

CS 421 Wireshark Assignment

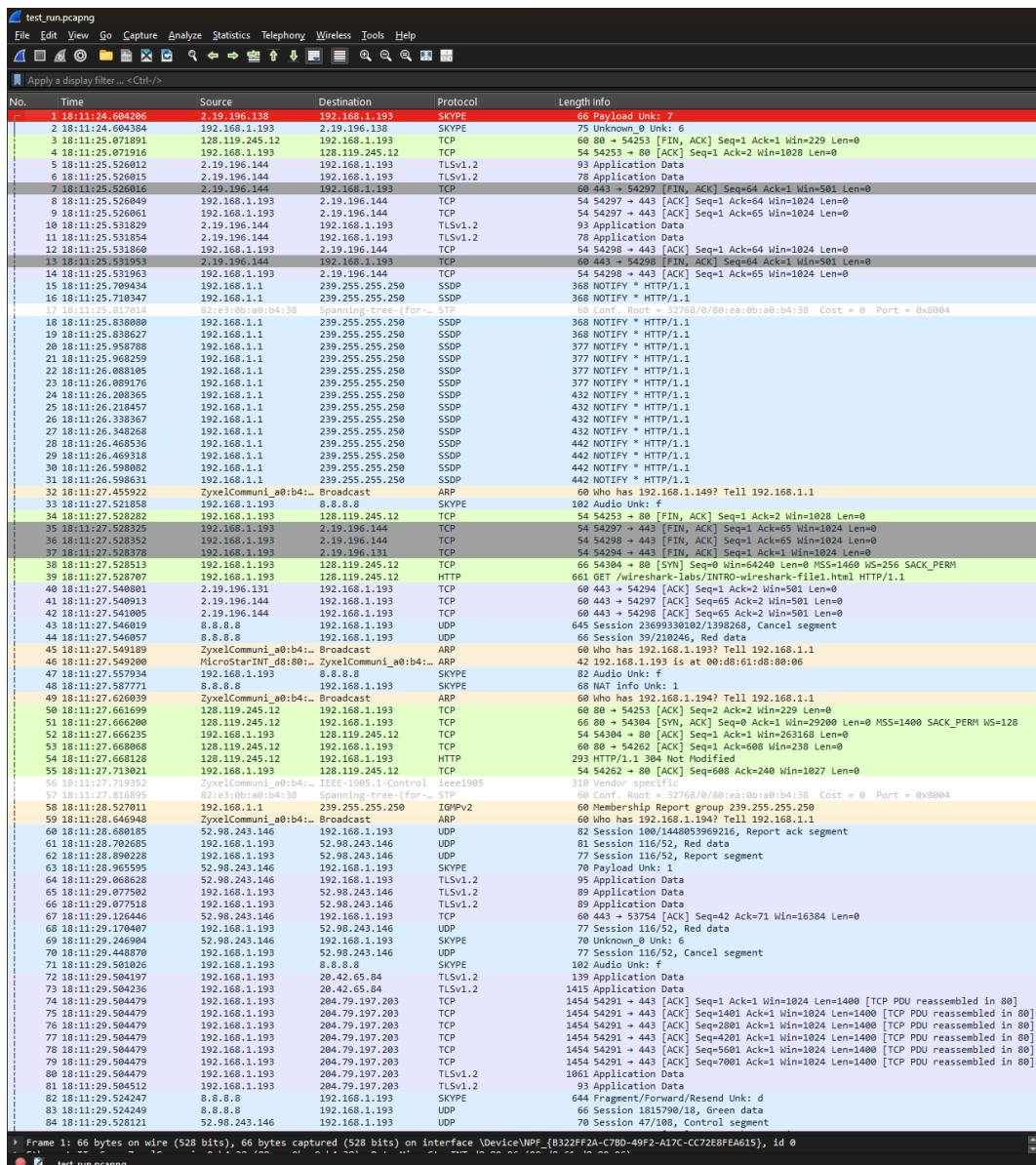
Görkem Kadir Solun 22003214

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	18:11:25.071939	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	18:11:25.819814	02:01:00:00:b4:38	Spanning-tree (for-...	STP	60	Conf. Root = 32768/0/80:ea:0b:a0:b4:38 Cost = 0 Port = 0x0004
18	18:11:25.838008	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	18:11:26.000105	192.168.1.1	239.255.255.250	SSDP	377	NOTIFY * HTTP/1.1
23	18:11:26.009176	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	18:11:26.340268	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	18:11:26.598802	192.168.1.1	239.255.255.250	SSDP	442	NOTIFY * HTTP/1.1
31	18:11:26.598831	192.168.1.1	239.255.255.250	SSDP	442	NOTIFY * HTTP/1.1
32	18:11:27.455922	ZyxelCommuni_00:b4:38	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	18:11:27.540091	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	65	Session 39/210246, Red data
45	18:11:27.549109	ZyxelCommuni_00:b4:38	Broadcast	ARP	60	Who has 192.168.1.193? Tell 192.168.1.1
46	18:11:27.549200	MicroStarINT_d8:00:00	ZyxelCommuni_00:b4:38	ARP	42	192.168.1.193 is at 00:d8:00:00:00:00
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	18:11:27.626030	ZyxelCommuni_00:b4:38	Broadcast	ARP	60	Who has 192.168.1.194? Tell 192.168.1.1
50	18:11:27.666199	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	60	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	18:11:27.668060	128.119.245.12	192.168.1.193	TCP	60	80 → 54262 [ACK] Seq=1 Ack=600 Win=230 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	18:11:27.713952	ZyxelCommuni_00:b4:38	IEEE1905.1-Control	IEEE1905	310	Vendor specific
57	18:11:27.810095	02:01:00:00:b4:38	Spanning-tree (for-...	STP	60	Conf. Root = 32768/0/80:ea:0b:a0:b4:38 Cost = 0 Port = 0x0004
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_00:b4:38	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	18:11:28.955595	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?

My computer: 192.169.1.193

gaia.cs.umass.edu: 128.119.245.12

```
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
```

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.

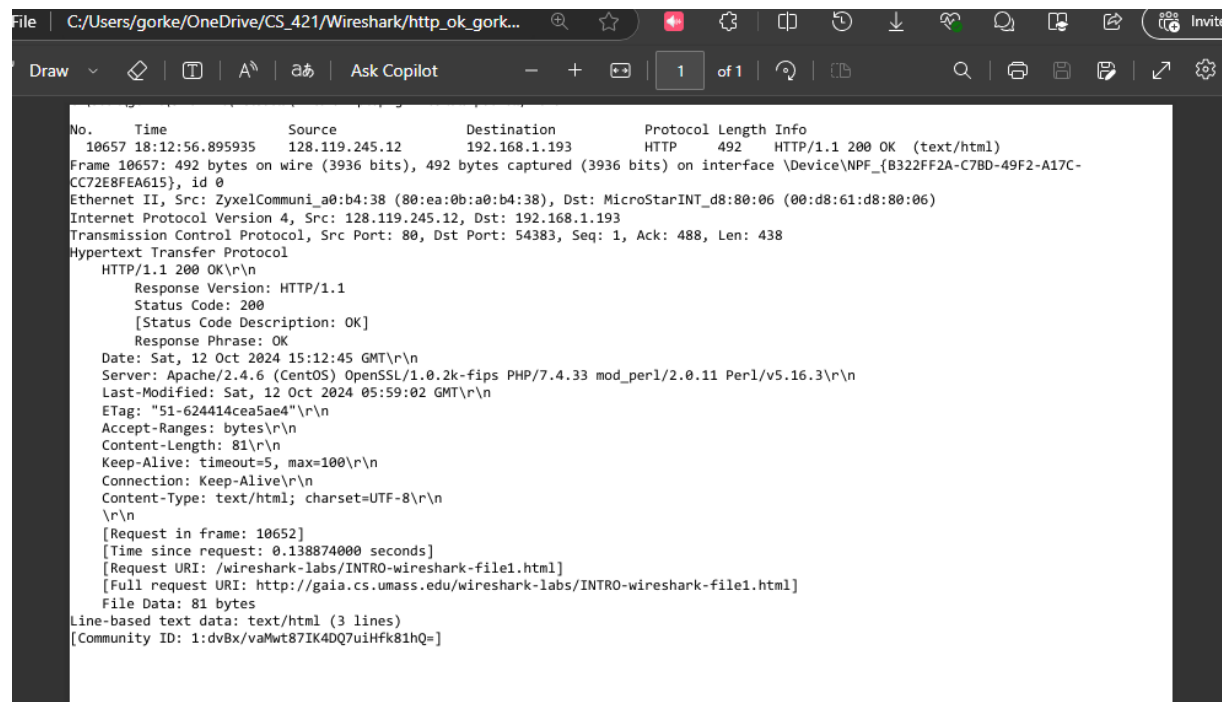


Figure 2: Print of HTTP OK

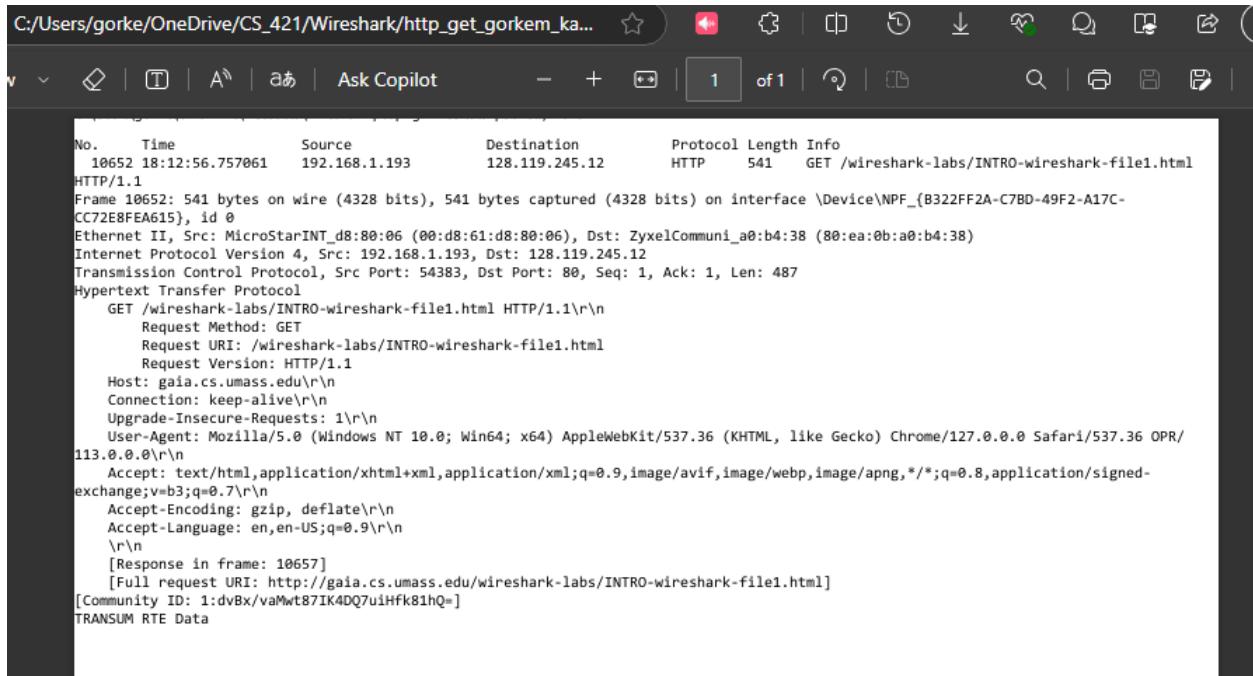


Figure 3: Print of HTTP OK

Wireshark Lab: HTTP

1. The Basic HTTP GET/response interaction

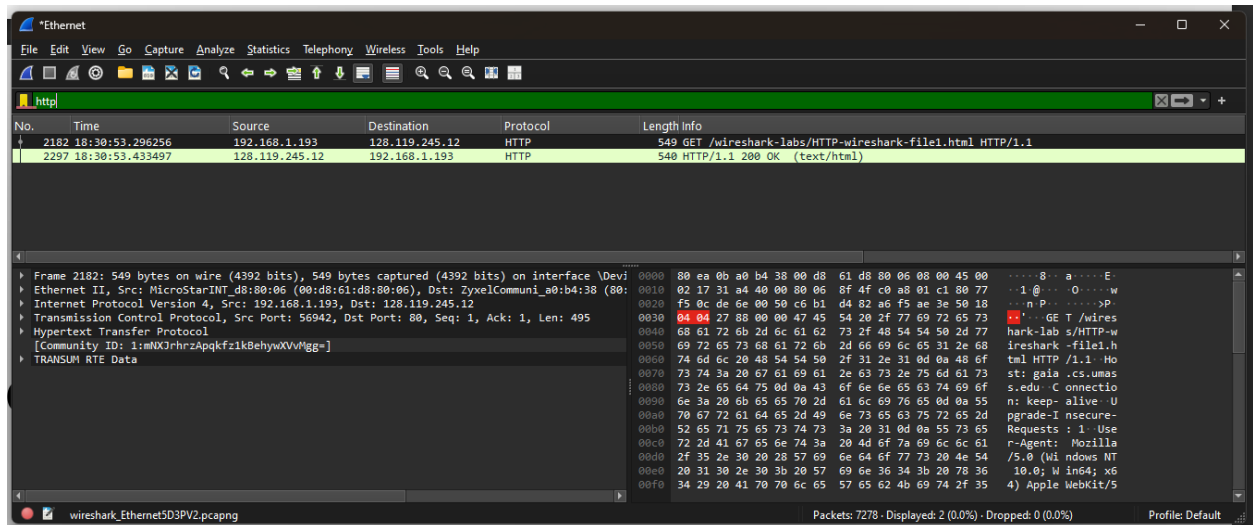


Figure 4: Downloaded the first HTML file

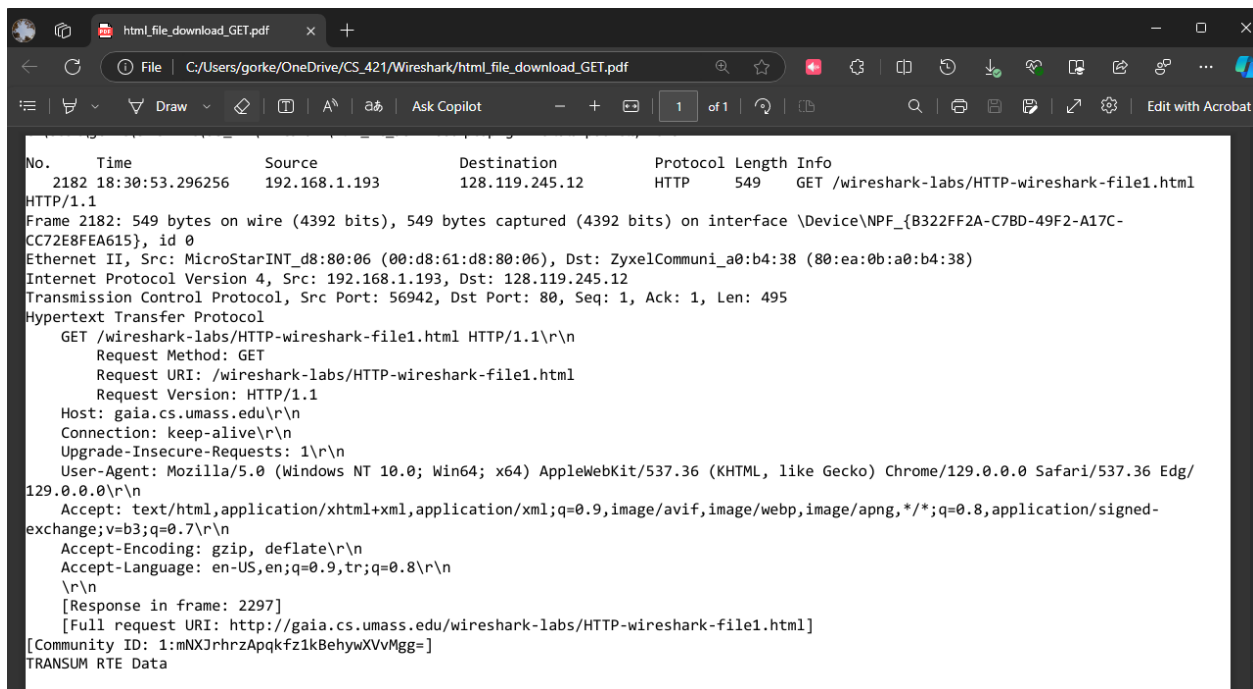


Figure 5: HTML file download GET

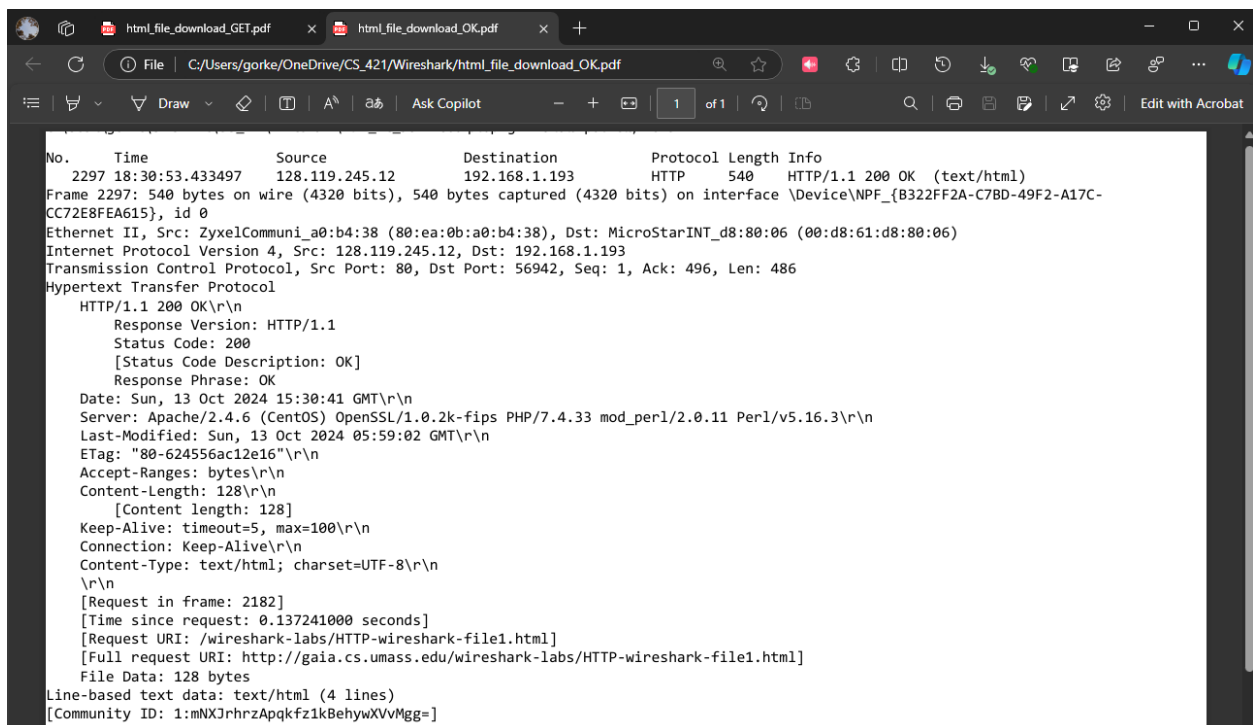


Figure 6: HTML file download OK

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\nETag: "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\nContent-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

The image shows a Wireshark packet capture of an HTTP transaction. The packet list on the left shows a GET request (No. 1201) and its corresponding 304 Not Modified response (No. 1202). The packet details pane for packet 1202 shows the response status and headers. The packet bytes pane shows the raw data of the response.

```
not_modified.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

No. Time Source Destination Protocol Length Info
1201 19:52:59.297484 128.119.245.12 192.168.1.193 HTTP 293 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
1202 19:52:59.745756 128.119.245.12 192.168.1.193 HTTP 293 HTTP/1.1 304 Not Modified

Frame 1201: 293 bytes on wire (2344 bits), 293 bytes captured (2344 bits) on interface \Device\NPF... [0322F2A-C7B0-49F2-A17C-CC72EBFEA615], id 0
Ethernet II, Src: ZyxelCommuni... [08:00:00:00:00:00], Dst: MicroStarINT... [00:0d:61:d8:00:00]
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.193
Transmission Control Protocol, Src Port: 80, Dst Port: 53167, Seq: 241, Ack: 1215, Len: 239
Hypertext Transfer Protocol
  GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
    Request Method: GET
    Request URI: /wireshark-labs/HTTP-wireshark-file2.html
    Request Version: HTTP/1.1
    Status Code: 304
    [Status Code Description: Not Modified]
    Response Phrase: Not Modified
    Date: Mon, 14 Oct 2024 16:52:43 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
    Connection: Keep-Alive
    Keep-Alive: timeout=5, max=99
    ETag: "173-6246988db937"
    \n\n
    [Request in frame: 1195]
    [Time since request: 0.127320000 seconds]
    [Request URI: /wireshark-labs/HTTP-wireshark-file2.html]
    [Link request: /wireshark-labs/HTTP-wireshark-file2.html]
    [Community ID: 1:aTCVstGTBMK+DN]oemfC6AA2C8o=
```

Figure 7: Not modified

The image shows a Wireshark packet capture of an HTTP transaction. The packet list on the left shows a GET request (No. 1201) and its corresponding 304 Not Modified response (No. 1202). The packet details pane for packet 1201 shows the request status and headers. The packet bytes pane shows the raw data of the request.

```
not_modified.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

No. Time Source Destination Protocol Length Info
1201 19:52:59.297484 128.119.245.12 192.168.1.193 HTTP 293 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
1202 19:52:59.745756 128.119.245.12 192.168.1.193 HTTP 293 HTTP/1.1 304 Not Modified

Frame 1201: 293 bytes on wire (2344 bits), 293 bytes captured (2344 bits) on interface \Device\NPF... [0322F2A-C7B0-49F2-A17C-CC72EBFEA615], id 0
Ethernet II, Src: ZyxelCommuni... [08:00:00:00:00:00], Dst: MicroStarINT... [00:0d:61:d8:00:00]
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.193
Transmission Control Protocol, Src Port: 80, Dst Port: 53167, Seq: 241, Ack: 1215, Len: 239
Hypertext Transfer Protocol
  GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
    Request Method: GET
    Request URI: /wireshark-labs/HTTP-wireshark-file2.html
    Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu
    Connection: Keep-Alive
    Cache-Control: max-age=0
    Upgrade-Insecure-Requests: 1
    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
    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
    Accept-Encoding: gzip, deflate
    Accept-Language: en-US,en;q=0.9,tri;q=0.8
    If-None-Match: "173-6246988db937"
    If-Modified-Since: Mon, 14 Oct 2024 05:59:01 GMT
    \n\n
    [Response in frame: 1202]
    [Link request: /wireshark-labs/HTTP-wireshark-file2.html]
    [Community ID: 1:aTCVstGTBMK+DN]oemfC6AA2C8o=
  TRANSMISSION RATE
```

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

No.	Time	Source	Destination	Protocol	Length	Info
193	19:52:45.417850	192.168.1.193	128.119.245.12	HTTP	784	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
221	19:52:45.546891	128.119.245.12	192.168.1.193	HTTP	784	HTTP/1.1 200 OK (text/html)
1164	19:52:58.398570	192.168.1.193	128.119.245.12	HTTP	661	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
1178	19:52:58.539640	128.119.245.12	192.168.1.193	HTTP	294	HTTP/1.1 304 Not Modified
1195	19:52:59.178164	192.168.1.193	128.119.245.12	HTTP	661	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
1201	19:52:59.297484	128.119.245.12	192.168.1.193	HTTP	293	HTTP/1.1 304 Not Modified
1218	19:52:59.745756	192.168.1.193	128.119.245.12	HTTP	661	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
1216	19:52:59.873531	128.119.245.12	192.168.1.193	HTTP	293	HTTP/1.1 304 Not Modified
1233	19:53:00.346282	192.168.1.193	128.119.245.12	HTTP	661	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
1255	19:53:00.473485	128.119.245.12	192.168.1.193	HTTP	293	HTTP/1.1 304 Not Modified

<p>Frame 221: 784 bytes on wire (6272 bits), 784 bytes captured (6272 bits) on interface \Device\NPF{B322FF2A-C78D-49F2-A17C-CC72E8FEA615}, id 0</p> <p>Ethernet II, Src: ZyxelCommuni_00:b4:38 (00:ea:0b:a0:b4:38), Dst: MicroStarINT_d8:80:06 (00:d8:61:d8:80:06)</p> <p>Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.193</p> <p>Transmission Control Protocol, Src Port: 80, Dst Port: 53166, Seq: 1, Ack: 496, Len: 730</p> <p>Hypertext Transfer Protocol</p> <p>GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1</p> <p>Response Version: HTTP/1.1</p> <p>Status Code: 200</p> <p>[Status Code Description: OK]</p> <p>Response Phrase: OK</p> <p>Date: Mon, 14 Oct 2024 16:52:29 GMT</p> <p>Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3</p> <p>Last-Modified: Mon, 14 Oct 2024 05:59:01 GMT</p> <p>Etag: "173-6246588d0937"</p> <p>Accept-Ranges: bytes</p> <p>Content-Length: 371</p> <p>Keep-Alive: timeout=5, max=100</p> <p>Connection: keep-alive</p> <p>Content-Type: text/html; charset=UTF-8</p> <p>[Time since request: 0.129041000 seconds]</p> <p>[Request URI: /wireshark-labs/HTTP-wireshark-file2.html]</p> <p>[Full request URI: http://gala.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]</p> <p>File Data: 371 bytes</p> <p>Line-based text data: text/html (10 lines)</p> <p>[Community ID: 1d:PRRbWkK1x4Uih3HnYBndg97pa=]</p>	<pre> 0000 00 d8 61 d8 80 06 00 ea 0b a0 b4 38 00 00 45 00 a.....B..E 0010 03 02 7b 89 40 00 2c 06 98 7f 80 77 f5 0c c0 a8 { @ , . . . w . . 0020 01 c1 00 50 cf ae 1c 6c 2b e6 a0 fa 72 cf 5b 18 P l e . r . P 0030 00 ed ea 3a 80 00 45 54 54 50 2f 31 2e 31 20 32 4 HT TP/1.1 2 0040 30 30 20 4f 4b 0d 0a 44 61 74 65 3a 20 4d 6f 6e 00 OK D ate: Mon 0050 2c 20 31 34 20 4f 63 74 20 32 30 32 34 20 31 36 14 Oct 2024 16 0060 3a 12 3a 12 39 20 47 4d 54 0d 0a 53 65 72 76 15229 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 0080 20 28 43 65 6e 74 4f 53 29 20 4f 70 65 6e 53 53 (CentOS) OpenS 0090 4c 2f 31 2e 30 2e 32 65 2d 66 69 73 20 58 48 L/1.0.2k-fips PH 0100 50 2f 37 2e 34 2e 33 33 20 6d 6f 64 5f 70 65 72 P/7.4.33 mod_per 0110 6c 2f 32 2e 30 2e 31 31 20 50 65 72 6c 2f 76 35 1/2.0.11 Perl/v 0120 2e 31 36 2e 33 0d 0a 4c 61 73 74 2d 4d 6f 64 69 .16.3 L ast-Modi 0130 66 69 65 64 3a 20 4d 6f 6e 2c 20 31 34 20 4f 63 find: No n, 14 Oc 0140 74 20 32 30 32 34 20 30 35 3a 35 39 3a 30 31 20 T 2024 0 5:59:01 0150 47 4d 54 0d 0a 54 61 67 3a 20 22 31 37 33 32 2d GMT Etag: "173- 0160 36 32 34 26 39 38 38 38 64 62 39 33 37 22 0d 0a 6246588d0937" 0170 41 63 63 65 70 74 2d 52 61 6e 67 65 73 3a 20 62 accept-R anges: b 0180 79 74 65 73 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 ytes C ontent-Le 0190 6e 67 74 68 3a 20 33 37 31 0d 0a 4b 65 65 70 2d ngth: 37 1 keep- 0200 41 6c 69 76 65 3a 20 74 69 6d 65 6f 75 74 3d 35 alive: t imeout=5 0210 2c 20 6d 61 78 3d 31 30 30 0d 0a 43 6f 6e 6e 65 , max=10 0 Conne 0220 63 74 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 ction: K eep-Aliv 0230 65 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 78 65 3a e Conte nt-type: 0240 20 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 text/ht ml; char 0250 73 65 74 3d 55 54 46 2d 38 0d 0a 0d 0a 0a 3c 68 set/UTF- 8 ch 0260 74 6d 6c 3e 0a 0a 43 6f 6e 67 72 74 75 6c 61 61 tml; C ongratula 0270 74 69 6f 6e 70 61 67 61 69 6e 6e 21 20 20 4e 6f tions ag ain! No 0280 77 20 79 6f 75 27 76 65 20 64 6f 77 76 6c 6f 61 w you've downloa 0290 64 65 64 20 74 68 65 20 66 69 6c 65 20 6c 61 62 ded the file lab 0300 2d 32 2e 68 74 6d 6c 2e 20 3c 62 72 3e 0a 54 2 2.html . doc/T 0310 68 69 73 20 66 69 6c 65 27 73 20 6c 61 73 74 20 his file 's last 0320 6d 6f 64 69 66 69 63 61 74 69 6f 6e 20 64 74 74 modifi cation dat 0330 65 20 77 69 6c 6c 20 6e 6f 74 20 63 68 61 6e 67 e will n ot chang </pre>
--	---

Figure 9: Successful file retrieval with an OK response.

No.	Time	Source	Destination	Protocol	Length	Info
193	19:52:45.417850	192.168.1.193	128.119.245.12	HTTP	549	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
221	19:52:45.546891	128.119.245.12	192.168.1.193	HTTP	784	HTTP/1.1 200 OK (text/html)
1164	19:52:58.398570	192.168.1.193	128.119.245.12	HTTP	661	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
1178	19:52:58.539640	128.119.245.12	192.168.1.193	HTTP	294	HTTP/1.1 304 Not Modified
1195	19:52:59.178164	192.168.1.193	128.119.245.12	HTTP	661	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
1201	19:52:59.297484	128.119.245.12	192.168.1.193	HTTP	293	HTTP/1.1 304 Not Modified
1218	19:52:59.745756	192.168.1.193	128.119.245.12	HTTP	661	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
1216	19:52:59.873531	128.119.245.12	192.168.1.193	HTTP	293	HTTP/1.1 304 Not Modified
1233	19:53:00.346282	192.168.1.193	128.119.245.12	HTTP	661	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
1255	19:53:00.473485	128.119.245.12	192.168.1.193	HTTP	293	HTTP/1.1 304 Not Modified

<p>Frame 193: 549 bytes on wire (4392 bits), 549 bytes captured (4392 bits) on interface \Device\NPF{B322FF2A-C78D-49F2-A17C-CC72E8FEA615}, id 0</p> <p>Ethernet II, Src: MicroStarINT_d8:80:06 (00:d8:61:d8:80:06), Dst: ZyxelCommuni_00:b4:38 (00:ea:0b:a0:b4:38)</p> <p>Internet Protocol Version 4, Src: 192.168.1.193, Dst: 128.119.245.12</p> <p>Transmission Control Protocol, Src Port: 80, Dst Port: 53166, Seq: 1, Len: 495</p> <p>Hypertext Transfer Protocol</p> <p>GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1</p> <p>Request Method: GET</p> <p>Request URI: /wireshark-labs/HTTP-wireshark-file2.html</p> <p>Request Version: HTTP/1.1</p> <p>Host: gala.cs.umass.edu</p> <p>Connection: keep-alive</p> <p>Upgrade-Insecure-Requests: 1</p> <p>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</p> <p>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</p> <p>Accept-encoding: gzip, deflate</p> <p>Accept-Language: en-US,en;q=0.9,tri;q=0.8</p> <p>[Time since request: 0.129041000 seconds]</p> <p>[Full request URI: http://gala.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]</p> <p>[Community ID: 1d:PRRbWkK1x4Uih3HnYBndg97pa=]</p> <p>TRANSMISSION DATA</p>	<pre> 0000 80 ea 0b a0 b4 38 00 d8 61 d8 80 06 00 00 45 00 B.....w 0010 02 17 2e ec 40 00 80 06 92 07 c0 a0 01 c1 80 77 p l e . r . P 0020 f5 0c cf ae 00 50 a0 fa 70 e0 1c 6c 2b e6 50 18 GET /wireshark-labs/HTTP-w 0030 04 04 c8 82 00 00 47 45 54 50 2f 31 2e 31 20 32 ark-lab s/HTTP-w 0040 68 61 72 6b 2d 6c 61 62 73 2f 48 54 50 2d 7f ireshark -file2.h 0050 69 72 65 73 68 61 72 6b 2d 66 69 6c 65 32 2e 68 tml HTTP/1.1 20 0060 74 6d 6c 20 48 54 50 2f 31 2e 31 0d 0a 4b 65 6f 73 0070 73 74 3a 20 6f 61 69 61 2e 63 73 2e 75 6d 61 73 t: gala.cs.umass 0080 73 2e 65 64 75 0d 0a 43 6f 6e 6e 65 63 74 69 6f s,educat ion 0090 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 55 n keep-alive: U 0100 70 67 72 61 64 65 2d 49 6e 73 65 63 75 72 65 2d pgrade-I nsecure- 0110 52 65 61 75 65 73 74 73 3a 20 31 0d 0a 55 73 65 Requests: 1 Use 0120 72 2d 41 67 65 6e 74 3a 20 4d 6f 74 69 6c 6e 61 r-Agent: Mozilla 0130 2f 35 2e 30 28 5f 69 6e 64 6f 77 73 20 4e 54 /5.0 (W indows NT 0140 20 31 38 2e 30 3b 20 57 60 6e 30 3a 3b 20 78 36 10.0; W ind; x6 0150 34 29 20 41 70 70 6c 65 57 65 62 4b 69 74 2f 35 4) Apple WebKit/5 0160 33 37 2e 33 36 20 2b 4b 48 54 4d 4c 2c 20 6c 69 37.36 (K HTML, li 0170 6b 65 20 47 65 63 6b 6f 29 20 4b 68 72 6f 6d 65 ke Gecko) Chrome 0180 2f 31 32 39 2a 30 2e 30 2e 30 20 53 61 61 66 72 /129.0.0 Safari 0190 69 2f 35 33 37 2e 33 36 20 45 64 6f 2f 31 32 39 i/537.36 Edg/129 0200 2e 28 2e 30 2e 28 0d 61 6c 63 63 6e 70 74 3a 20 .0.0 Accept: 0210 6e 65 64 2d 65 78 61 68 61 6e 67 65 30 7b 3d 62 text/ht ml; applic 0220 33 3b 71 3d 30 2e 37 0d 0a 41 63 65 70 74 2d 3 3;q=0.7 0230 45 6e 63 6f 64 69 6e 67 3a 20 6f 74 69 70 7c 20 Encoding: gzip, 0240 64 65 6c 61 74 65 0d 0a 41 63 65 70 74 2d 3a 20 deflate Acc 0250 4c 61 67 61 67 65 3a 20 65 6e 2d 55 53 2c 20 Language : en-US, 0260 65 6e 3b 71 3d 30 2e 39 2c 74 72 3b 71 3d 30 2e en;q=0.9 ,tri;q=0 </pre>
--	---

Figure 10: The first GET request of the file.

```

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)

```

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

File Data: 371 bytes

- Line-based text data: text/html (10 lines)

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

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

The image shows a Wireshark capture of an HTTP GET request. The packet list at the top shows two packets: packet 906 (a GET request) and packet 921 (the response). The packet details pane for packet 906 shows the request structure, including the method (GET), URI, version, host, and various headers. The packet bytes pane shows the raw data of the request, with the GET line highlighted in red. The response packet (921) is also visible in the packet list, showing a 200 OK status and a text/html content type.

No.	Time	Source	Destination	Protocol	Length	Info
906	20:51:43.895189	192.168.1.193	128.119.245.12	HTTP	549	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
921	20:51:44.028168	128.119.245.12	192.168.1.193	HTTP	715	HTTP/1.1 200 OK (text/html)

Frame 906: 549 bytes on wire (4392 bits), 549 bytes captured (4392 bits) on interface \Device\NPF{B32...}

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: 55331, Dst Port: 80, Seq: 1, Ack: 1, Len: 495

Hypertext Transfer Protocol

- GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\n
 - Request Method: GET
 - Request URI: /wireshark-labs/HTTP-wireshark-file3.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... \r\n
 - Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;... \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: 921]

[Full request URI: <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html>]

[Community ID: 1:vGvNUngsw/w24VStEPXNE1x+d4=]

TRANSUM RTE Data

Figure 11: GET request for the long file.

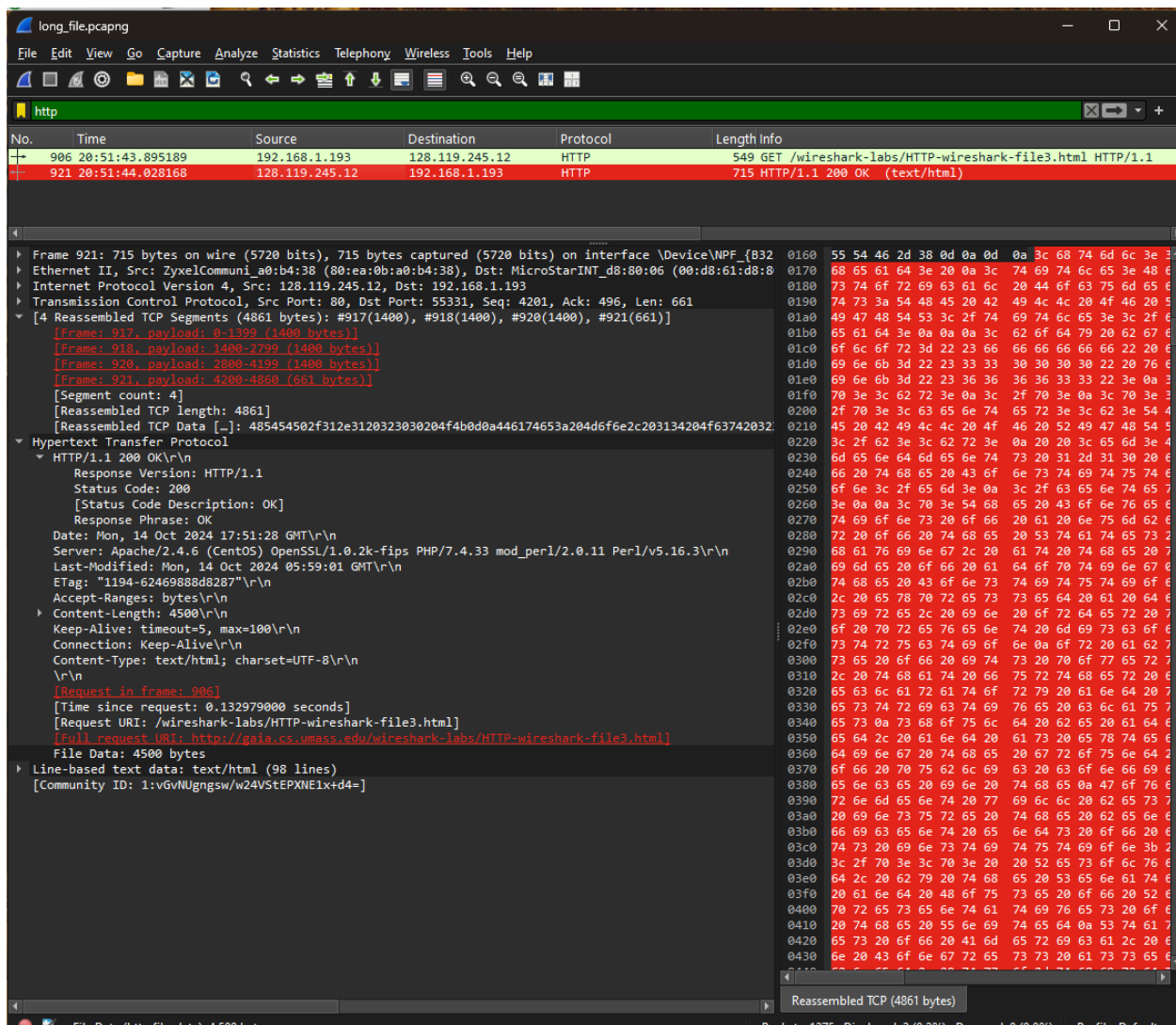


Figure 12: Retrieved long file

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.

Time	Source	Destination	Protocol	Length	Info
906 20:51:43.895189	192.168.1.193	128.119.245.12	HTTP	549	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
921 20:51:44.028168	128.119.245.12	192.168.1.193	HTTP	715	HTTP/1.1 200 OK (text/html)

Transmission Control Protocol, Src Port: 80, Dst Port: 55331, Seq: 4201, Ack: 496, Len: 661
[4 Reassembled TCP Segments (4861 bytes): #917(1400), #918(1400), #920(1400), #921(661)]
[Frame: 917, payload: 0-1399 (1400 bytes)]
[Frame: 918, payload: 1400-2799 (1400 bytes)]
[Frame: 920, payload: 2800-4199 (1400 bytes)]
[Frame: 921, payload: 4200-4860 (661 bytes)]
[Segment count: 4]
[Reassembled TCP length: 4861]
[Reassembled TCP Data [...]: 485454502f312e3120323030204f4b0d0a446174653a204d6f6e2c203134204f63742032:

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

200 OK.

```
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: Mon, 14 Oct 2024 17:51:28
```

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

The image shows a Wireshark packet capture window titled 'image_http_get.pcapng'. The top pane displays a list of captured packets. The selected packet is packet 9, which is an HTTP GET request from 192.168.1.193 to 128.119.245.12. The packet details pane shows the following information:

- Frame 9: 549 bytes on wire (4392 bits), 549 bytes captured (4392 bits) on interface \Device\NPF_{B322FF2F-...}
- 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: 65313, Dst Port: 80, Seq: 1, Ack: 1, Len: 495
- Hypertext Transfer Protocol
 - GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1\r\n
 - Request Method: GET
 - Request URI: /wireshark-labs/HTTP-wireshark-file4.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/120.0.6322.59 Safari/537.36\r\n
 - Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8\r\n
 - Accept-Encoding: gzip, deflate\r\n
 - Accept-Language: en-US,en;q=0.9,fr;q=0.8\r\n
 - [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html]
 - [Community ID: 1:W8tw9WCP1Sxr+Lg6b519EnAycyI=]
- TRANSMISSION DATA

The packet bytes pane shows the raw data of the request, including the status line 'HTTP/1.1 200 OK' and the response phrase 'OK'.

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?

```
\r\n
[Response in frame: 101]
[Full request URI: http://gaia.cs.umass.edu/pearson.png]
[Community ID: 1:Vq88fEOejxAHY49Muy00McWdTsU=]
TRANSUM RTE Data
\r\n
[Response in frame: 125]
[Full request URI: http://kurose.cslash.net/8E_cover_small.jpg]
[Community ID: 1:stIxOvDdFN5cJJdyFzqKk2X8uS8=]
TRANSUM RTE Data
```

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

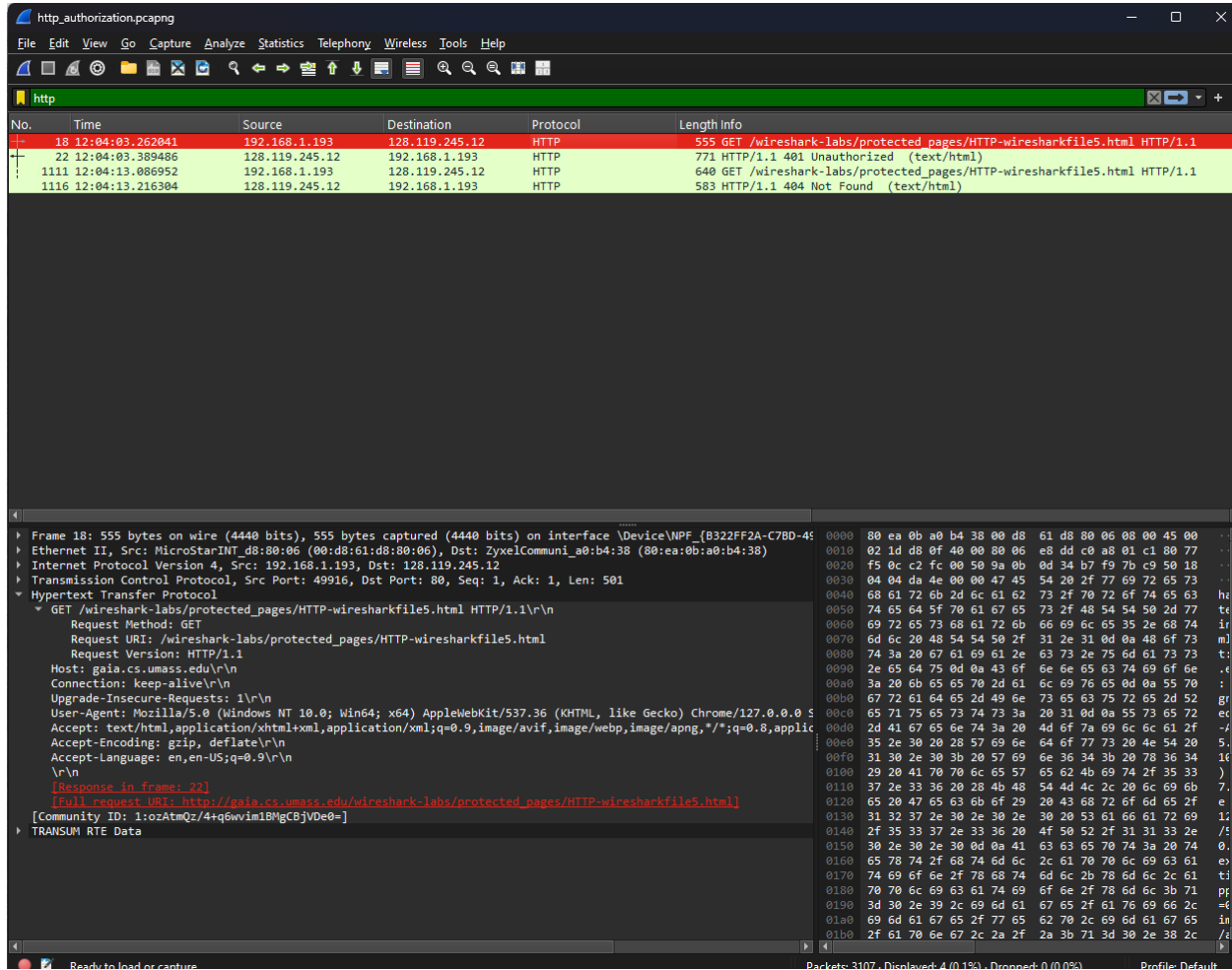


Figure 14: HTTP authorization

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

```
HTTP/1.1 401 Unauthorized\r\n
Response Version: HTTP/1.1
Status Code: 401
[Status Code Description: Unauthorized]
Response Phrase: Unauthorized
```

```
Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcm5=\r\n
Credentials: wireshark-students:network
Upgrade-Insecure-Requests: 1\r\n
```

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
```

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 \(baidu.com\)](https://www.baidu.com)

Addresses: 45.113.192.102, 45.113.192.101

```
PS C:\Users\gorke> |
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](https://www.tum.de)

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


    crt3.digicert.com
    -----
    Record Name . . . . . : crt3.digicert.com
    Record Type . . . . . : 5
    Time To Live . . . . . : 428
    Data Length . . . . . : 8
    Section . . . . . : Answer
    CNAME Record . . . . . : crt.edge.digicert.com


    Record Name . . . . . : crt.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.

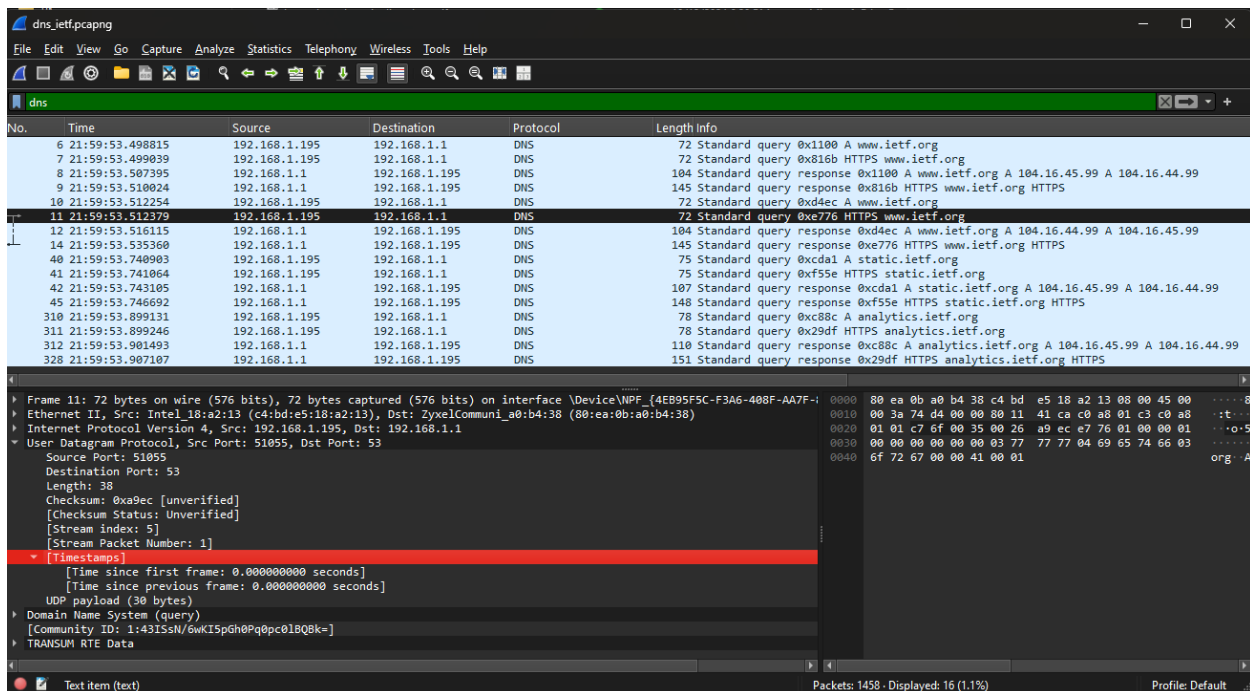


Figure 18: DNS query for ietf

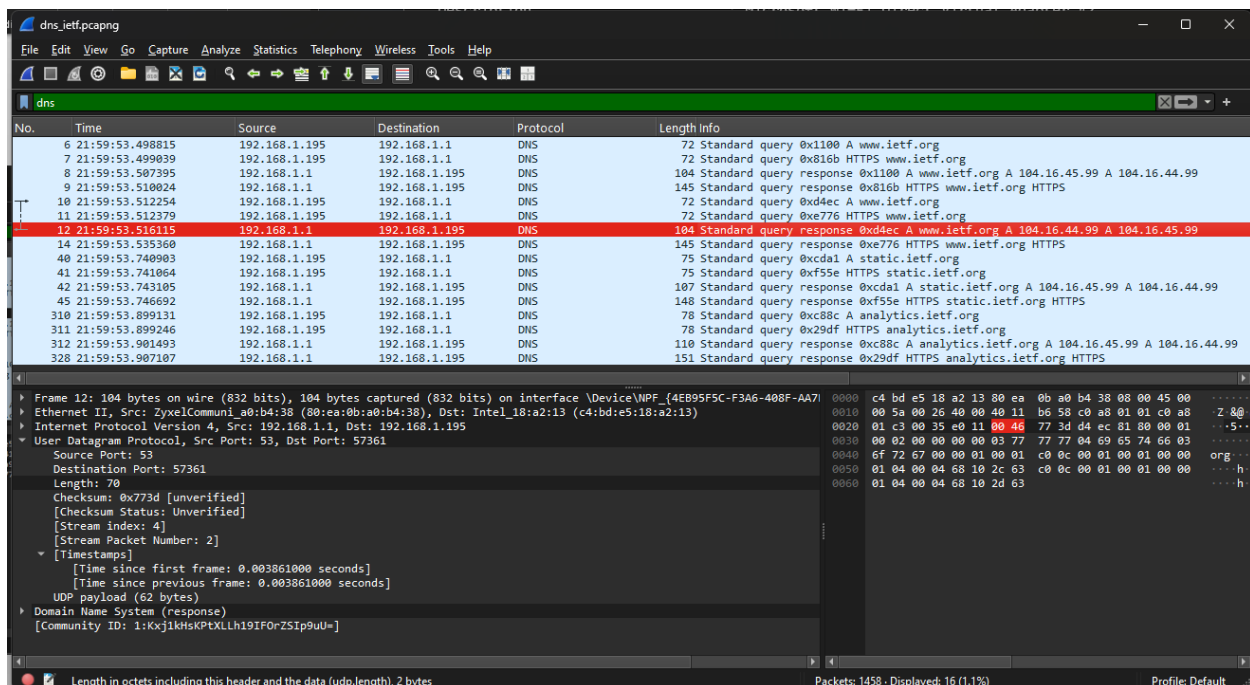


Figure 19: DNS response for ietf

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.

```

User Datagram Protocol, Src Port: 51055, Dst Port: 53
  Source Port: 51055
  Destination Port: 53
  Length: 38
  Checksum: 0xa9ec [unverified]
  [Checksum Status: Unverified]
  [Stream index: 5]
  [Stream Packet Number: 1]
  [Timestamps]
    [Time since first frame: 0.00000000 seconds]
    [Time since previous frame: 0.00000000 seconds]
  UDP payload (30 bytes)

User Datagram Protocol, Src Port: 53, Dst Port: 51055
  Source Port: 53
  Destination Port: 51055
  Length: 111
  Checksum: 0xb690 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 5]
  [Stream Packet Number: 2]
  [Timestamps]
    [Time since first frame: 0.022981000 seconds]
    [Time since previous frame: 0.022981000 seconds]
  UDP payload (103 bytes)

```

```

DHCPv6 Client DUID. . . . . : 00-01-00-01-2
DNS Servers . . . . . : 192.168.1.1
NetBIOS over Tcpip. . . . . : Enabled
PS C:\Users\gorke> D

```

```

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)
    [Response In: 12]

```

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.

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?

```
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:Kxj1kHsKPtXLLh19IF0rZ5IP9uU=]
```

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.

The image shows a Wireshark network traffic capture. The top pane displays a list of packets. Packet 13 is a DNS response from 192.168.1.195 to 104.16.44.99. Packet 14 is a TCP SYN packet from 192.168.1.195 to 104.16.44.99. Packet 15 is a TCP SYN packet from 192.168.1.195 to 104.16.45.99. The bottom pane shows the details of packet 15, which is a TCP SYN packet. The 'Flags' field is set to '0x002 (SYN)'. The 'Destination Port' is 443. The 'Sequence Number' is 1422386297. The 'Acknowledgment Number' is 0. The 'Window' is 64240. The 'Checksum' is 0x1dfa. The 'Urgent Pointer' is 0. The 'Options' field is set to '(12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP)'. The 'Community ID' is 1:lwP8Q5NvUE0j1S3rjzFrrr4=.

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> |
```

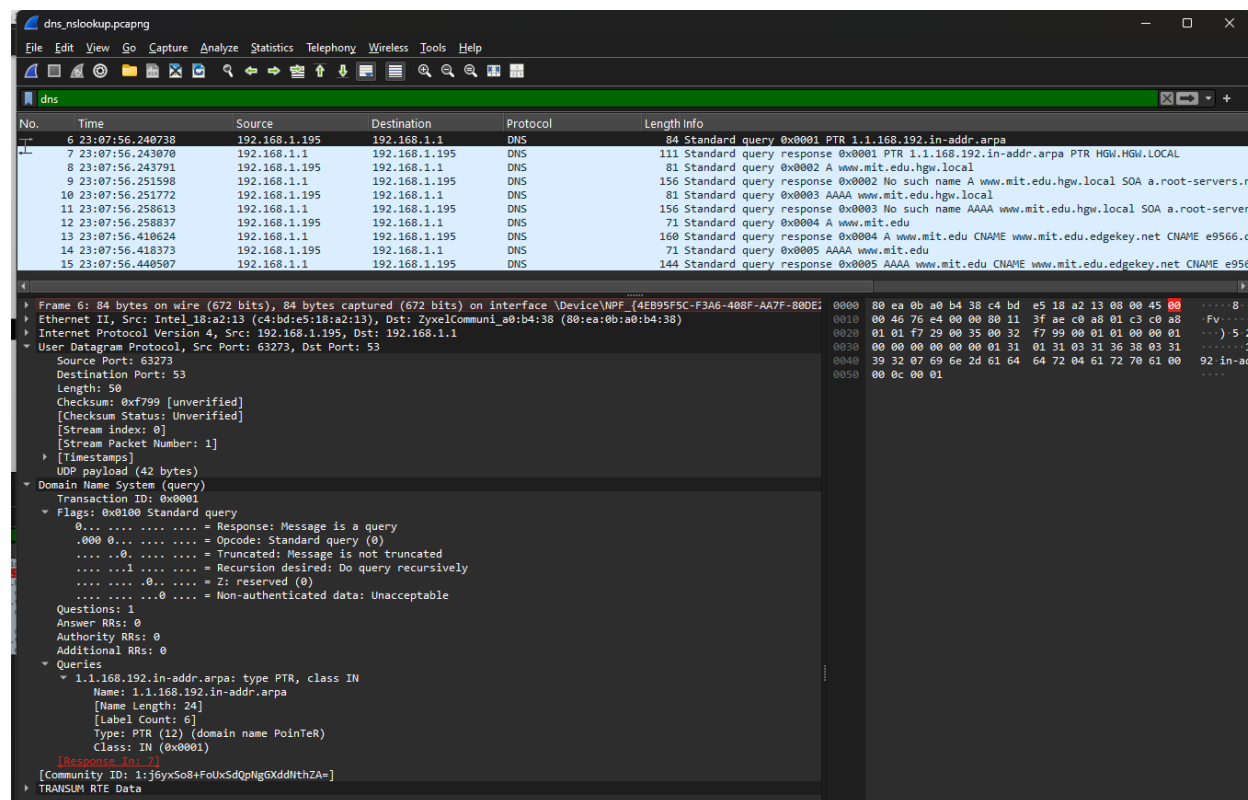


Figure 20: nslookup mit query

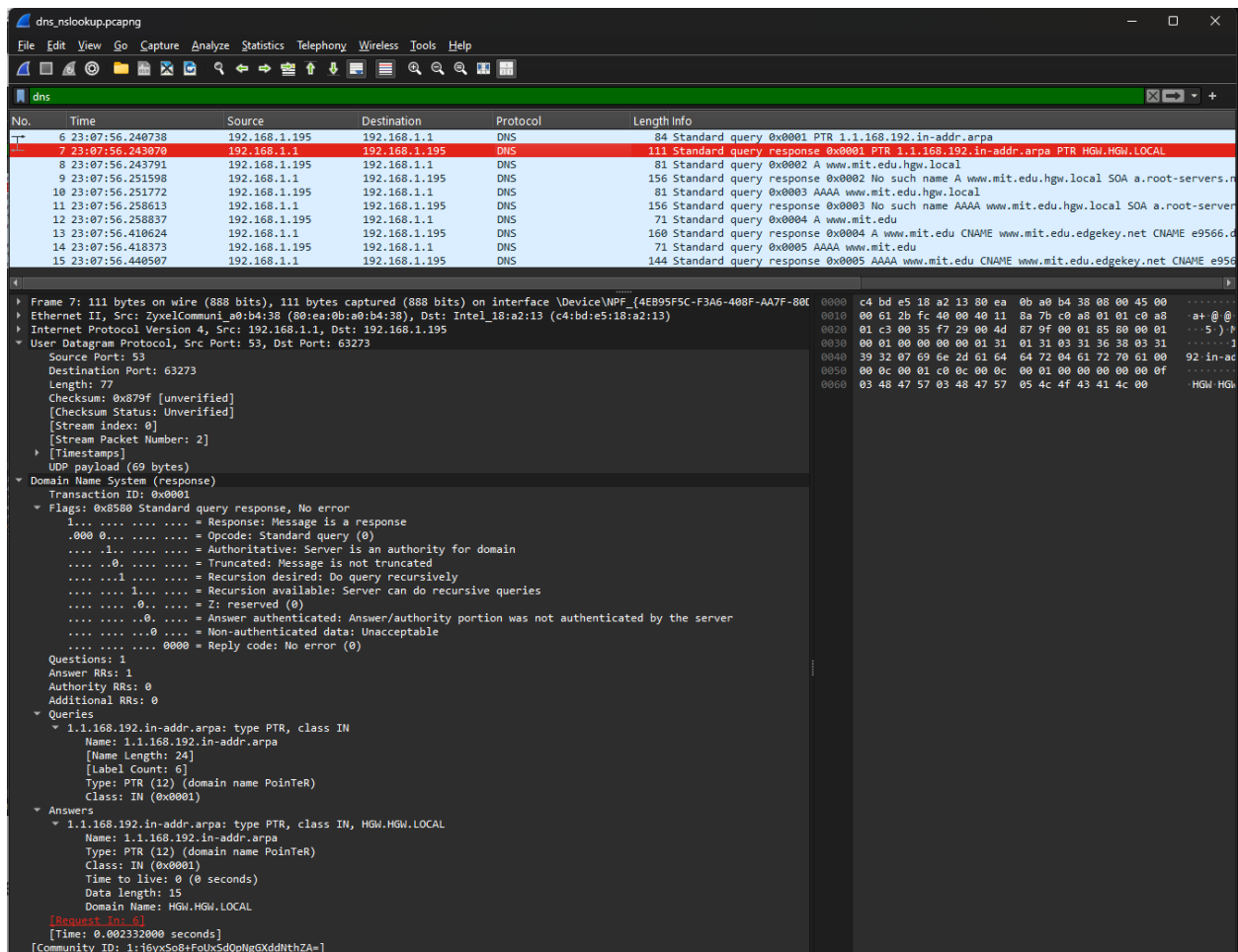


Figure 21: nslookup mit response

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.

The screenshot shows a Wireshark capture of a DNS query and response. The packet list pane displays the following packets:

No.	Time	Source	Destination	Protocol	Length	Info
6	23:07:56.240738	192.168.1.195	192.168.1.1	DNS	84	Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
7	23:07:56.243070	192.168.1.1	192.168.1.195	DNS	111	Standard query response 0x0001 PTR 1.1.168.192.in-addr.arpa PTR HGW.HGW.LOCAL
8	23:07:56.243791	192.168.1.195	192.168.1.1	DNS	81	Standard query 0x0002 A www.mit.edu.hgw.local
9	23:07:56.251598	192.168.1.1	192.168.1.195	DNS	156	Standard query response 0x0002 No such name A www.mit.edu.hgw.local SOA a.root-servers.n
10	23:07:56.251772	192.168.1.195	192.168.1.1	DNS	81	Standard query 0x0003 AAAA www.mit.edu.hgw.local
11	23:07:56.258613	192.168.1.1	192.168.1.195	DNS	156	Standard query response 0x0003 No such name AAAA www.mit.edu.hgw.local SOA a.root-server
12	23:07:56.258837	192.168.1.195	192.168.1.1	DNS	71	Standard query 0x0004 A www.mit.edu
13	23:07:56.410024	192.168.1.1	192.168.1.195	DNS	160	Standard query response 0x0004 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.d
14	23:07:56.418373	192.168.1.195	192.168.1.1	DNS	71	Standard query 0x0005 AAAA www.mit.edu
15	23:07:56.440507	192.168.1.1	192.168.1.195	DNS	144	Standard query response 0x0005 AAAA www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e956

The packet details pane for packet 13 shows the following structure:

- Frame 13: 160 bytes on wire (1280 bits), 160 bytes captured (1280 bits) on interface \Device\NPF_{4EB95F5C-F3A6-408F-AA7F-000000000000}
- Ethernet II, Src: ZyxelCommuni_a0:b4:38 (08:ea:0b:a0:b4:38), Dst: Intel_18:a2:13 (c4:bd:e5:18:a2:13)
- Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.195
- User Datagram Protocol, Src Port: 53, Dst Port: 63276
- Domain Name System (response)
 - Transaction ID: 0x0004
 - Flags: 0x8180 Standard query response, No error
 - Questions: 1
 - Answer RRs: 3
 - Authority RRs: 0
 - Additional RRs: 0
 - 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)
 - 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

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> |
```

The screenshot shows a Wireshark capture of a DNS query. The packet list table is as follows:

No.	Time	Source	Destination	Protocol	Length	Info
27	23:55:02.947258	192.168.1.195	192.168.1.1	DNS	67	Standard query 0xba3b A mit.edu
28	23:55:02.965689	192.168.1.1	192.168.1.195	DNS	83	Standard query response 0xba3b A mit.edu A 104.66.66.27
29	23:55:02.968489	192.168.1.195	104.66.66.27	DNS	85	Standard query 0x0001 PTR 27.66.66.104.in-addr.arpa
39	23:55:04.970667	192.168.1.195	104.66.66.27	DNS	78	Standard query 0x0002 A type=NS.hgw.local
40	23:55:04.971394	192.168.1.195	192.168.1.1	DNS	89	Standard query 0xf0c5 A v10.events.data.microsoft.com
41	23:55:04.997224	192.168.1.1	192.168.1.195	DNS	229	Standard query response 0xf0c5 A v10.events.data.microsoft.com CNAME win-global-asimov-1
69	23:55:06.986313	192.168.1.195	104.66.66.27	DNS	78	Standard query 0x0003 AAAA type=NS.hgw.local

The details pane for the selected packet (No. 27) shows:

- Frame 27: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface \Device\NPF... (00:00:00:00:00:00)
- Ethernet II, Src: Intel_18:a2:13 (c4:bd:e5:18:a2:13), Dst: ZyxelCommuni_00:b4:38 (00:ea:0b:a0:b4:38)
- Internet Protocol Version 4, Src: 192.168.1.195, Dst: 192.168.1.1
- User Datagram Protocol, Src Port: 61962, Dst Port: 53
- Domain Name System (query)
 - Transaction ID: 0xba3b
 - Flags: 0x0100 Standard query
 - Questions: 1
 - Answer RRs: 0
 - Authority RRs: 0
 - Additional RRs: 0
 - Queries
 - mit.edu: type A, class IN

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).

Standard query response 0xba3b A mit.edu A 104.66.66.27
PTR 27.66.66.104.in-addr.arpa

The screenshot shows a Wireshark capture of a DNS response. The details pane for the selected packet (No. 28) shows:

- 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
 - Answers
 - mit.edu: type A, class IN
 - Name: mit.edu
 - [Name Length: 7]
 - [Label Count: 2]
 - Type: A (1) (Host Address)
 - Class: IN (0x0001)

19. Provide a screenshot.

```
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 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.

The screenshot shows a Wireshark capture of a DNS query. The packet list at the top shows a query for bitsy.mit.edu sent to 192.168.1.1. The packet details pane shows the query structure, including the domain name and the IP address of the host. The packet bytes pane shows the raw data of the query.

No.	Time	Source	Destination	Protocol	Length	Info
73	23:58:33.978039	192.168.1.195	192.168.1.1	DNS	73	Standard query 0xffa9 A bitsy.mit.edu
74	23:58:33.979963	192.168.1.1	192.168.1.195	DNS	89	Standard query response 0xffa9 A bitsy.mit.edu A 18.0.72.3
75	23:58:33.981428	192.168.1.195	18.0.72.3	DNS	82	Standard query 0x0001 PTR 3.72.0.18.in-addr.arpa
76	23:58:35.985369	192.168.1.195	18.0.72.3	DNS	84	Standard query 0x0002 A www.aiit.or.kr.hgw.local
81	23:58:37.861443	192.168.1.195	192.168.1.1	DNS	91	Standard query 0xddc7 A identity.nel.measure.office.net
82	23:58:37.861961	192.168.1.195	192.168.1.1	DNS	91	Standard query 0x7014 HTTPS identity.nel.measure.office.net
85	23:58:37.873291	192.168.1.1	192.168.1.195	DNS	202	Standard query response 0xddc7 A identity.nel.measure.office.net CNAME nel.measure.office.net
94	23:58:37.877927	192.168.1.1	192.168.1.195	DNS	234	Standard query response 0x7014 HTTPS identity.nel.measure.office.net CNAME nel.measure.office.net
98	23:58:38.002217	192.168.1.195	18.0.72.3	DNS	84	Standard query 0x0003 AAAA www.aiit.or.kr.hgw.local
116	23:58:40.010610	192.168.1.195	18.0.72.3	DNS	74	Standard query 0x0004 A www.aiit.or.kr
117	23:58:42.012844	192.168.1.195	18.0.72.3	DNS	74	Standard query 0x0005 AAAA www.aiit.or.kr
123	23:58:43.448727	192.168.1.195	192.168.1.1	DNS	76	Standard query 0xbe5c A go.microsoft.com
124	23:58:43.458770	192.168.1.1	192.168.1.195	DNS	171	Standard query response 0xbe5c A go.microsoft.com CNAME go.microsoft.com.edgekey.net CNAME e11
136	23:58:43.524708	192.168.1.195	192.168.1.1	DNS	77	Standard query 0xd4c9 A www.microsoft.com
137	23:58:43.538616	192.168.1.1	192.168.1.195	DNS	244	Standard query response 0xd4c9 A www.microsoft.com CNAME www.microsoft.com-c-3.edgekey.net CNAME

Frame 73: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface \Device\NPF... (4E95F5C-F3A6-408F-AA7F-80DE2955...)

Ethernet II, Src: Intel_18:a2:13 (c4:bd:e5:18:a2:13), Dst: ZyxelCommuni_0:b4:38 (00:ea:0b:a0:b4:38)

Internet Protocol Version 4, Src: 192.168.1.195, Dst: 192.168.1.1

User Datagram Protocol, Src Port: 58264, Dst Port: 53

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 ID: 74]

[Community ID: 1:PMKKfd5AUGsdyXACVprnLwGpF=]

TRANSMISSION Data

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.

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 (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:MHkKfd5AUgsGyXACVprmlLwwGpfE=]
  TRANSM RTE Data
```

```
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:MHkKfd5AUgsGyXACVprmlLwwGpfE=]
```

The figure displays a Wireshark packet capture titled "dns_nsloukup_3.pcapng". The top pane shows a list of packets, with packet 74 selected. The middle pane shows the details of packet 74, which is a Standard query response from 192.168.1.1 to 192.168.1.195. The bottom pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length Info
73	23:58:33.978839	192.168.1.195	192.168.1.1	DNS	73 Standard query 0xffa9 A bitsy.mit.edu
74	23:58:33.979963	192.168.1.1	192.168.1.195	DNS	89 Standard query response 0xffa9 A bitsy.mit.edu A 18.0.72.3
75	23:58:33.981428	192.168.1.195	18.0.72.3	DNS	82 Standard query 0x0001 PTR 3.72.0.18.in-addr.arpa
76	23:58:35.985369	192.168.1.195	18.0.72.3	DNS	84 Standard query 0x0001 A www.aait.or.kr.hgw.local
81	23:58:37.861443	192.168.1.195	192.168.1.1	DNS	91 Standard query 0xddc7 A identity.nel.measure.office.net
82	23:58:37.861961	192.168.1.195	192.168.1.1	DNS	91 Standard query 0x7014 HTTPS identity.nel.measure.office.net
85	23:58:37.873291	192.168.1.1	192.168.1.195	DNS	282 Standard query response 0xddc7 A identity.nel.measure.office.net CNAME identity.nel.measure.office.net
94	23:58:37.877927	192.168.1.1	192.168.1.195	DNS	234 Standard query response 0x7014 HTTPS identity.nel.measure.office.net CNAME nel.measure.office
98	23:58:38.002217	192.168.1.195	18.0.72.3	DNS	84 Standard query 0x0003 AAAA www.aait.or.kr.hgw.local
116	23:58:40.010610	192.168.1.195	18.0.72.3	DNS	74 Standard query 0x0004 A www.aait.or.kr
117	23:58:42.012844	192.168.1.195	18.0.72.3	DNS	74 Standard query 0x0005 AAAA www.aait.or.kr
123	23:58:43.448727	192.168.1.195	192.168.1.1	DNS	76 Standard query 0xbe5c A go.microsoft.com
124	23:58:43.458770	192.168.1.1	192.168.1.195	DNS	171 Standard query response 0xbe5c A go.microsoft.com CNAME go.microsoft.com.edgekey.net CNAME e1
136	23:58:43.524708	192.168.1.195	192.168.1.1	DNS	77 Standard query 0xd4c9 A www.microsoft.com
137	23:58:43.530616	192.168.1.1	192.168.1.195	DNS	244 Standard query response 0xd4c9 A www.microsoft.com CNAME www.microsoft.com-c-3.edgekey.net Clu

Packet Details:

- Ethernet II, Src: IntelCommunity-a0:b4:38 (08:ea:0b:a4:38), Dst: Intel_18:a2:13 (c4:bd:e5:18:a2:13)
- Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.195
- User Datagram Protocol, Src Port: 53, Dst Port: 58264
- Domain Name System (response)
 - Transaction ID: 0xffa9
 - Flags: 0xb180 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: 2]
 - 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

Raw Data:

```
[Request ID: 72]
[Time: 0.001924000 seconds]
[Community ID: 1;HkkfkdSAUgfsGACVPnLwGpfE=]
```