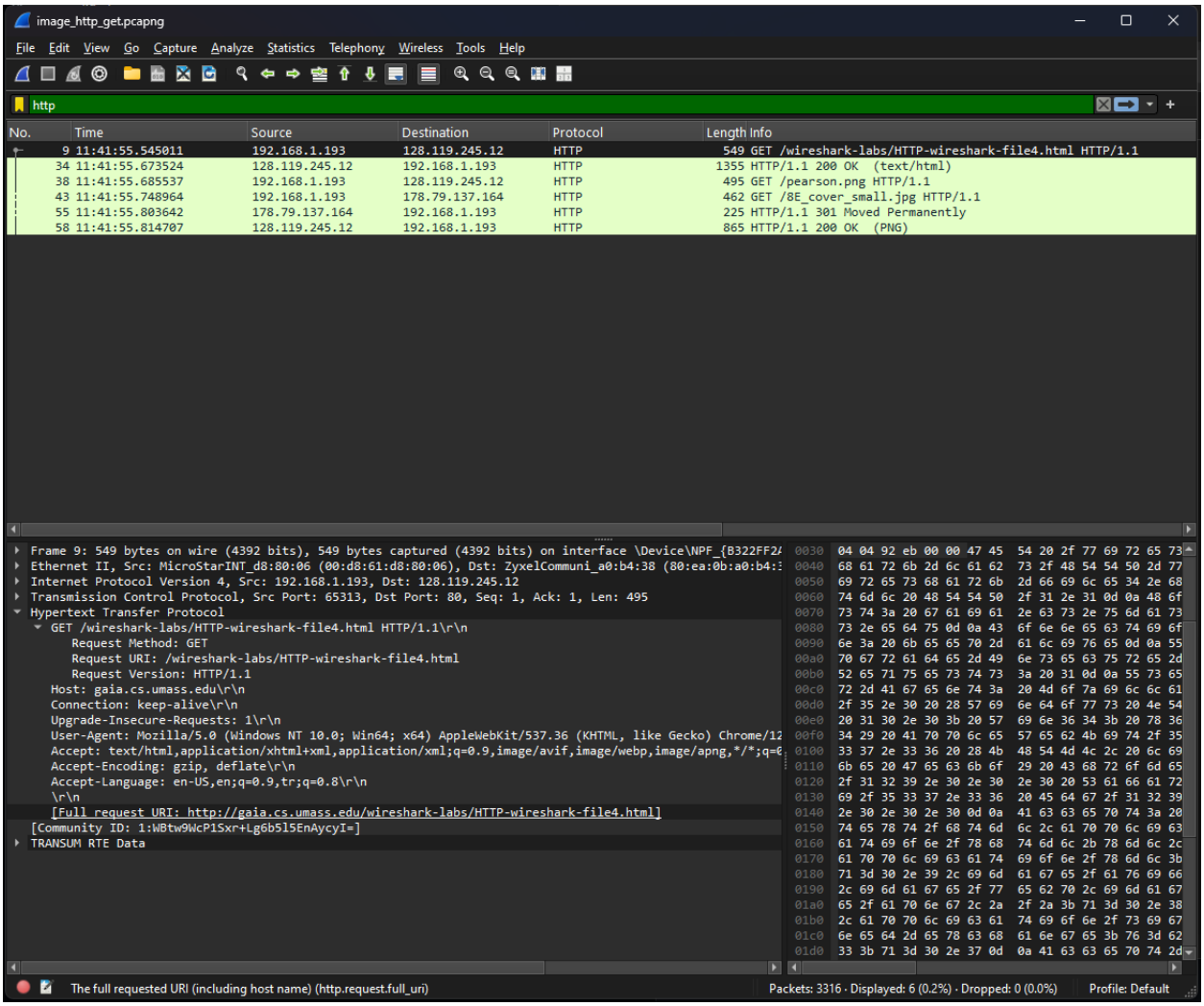
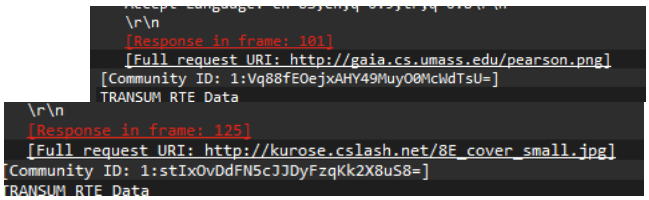


Figure 13: HTTP image get

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



3. One base HTML file and two objects. Addresses are the following: http://kurose.cslash.net/8E_cover_small.jpg, http://gaia.cs.umass.edu/pearson.png. 178.79.137.164, 128.119.245.12

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.

Parallel. You can see that two GET requests are sent consecutively immediately after the HTML file is downloaded.

5. HTTP Authentication

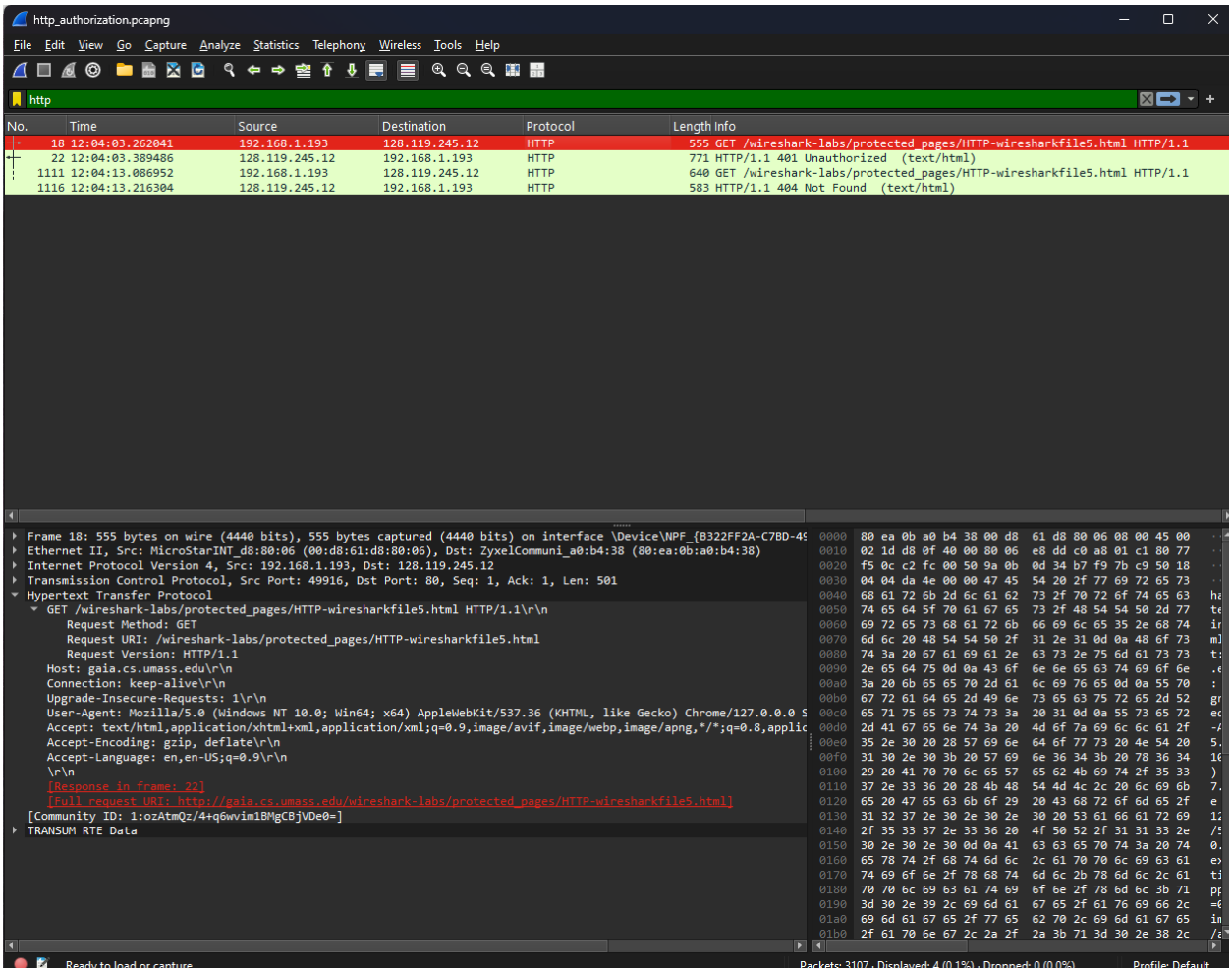
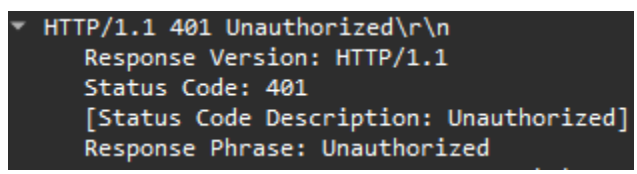


Figure 14: HTTP authorization

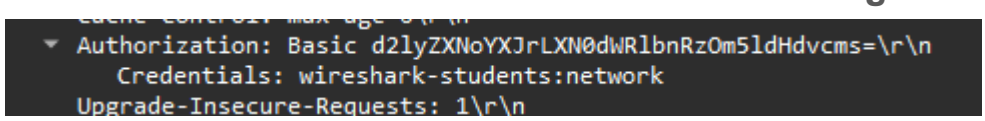
18. What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser?



401 Unauthorized.

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

Authorization



DNS

nslookup

```
PowerShell 7.4.5
PS C:\Users\gorke> nslookup www.mit.edu
Server:  dns.google
Address:  8.8.4.4

Non-authoritative answer:
Name:    e9566.dscb.akamaiedge.net
Addresses:  2a02:26f0:cc00:291::255e
          2a02:26f0:cc00:29d::255e
          104.66.66.27
Aliases:  www.mit.edu
          www.mit.edu.edgekey.net
```

```
PS C:\Users\gorke> nslookup -type=NS mit.edu
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  23.43.64.242

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** Request to UnKnown timed-out
PS C:\Users\gorke>
```

```
PS C:\Users\gorke> nslookup www.aiit.or.kr bitsy.mit.edu
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  18.0.72.3

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** Request to UnKnown timed-out
PS C:\Users\gorke>
```

```
PS C:\Users\gorke> nslookup www.baidu.com
Server:  dns.google
Address:  8.8.4.4

Non-authoritative answer:
Name:    www.wshifen.com
Addresses:  45.113.192.102
          45.113.192.101
Aliases:  www.baidu.com
          www.a.shifen.com

PS C:\Users\gorke>
```

General syntax: nslookup –option1 –option2 host-to-find dns-server

1. Run nslookup to obtain the IP address of a Web server in Asia.

[百度一下，你就知道 (baidu.com)]

Addresses: 45.113.192.102, 45.113.192.101

```
PS C:\Users\gorke> nslookup -type=ns tum.de
Server:  dns.google
Address:  8.8.4.4

Non-authoritative answer:
tum.de  nameserver = dns1.lrz.de
tum.de  nameserver = dns2.lrz.bayern
tum.de  nameserver = dns3.lrz.eu
PS C:\Users\gorke>
```

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

[The Entrepreneurial University - TUM]

3. Run nslookup so that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! mail.

They couldn't find the answer.

```
PS C:\Users\gorke> nslookup -query=mx mail.yahoo.com dns1.lrz.de
Server:  dns1.lrz.de
Address:  129.187.19.183

*** dns1.lrz.de can't find mail.yahoo.com: Query refused
PS C:\Users\gorke> nslookup -query=mx mail.yahoo.com dns2.lrz.bayern
Server:  dns2.lrz.de
Address:  141.40.9.211

*** dns2.lrz.de can't find mail.yahoo.com: Query refused
PS C:\Users\gorke> nslookup -query=mx mail.yahoo.com dns3.lrz.eu
Server:  UnKnown
Address:  78.128.211.180

*** UnKnown can't find mail.yahoo.com: Query refused
PS C:\Users\gorke>
```

2. ipconfig

```
PS C:\Users\gorke> ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : anfry
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : hgw.local

Ethernet adapter Ethernet 3:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Fortinet SSL VPN Virtual Ethernet Adapter
   Physical Address. . . . . . . . . : 00-09-0F-AA-00-01
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Ethernet adapter vEthernet (WSL (Hyper-V firewall)):

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Hyper-V Virtual Ethernet Adapter
   Physical Address. . . . . . . . . : 00-15-5D-57-2B-95
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::9c59:7d2c:5d37:7c7b%72(Preferred)
   IPv4 Address. . . . . . . . . . . : 172.30.16.1(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . :
   DHCPv6 IAID . . . . . . . . . . . : 1207965021
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2D-FE-EC-32-00-D8-61-D8-80-06
   NetBIOS over Tcpip. . . . . . . . : Enabled

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : hgw.local
   Description . . . . . . . . . . . : Intel(R) Ethernet Connection (7) I219-V
   Physical Address. . . . . . . . . : 00-D8-61-D8-80-06
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::e0b:bc48:fb62:1650%17(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.193(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Wednesday, October 16, 2024 8:35:13 PM
   Lease Expires . . . . . . . . . . : Wednesday, October 16, 2024 10:05:14 PM
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 100718689
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2D-FE-EC-32-00-D8-61-D8-80-06
   DNS Servers . . . . . . . . . . . : 8.8.4.4
   NetBIOS over Tcpip. . . . . . . . : Enabled

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
   Physical Address. . . . . . . . . : 4C-1D-96-0B-12-20
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
   Physical Address. . . . . . . . . : 4E-1D-96-0B-12-1F
   DHCP Enabled. . . . . . . . . . . : Yes
```

Figure 15: ipconfig /all

```
PS C:\Users\gorke>
PS C:\Users\gorke> ipconfig /displaydns

Windows IP Configuration

    ns1.mythic-beasts.com
    ----------------------------------------
    Record Name . . . . . : ns1.mythic-beasts.com
    Record Type . . . . . : 1
    Time To Live  . . . . : 1122
    Data Length . . . . . : 4
    Section . . . . . : Answer
    A (Host) Record . . . : 45.33.127.156


    crl3.digicert.com
    ----------------------------------------
    Record Name . . . . . : crl3.digicert.com
    Record Type . . . . . : 5
    Time To Live  . . . . : 428
    Data Length . . . . . : 8
    Section . . . . . : Answer
    CNAME Record  . . . . : crl.edge.digicert.com


    Record Name . . . . . : crl.edge.digicert.com
    Record Type . . . . . : 5
    Time To Live  . . . . : 428
    Data Length . . . . . : 8
    Section . . . . . : Answer
    CNAME Record  . . . . : fp2e7a.wpc.2be4.phicdn.net


    Record Name . . . . . : fp2e7a.wpc.2be4.phicdn.net
    Record Type . . . . . : 5
    Time To Live  . . . . : 428
    Data Length . . . . . : 8
    Section . . . . . : Answer
    CNAME Record  . . . . : fp2e7a.wpc.phicdn.net


    Record Name . . . . . : fp2e7a.wpc.phicdn.net
    Record Type . . . . . : 1
    Time To Live  . . . . : 428
    Data Length . . . . . : 4
    Section . . . . . : Answer
    A (Host) Record . . . : 192.229.221.95


    dns2.lrz.bayern
    ----------------------------------------
    Record Name . . . . . : dns2.lrz.bayern
    Record Type . . . . . : 1
    Time To Live  . . . . : 15419
    Data Length . . . . . : 4
    Section . . . . . : Answer
    A (Host) Record . . . : 141.40.9.211


    dns1.lrz.de
    ----------------------------------------
    Record Name . . . . . : dns1.lrz.de
    Record Type . . . . . : 1
    Time To Live  . . . . : 20481
    Data Length . . . . . : 4
    Section . . . . . : Answer
    A (Host) Record . . . : 129.187.19.183


    kubernetes.docker.internal
    ----------------------------------------
```

Figure 16: ipconfig /displaydns

```
PS C:\Users\gorke> ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.
```

Figure 17: ipconfig /flushdns

3. Tracing DNS with Wireshark

I switched to my laptop.

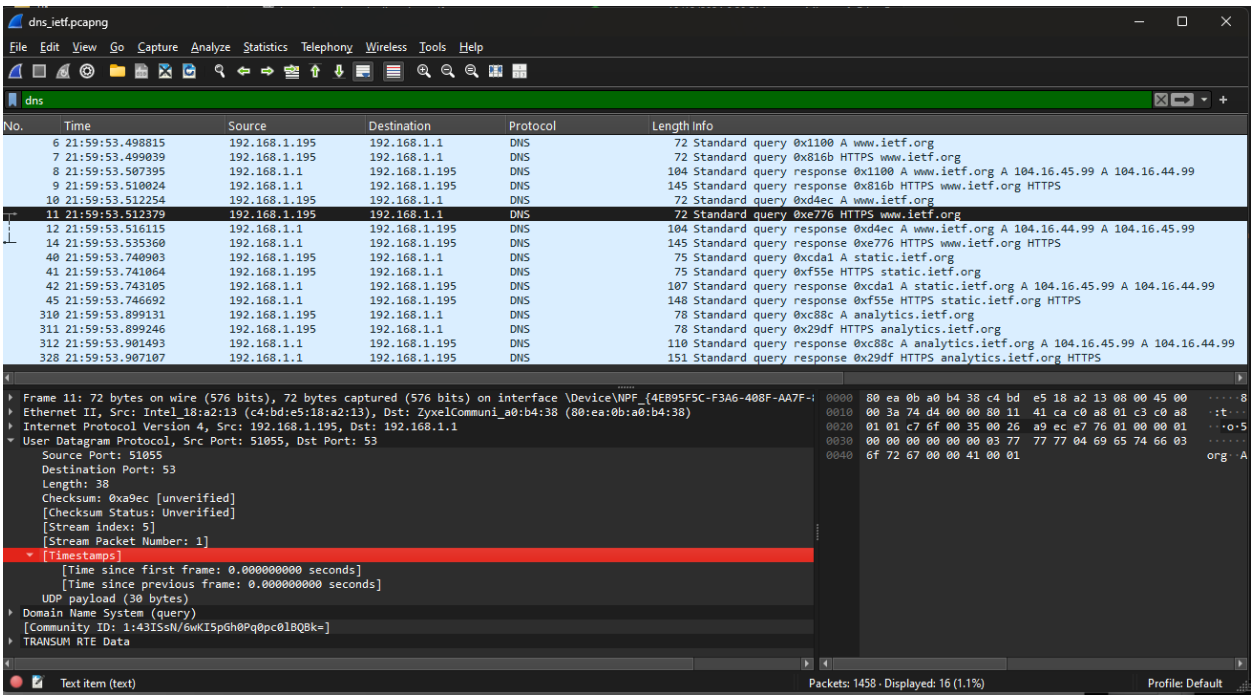


Figure 18: DNS query for ietf

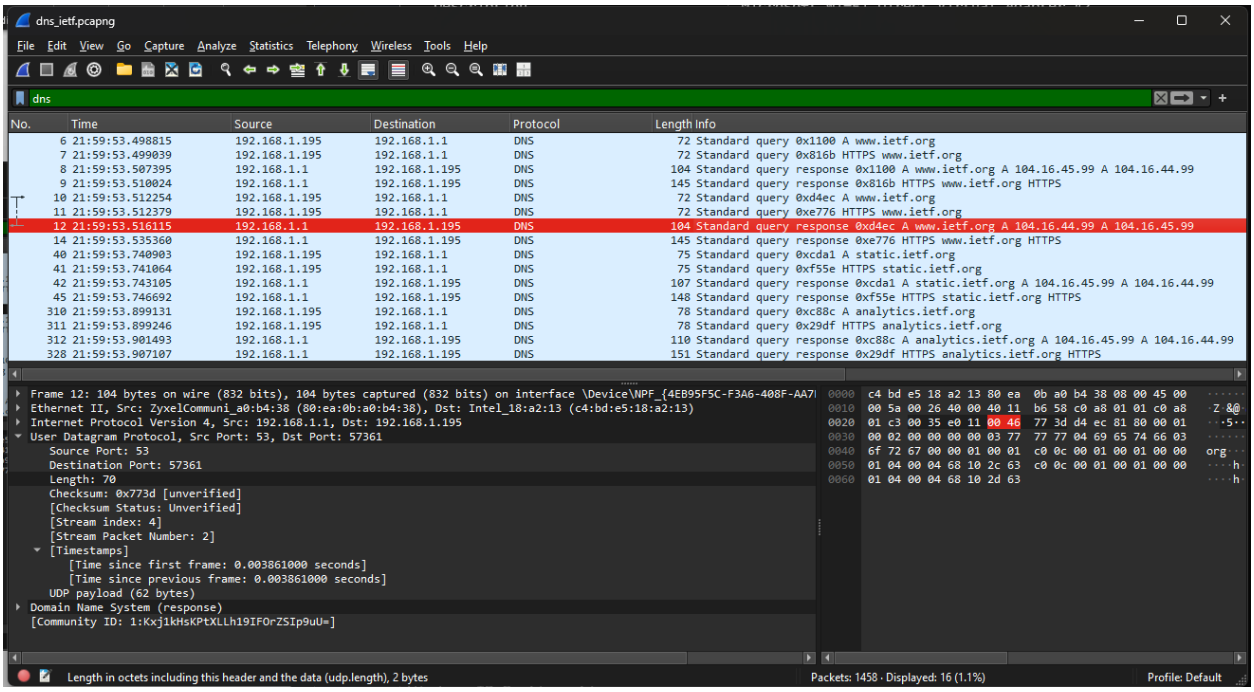
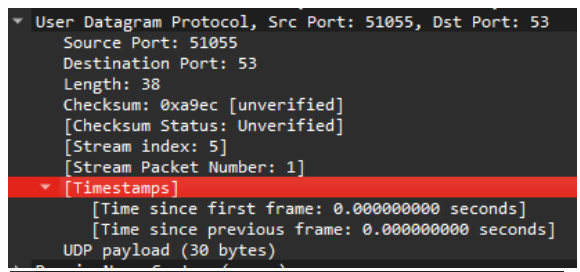


Figure 19: DNS response for ietf

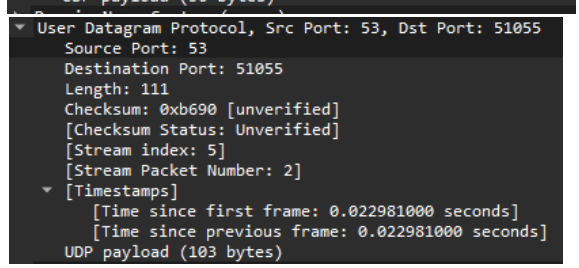
4. Locate the DNS query and response messages. Are they sent over UDP or TCP?

UDP



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

Both 53

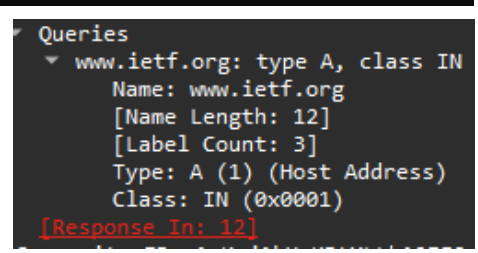


6. To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?

They are the same 192.168.1.1

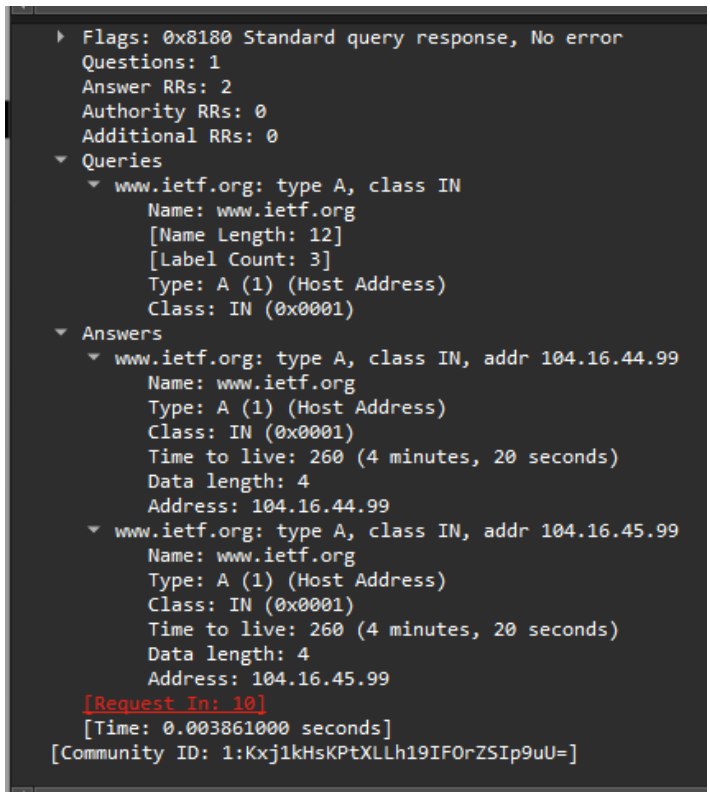
7. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?

A type A query. However, it does not contain any answers.



8. Examine the DNS response message. How many “answers” are provided? What does each of these answers contain?

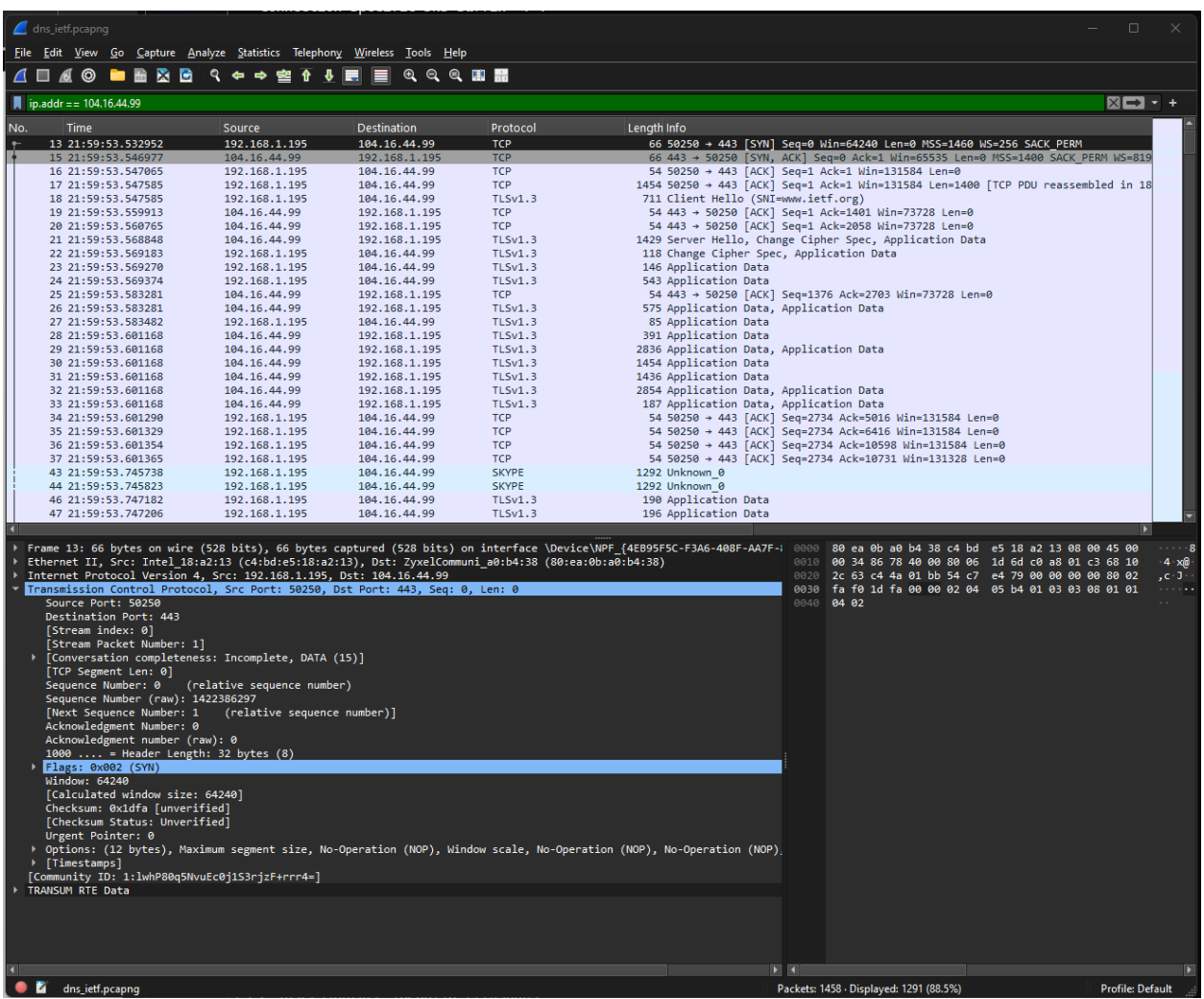
2. These include name, type, class, TTL, data length, and address information.



```
▸ Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 2
  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 (1) (Host Address)
      Class: IN (0x0001)
▾ Answers
  ▾ www.ietf.org: type A, class IN, addr 104.16.44.99
      Name: www.ietf.org
      Type: A (1) (Host Address)
      Class: IN (0x0001)
      Time to live: 260 (4 minutes, 20 seconds)
      Data length: 4
      Address: 104.16.44.99
  ▾ www.ietf.org: type A, class IN, addr 104.16.45.99
      Name: www.ietf.org
      Type: A (1) (Host Address)
      Class: IN (0x0001)
      Time to live: 260 (4 minutes, 20 seconds)
      Data length: 4
      Address: 104.16.45.99
  [Request In: 10]
  [Time: 0.003861000 seconds]
[Community ID: 1:Kxj1kHsKPtXLLh19IFOrZSIp9uU=]
```

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?

Yes, the TCP SYN packets are sent to 104.16.45.99, which is one of the provided answers from the DNS response message. You can check the image below.



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

There is no need for extra DNS requests since all the images are loaded from www.ietf.org, and the host uses a cached address.

```
PS C:\Users\gorke> nslookup www.mit.edu
Server:  HGW.HGW.LOCAL
Address:  192.168.1.1

Non-authoritative answer:
Name:    e9566.dscb.akamaiedge.net
Address:  104.66.66.27
Aliases:  www.mit.edu
          www.mit.edu.edgekey.net

PS C:\Users\gorke>
```

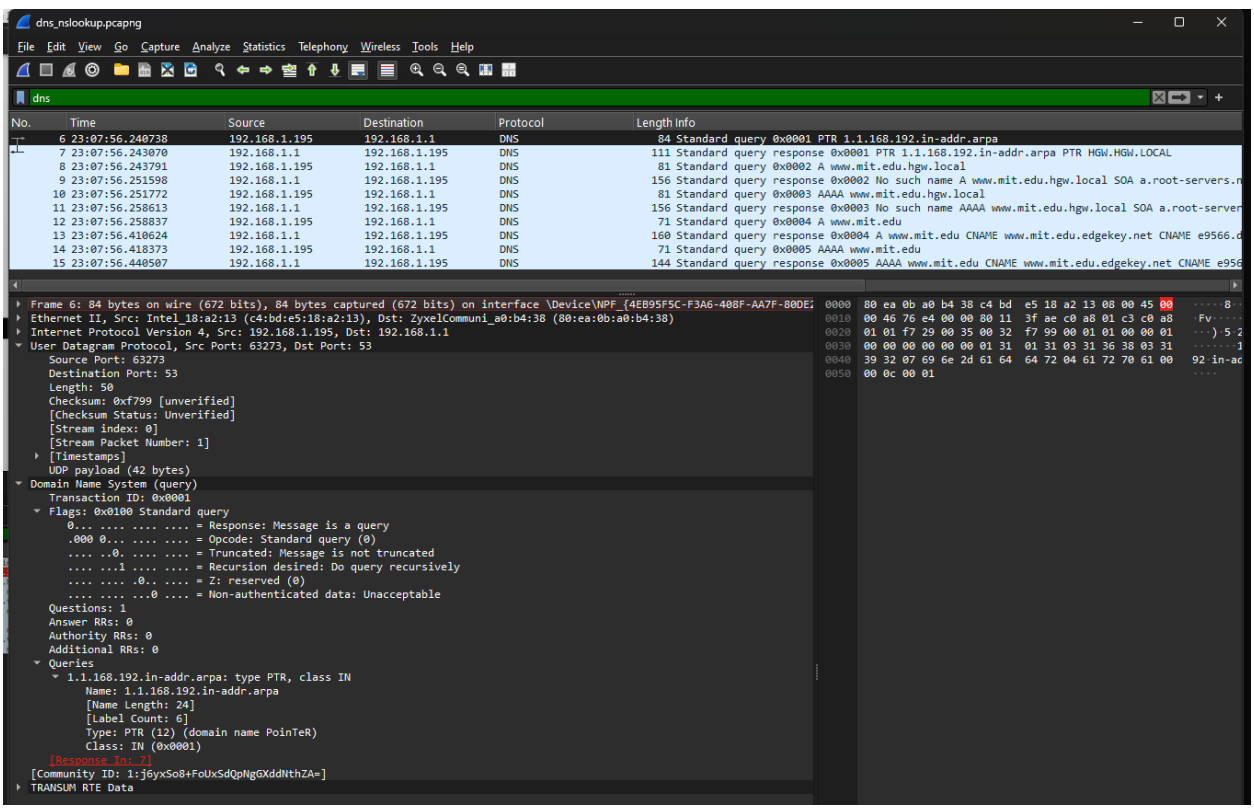


Figure 20: nslookup mit query

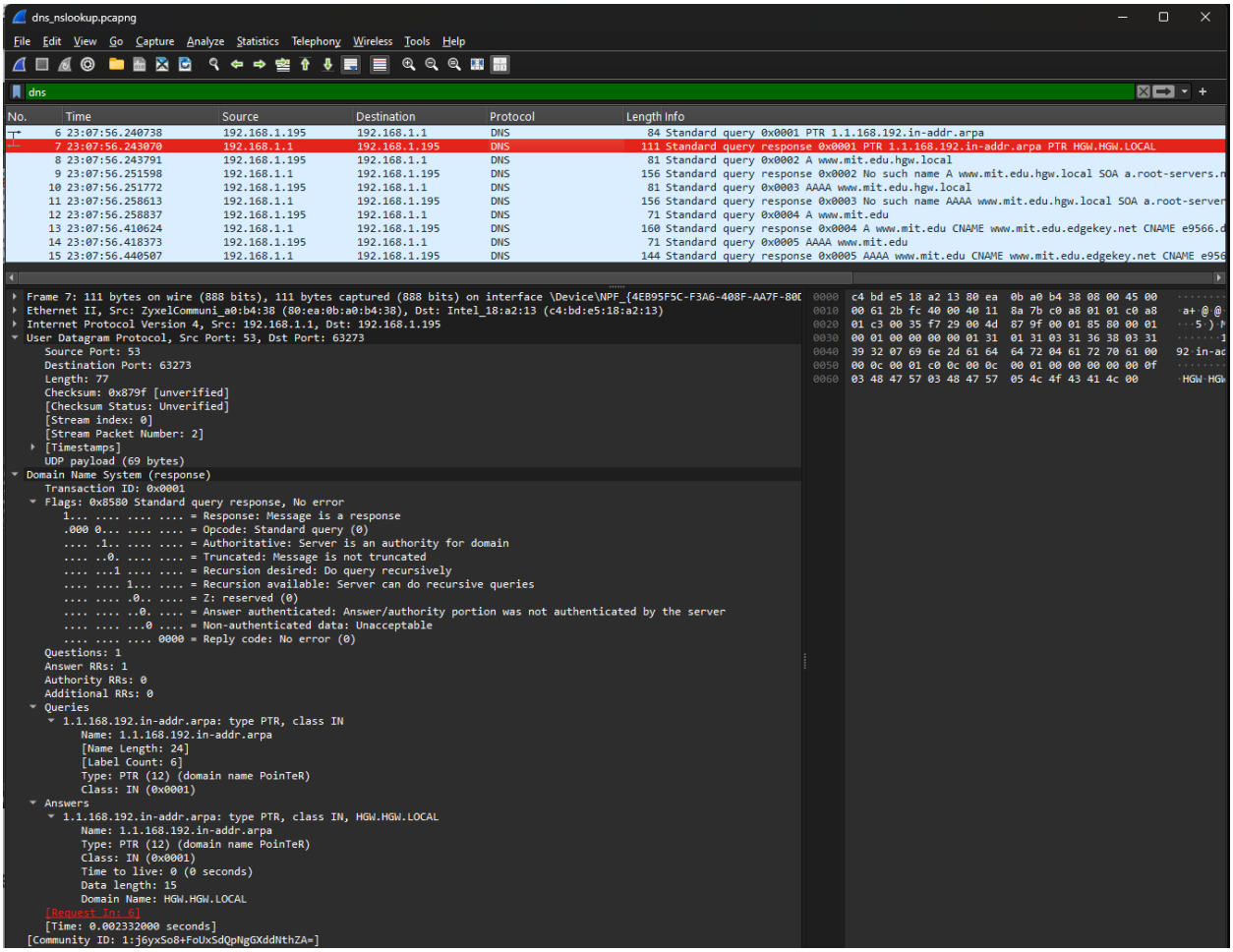


Figure 21: nslookup mit response

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

As seen in figures 20 and 21, both are 53.

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

The query is sent to the IP address 192.168.1.1, which corresponds to my default local DNS server.

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

The query is classified as an A type. It does not contain any answers.

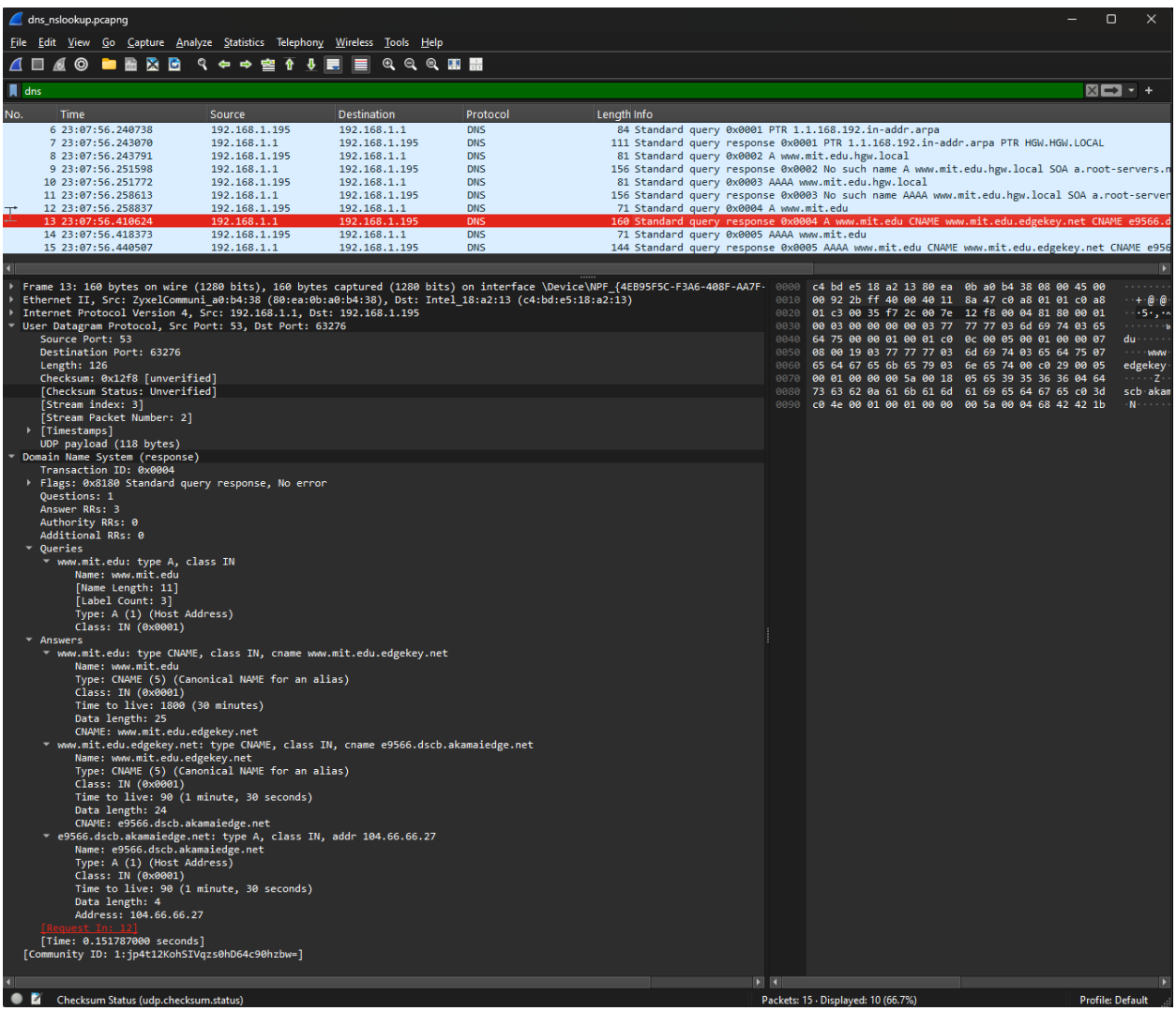
```
Queries
  www.mit.edu: type A, class IN
      Name: www.mit.edu
      [Name Length: 11]
      [Label Count: 3]
      Type: A (1) (Host Address)
      Class: IN (0x0001)
[Response In: 13]
```

14. Examine the DNS response message. How many “answers” are provided? What does each of these answers contain?

There are 3 answers. These include name, type, class, TTL, data length and cname or address information.

```
Answers
  www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
      Name: www.mit.edu
      Type: CNAME (5) (Canonical NAME for an alias)
      Class: IN (0x0001)
      Time to live: 1800 (30 minutes)
      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 (5) (Canonical NAME for an alias)
      Class: IN (0x0001)
      Time to live: 90 (1 minute, 30 seconds)
      Data length: 24
      CNAME: e9566.dscb.akamaiedge.net
  e9566.dscb.akamaiedge.net: type A, class IN, addr 104.66.66.27
      Name: e9566.dscb.akamaiedge.net
      Type: A (1) (Host Address)
      Class: IN (0x0001)
      Time to live: 90 (1 minute, 30 seconds)
      Data length: 4
      Address: 104.66.66.27
[Request In: 12]
```

15. Provide a screenshot.

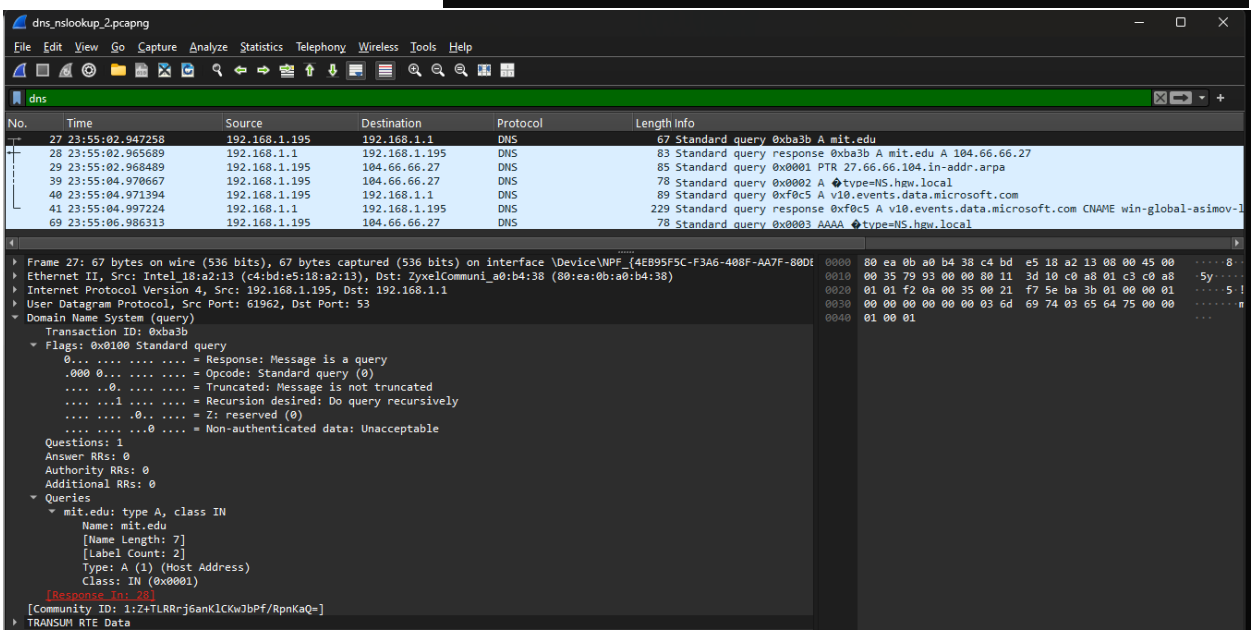


16. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

The query is sent to the IP address 192.168.1.1, which is my default local DNS server.

```
PS C:\Users\gorke> nslookup -type=NS mit.edu
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  104.66.66.27

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** Request to UnKnown timed-out
PS C:\Users\gorke>
```



17. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?

The query is an NS type query. The query does not contain any answer.

```
002 A type=NS.hgw.
003 AAAA type=NS.h
```

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 name servers?

It does not include any name servers, but it does contain the IP address of mit.edu's A record (104.66.66.27).

```
Domain Name System (response)
    Transaction ID: 0xba3b
    Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
    Queries
        mit.edu: type A, class IN
            Name: mit.edu
            [Name Length: 7]
            [Label Count: 2]
            Type: A (1) (Host Address)
            Class: IN (0x0001)
    Answers
    [Request In: 27]
    [Time: 0.018431000 seconds]
[Community ID: 1:Z+TLRRrj6anKlCKwJbPf/RpnKaQ=]
```

```
onse 0xba3b A mit.edu A 104.66.66.27
01 PTR 27.66.66.104.in-addr.arpa
```

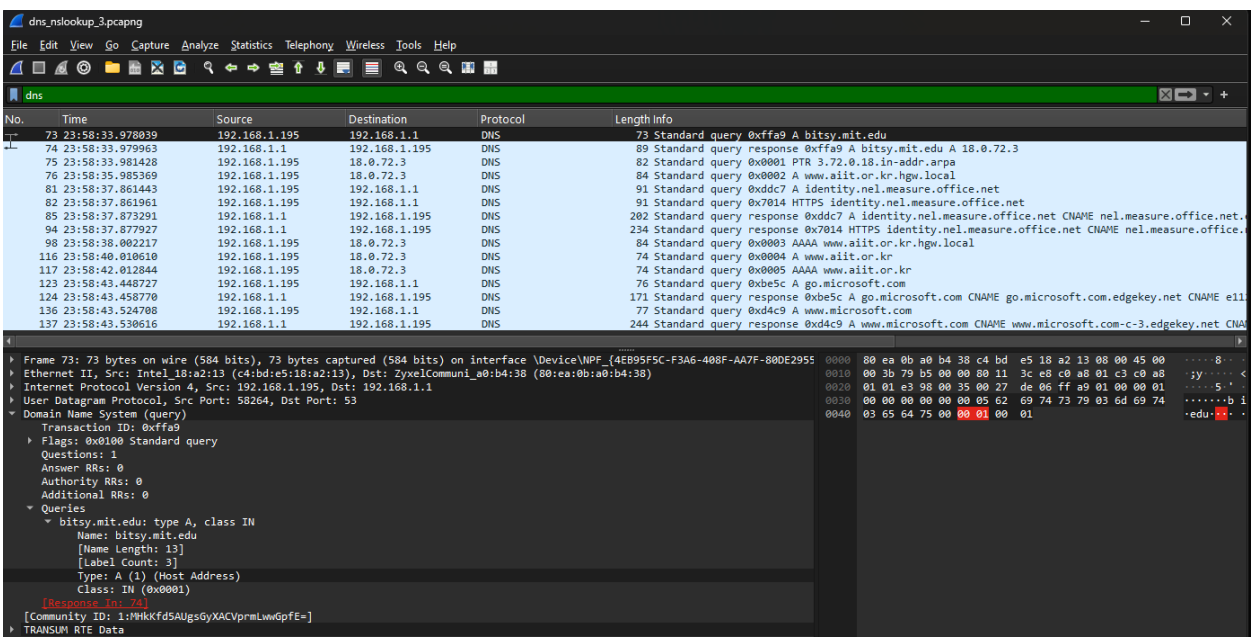
19. Provide a screenshot.

```
*** Request to UnKnown timed-out
PS C:\Users\gorke> nslookup www.aiit.or.kr bitsy.mit.edu
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  18.0.72.3

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** Request to UnKnown timed-out
PS C:\Users\gorke>
```

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?

The request is made to bitsy.mit.edu, which is located at 18.72.0.3.



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

It is a Standard Query of type. It does not contain any answers.

```
Domain Name System (query)
    Transaction ID: 0xffa9
  ▸ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
    ▾ bitsy.mit.edu: type A, class IN
        Name: bitsy.mit.edu
        [Name Length: 13]
        [Label Count: 3]
        Type: A (1) (Host Address)
        Class: IN (0x0001)
    [Response In: 74]
[Community ID: 1:MHkKfd5AUgsGyXACVprmLwwGpfE=]
▸ TRANSUM RTE Data
```

22. Examine the DNS response message. How many “answers” are provided? What does each of these answers contain?

The DNS response message provides a single solution, which includes the following details: the domain name is bitsy.mit.edu, with a type A record, class IN, and an address of 18.0.72.3. The record is classified as a host address (type A) with a class of IN (0x0001). The time to live (TTL) is set to 1315 seconds, and the data length is 4 bytes, representing the IP address 18.0.72.3.

```
▾ Domain Name System (response)
    Transaction ID: 0xffa9
  ▸ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
    ▾ bitsy.mit.edu: type A, class IN
        Name: bitsy.mit.edu
        [Name Length: 13]
        [Label Count: 3]
        Type: A (1) (Host Address)
        Class: IN (0x0001)
  ▾ Answers
    ▾ bitsy.mit.edu: type A, class IN, addr 18.0.72.3
        Name: bitsy.mit.edu
        Type: A (1) (Host Address)
        Class: IN (0x0001)
        Time to live: 1315 (21 minutes, 55 seconds)
        Data length: 4
        Address: 18.0.72.3
    [Request In: 73]
    [Time: 0.001924000 seconds]
[Community ID: 1:MHkKfd5AUgsGyXACVprmLwwGpfE=]
```

23. Provide a screenshot.