



BILKENT UNIVERSITY

CS 421 – COMPUTER NETWORKS

WIRESHARK ASSIGNMENT REPORT

Name: Deniz Yüksel

ID: 21600880

Responses for Questions per Section:

What to Hand In

1. 10 protocol names that I can see after I download the INTRO-wireshark-file1 page:

UDP, TCP, HTTP, SSDP, IGMPv2, ICMPv6, MDNS, ARP, DNS, STP (looks pale grey, as unavailable).

2. In terms of time of day, the GET request was captured at 19:57:30.192855 and the response, 19:57:30.339441. If I choose the time as milliseconds, I see 206 milliseconds.

3. My IP is 139.179.202.218. The IP address of gaia.cs.umass.edu is 128.119.245.12 .

4. Printed to 2 pdf files, indicated as images below.

```
No.      Time          Source          Destination      Protocol Length Info
192 19:57:30.192 139.179.202.218 128.119.245.12   HTTP      608      GET /wireshark-labs/INTRO-
wireshark-file1.html HTTP/1.1
Frame 192: 608 bytes on wire (4864 bits), 608 bytes captured (4864 bits) on interface 0
Ethernet II, Src: Micro-St_f3:64:12 (d8:cb:8a:f3:64:12), Dst: SuperMic_8e:b3:6f (0c:c4:7a:8e:b3:6f)
Internet Protocol Version 4, Src: 139.179.202.218, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 49934, Dst Port: 80, Seq: 1, Ack: 1, Len: 554
Hypertext Transfer Protocol
  GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
  Host: gaia.cs.umass.edu\r\n
  Connection: keep-alive\r\n
  Upgrade-Insecure-Requests: 1\r\n
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
77.0.3865.120 Safari/537.36\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/
signed-exchange;v=b3\r\n
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: en-US,en;q=0.9,tr;q=0.8\r\n
  If-None-Match: "51-595c9f6a2eef9"\r\n
  If-Modified-Since: Sat, 26 Oct 2019 05:59:02 GMT\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
[HTTP request 1/1]
[Response in frame: 198]
```

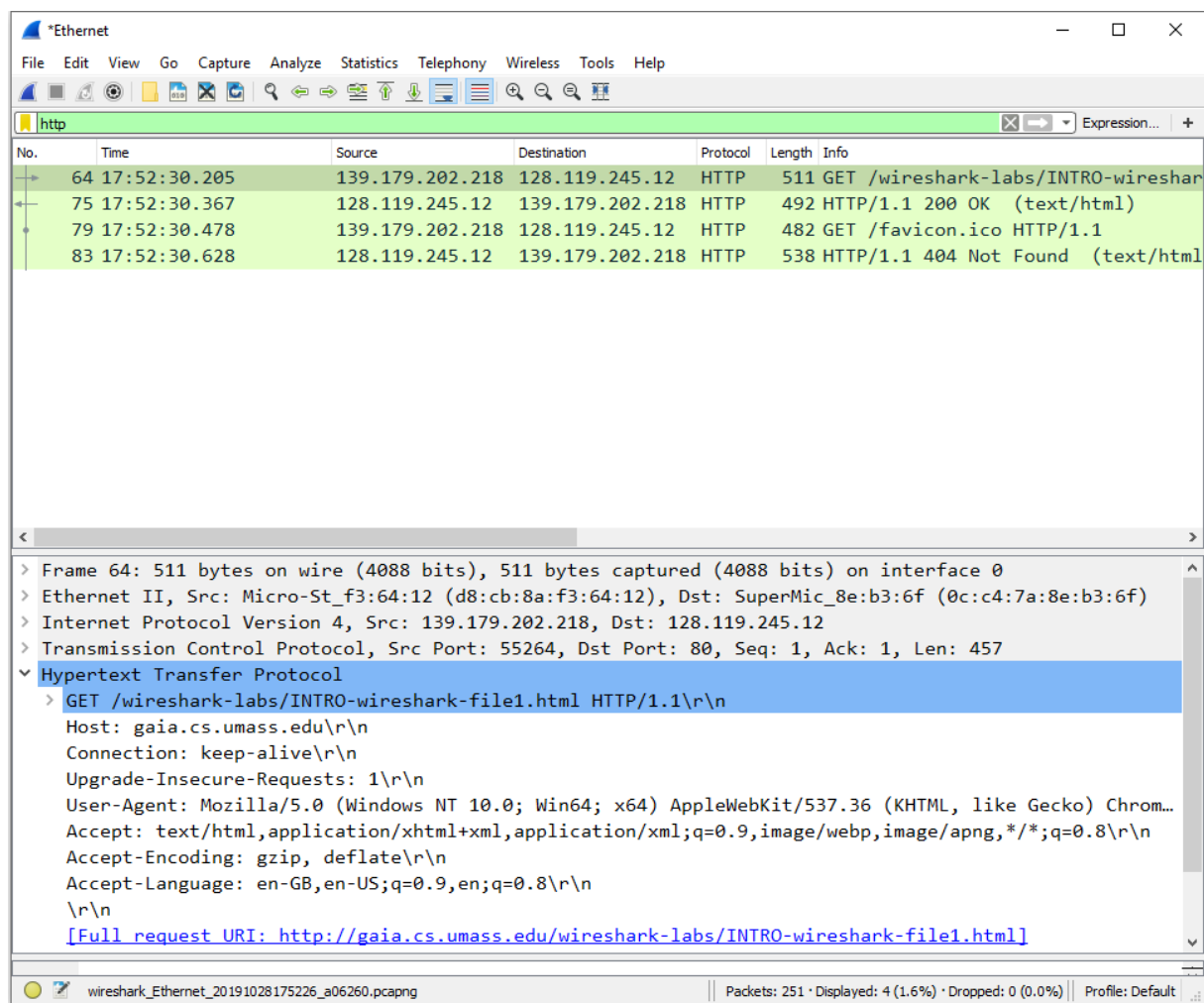
No.	Time	Source	Destination	Protocol	Length	Info
198	19:57:30.339	128.119.245.12	139.179.202.218	HTTP	293	HTTP/1.1 304 Not Modified

Frame 198: 293 bytes on wire (2344 bits), 293 bytes captured (2344 bits) on interface 0
 Ethernet II, Src: SuperMic_8e:b3:6f (0c:c4:7a:8e:b3:6f), Dst: Micro-St_f3:64:12 (d8:cb:8a:f3:64:12)
 Internet Protocol Version 4, Src: 128.119.245.12, Dst: 139.179.202.218
 Transmission Control Protocol, Src Port: 80, Dst Port: 49934, Seq: 1, Ack: 555, Len: 239
 Hypertext Transfer Protocol
 HTTP/1.1 304 Not Modified\r\n
 Date: Sat, 26 Oct 2019 16:57:30 GMT\r\n
 Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
 Connection: Keep-Alive\r\n
 Keep-Alive: timeout=5, max=100\r\n
 ETag: "51-595c9f6a2eef9"\r\n
 \r\n
 [HTTP response 1/1]
 [Time since request: 0.146586000 seconds]
 [Request in frame: 192]
 [Request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]

1. The Basic HTTP GET/response interaction

1. Both my browser and the server are running in HTTP 1.1.
2. The accept languages are en-US and tr.
3. My IP is 139.179.202.218. The internet address of gaia.cs.umass.edu is 128.119.245.12.
4. 200 OK.
5. The file was last modified at Sat, 26 Oct 2019 05:59:02 GMT.
6. 540 have been returned to my browser from the server.
7. If I only look at the HTTP raw data, I do not see any data that are not listed below. However, if I open up TCP the [Stream Index: 1] is not mapped anywhere on the packet-listing window.

Image is included on the next page.



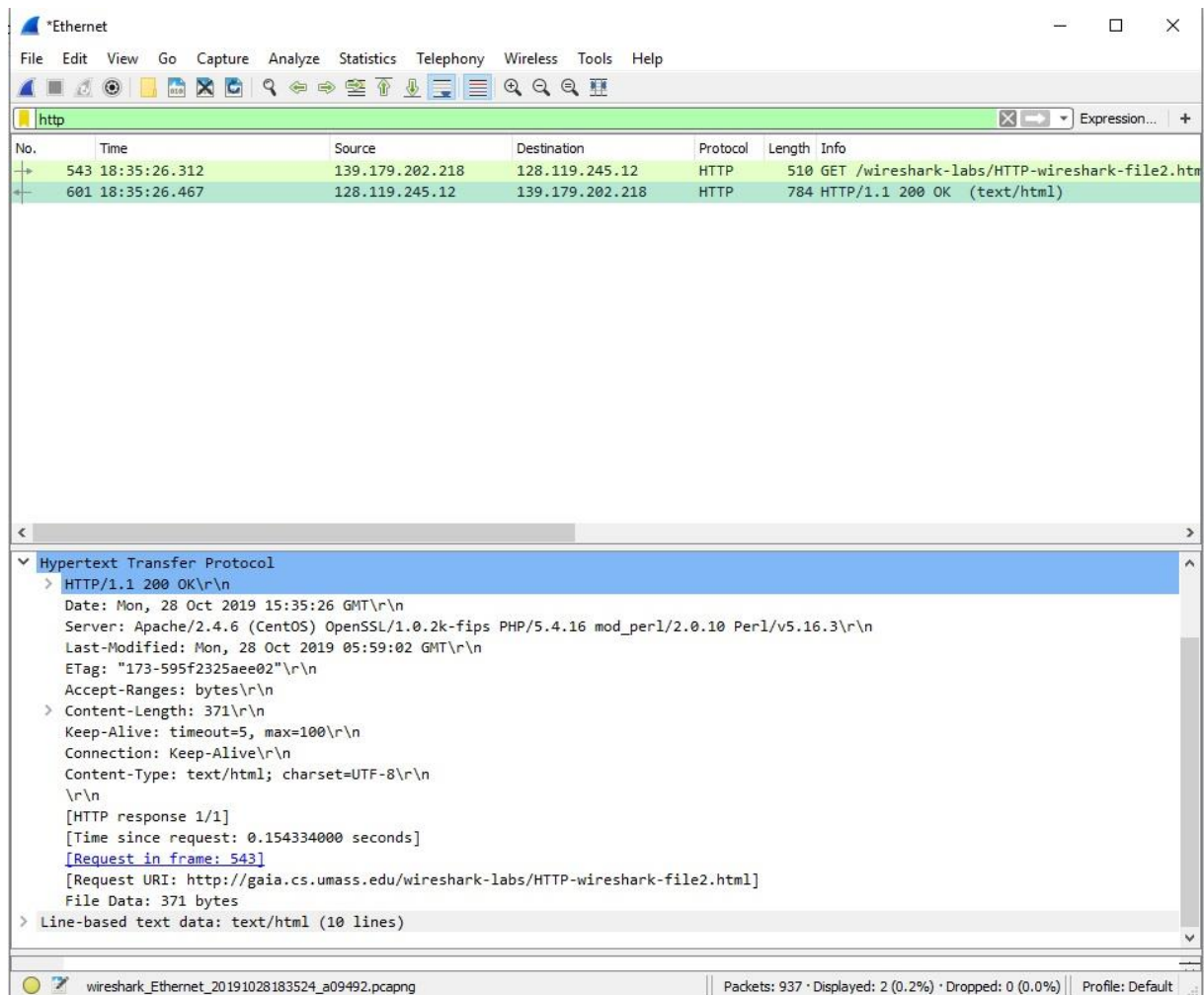
2. The HTTP CONDITIONAL GET/response Interaction

8. I do not see the following content.

9. Yes, the server returned the contents in a line-based text data. I can recognize it directly by the heading below HTTP information.

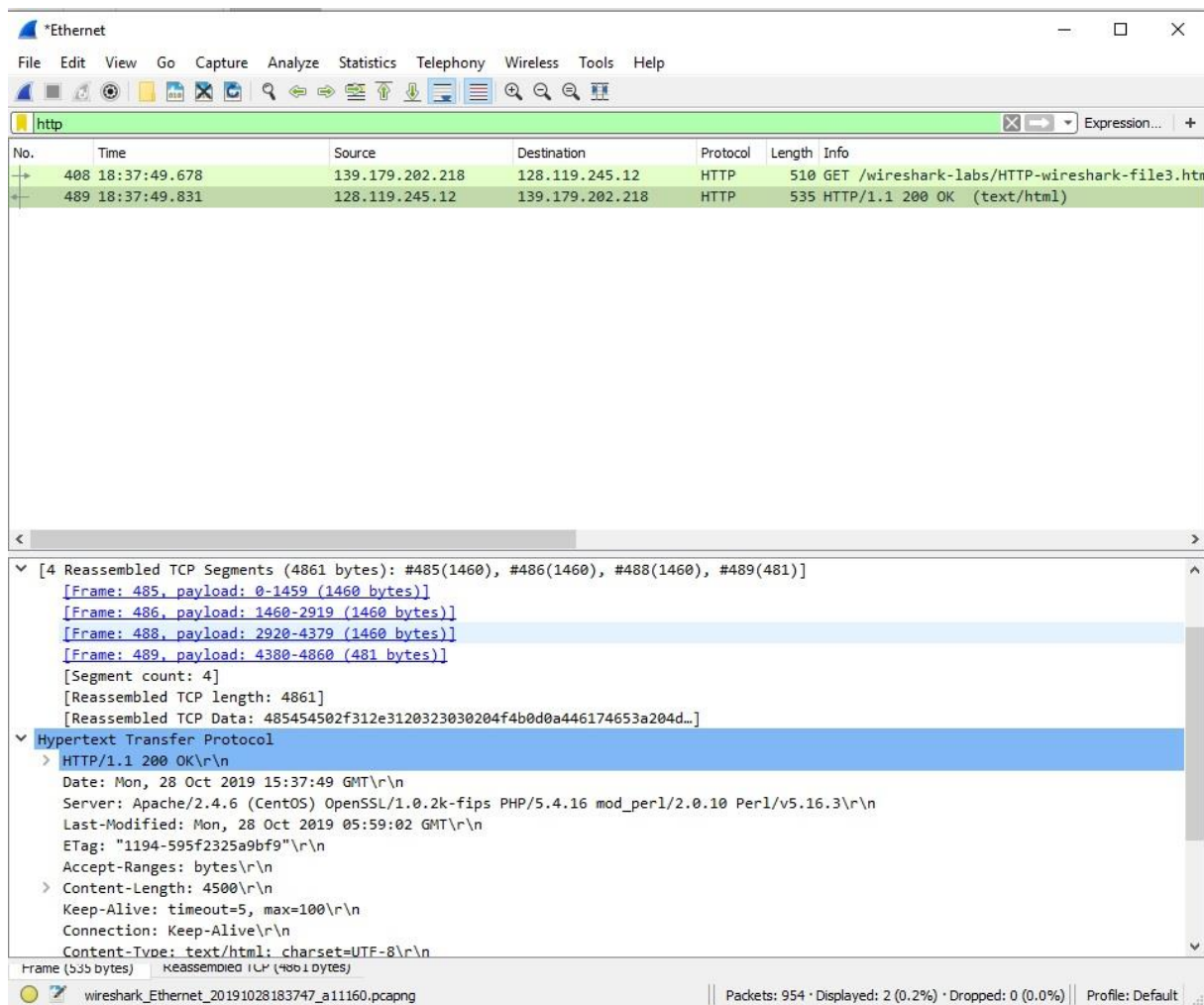
10. Now I see the line of If-Modified-Since in the raw data window below the HTTP GET request #2. It says: If-Modified-Since: Sat, 26 Oct 2019 05:59:02 GMT. This information is followed by full request URI and HTTP Request 3/3, and two other lines.

11. The response code is 304, not modified. This time, the file content is not sent to my browser. It was because if the page is not modified in a certain time interval, the contents are not sent again repeatedly.



3. Retrieving Long Documents

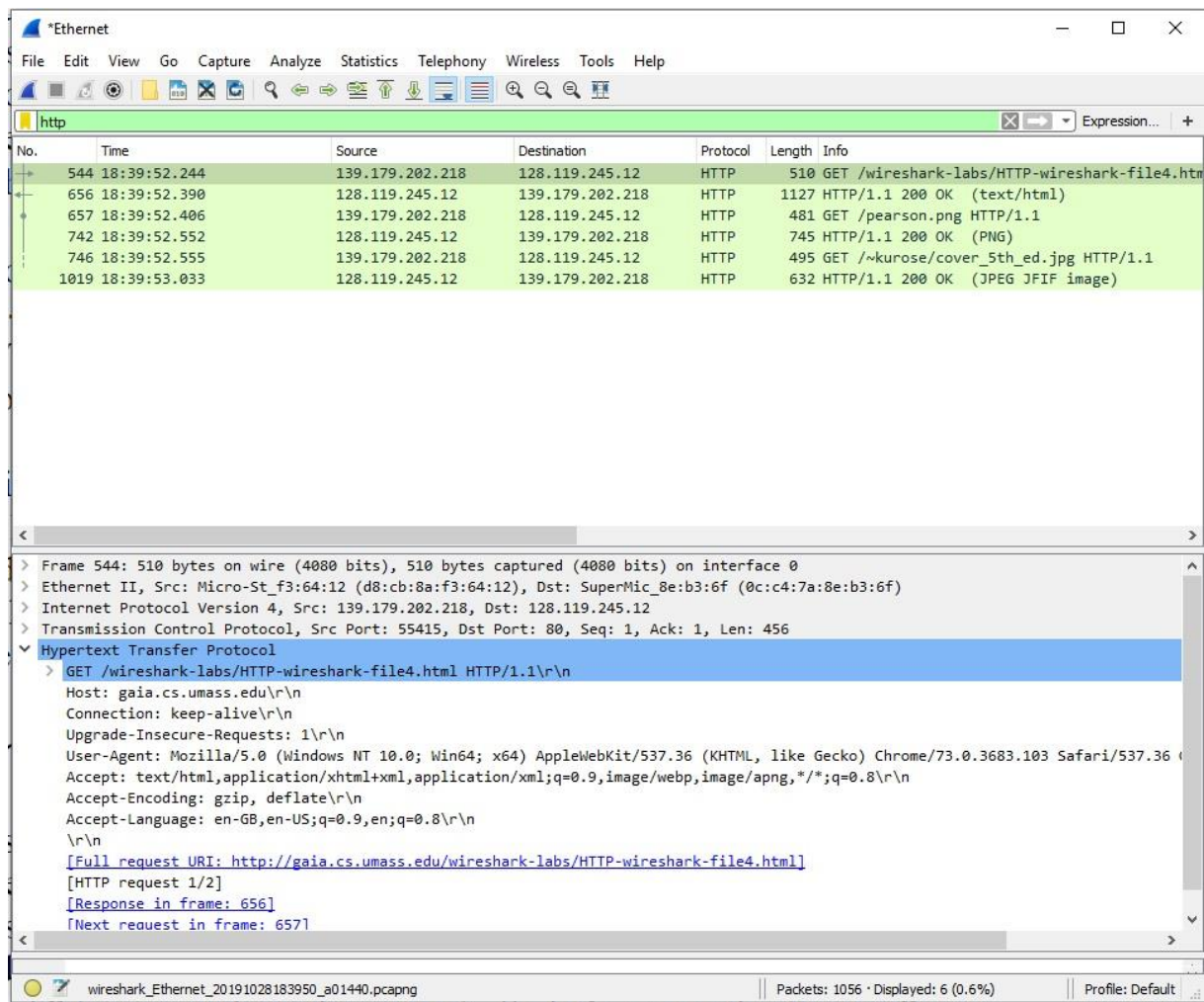
12. There is only one HTTP GET request sent by my browser.
13. 4 data containing TCP segments were needed to carry the single response. 3 of them had 1460 bytes where the last one had the remaining 481 bytes.
14. The request to the response had the status code of 200 and a message: "OK".
15. No.



4. HTML Documents with Embedded Objects

16. There are 3 HTTP GET request sent by my browser. They were sent to wireshark-labs, gaia.cs.umass.edu/pearson.png, and to ~/kurose/cover_5th_ed.jpg.

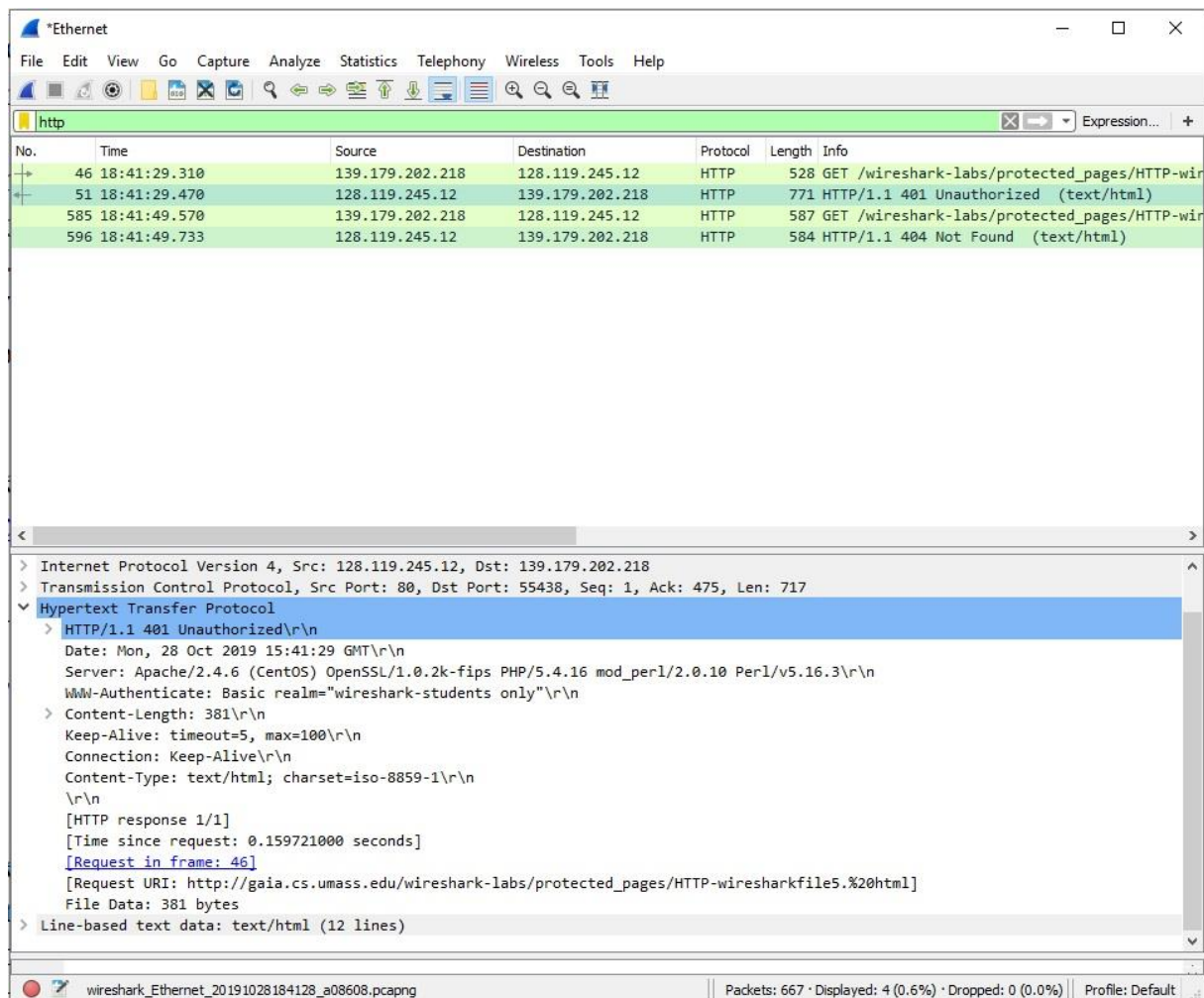
17. The first image sent to my browser was the Pearson logo in my opinion. Afterwards, the jpeg image of the book cover was sent. But both HTTP GET requests for the images are done back to back in a parallel manner, and both the responses came back to back. I can tell it from the listing of captured packets window.



5. HTTP Authentication

18. The server responded with response code 401 and response phrase: Unauthorized.

19. There is an additional line included with the information of credentials, username and password separated by a comma. The line has the following information of authorization: Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcm5=\r\n



DNS

1. nslookup

1. I ran nslookup with a web server in Singapore. The command I executed was:

nslookup secdns.sata.com.sg.

The response is:

Server: manyas.bcc.bilkent.edu.tr

Address: 139.179.30.24

Non-authoritative answer:

Name: secdns.sata.com.sg

Address: 203.126.23.54


```
Command Prompt
Microsoft Windows [Version 10.0.17763.805]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\deniz>nslookup secdns.sata.com.sg.
Server: manyas.bcc.bilkent.edu.tr
Address: 139.179.30.24

Non-authoritative answer:
Name:   secdns.sata.com.sg
Address: 203.126.23.54

C:\Users\deniz>
```

2. I ran nslookup with -NS parameter in type, as the following shown in the command prompt. I chose University of Twente in Netherlands, Twente. I found three non-authoritative answers that are listed below.

```
Command Prompt

    responsible mail addr = hostmaster.bilkent.edu.tr
    serial = 2019102800
    refresh = 43200 (12 hours)
    retry = 7200 (2 hours)
    expire = 604800 (7 days)
    default TTL = 300 (5 mins)

C:\Users\deniz>nslookup -type=NS utwente.nl
Server: manyas.bcc.bilkent.edu.tr
Address: 139.179.30.24

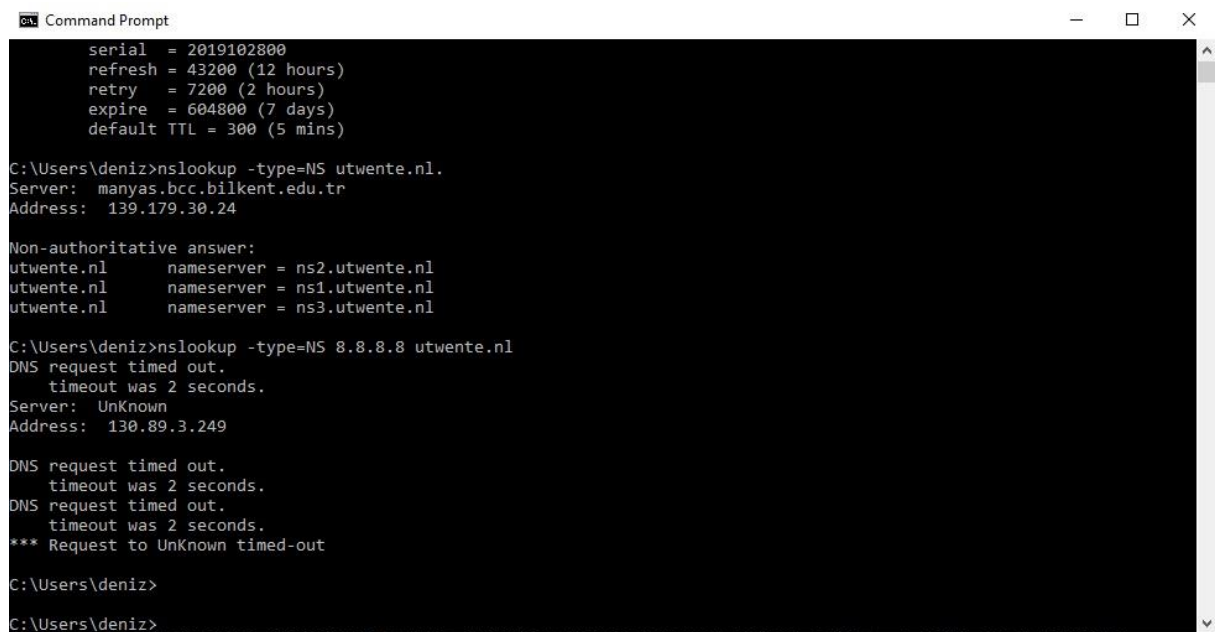
bilkent.edu.tr
    primary name server = firat.bcc.bilkent.edu.tr
    responsible mail addr = hostmaster.bilkent.edu.tr
    serial = 2019102800
    refresh = 43200 (12 hours)
    retry = 7200 (2 hours)
    expire = 604800 (7 days)
    default TTL = 300 (5 mins)

C:\Users\deniz>nslookup -type=NS utwente.nl.
Server: manyas.bcc.bilkent.edu.tr
Address: 139.179.30.24

Non-authoritative answer:
utwente.nl      nameserver = ns2.utwente.nl
utwente.nl      nameserver = ns1.utwente.nl
utwente.nl      nameserver = ns3.utwente.nl

C:\Users\deniz>
```

3. I could not find a public dns server for Yahoo mail, so I used open dns of Google. Then, I realized that maybe Twente University rejects the DNS request by giving timeouts, due to security policies.



```
Command Prompt
serial = 2019102800
refresh = 43200 (12 hours)
retry = 7200 (2 hours)
expire = 604800 (7 days)
default TTL = 300 (5 mins)

C:\Users\deniz>nslookup -type=NS utwente.nl.
Server: manyas.bcc.bilkent.edu.tr
Address: 139.179.30.24

Non-authoritative answer:
utwente.nl nameserver = ns2.utwente.nl
utwente.nl nameserver = ns1.utwente.nl
utwente.nl nameserver = ns3.utwente.nl

C:\Users\deniz>nslookup -type=NS 8.8.8.8 utwente.nl
DNS request timed out.
    timeout was 2 seconds.
Server: UnKnown
Address: 130.89.3.249

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** Request to UnKnown timed-out

C:\Users\deniz>
C:\Users\deniz>
```

3. Tracing DNS with Wireshark

4. I located several DNS query messages that that are more than 6 in count. All of them are sent with UDP. I checked it from the raw-data window's Internet Protocol Version line.

5. Destination port is 53. The source port of the response message is 53 as well.

6. DNS request is sent to ip 139.179.30.24. When I execute the command ipconfig /all, I see this same ip address as a DNS server.

7. It is a Standard Query with 1 question and no answers.

8. There are 2 answers. Answers are included below:

Answers

desktop-static.operacdn.com: type CNAME, class IN, cname m.shared.global.fastly.net

Name: desktop-static.operacdn.com

Type: CNAME (Canonical NAME for an alias) (5)

Class: IN (0x0001)

Time to live: 281

Data length: 28

CNAME: m.shared.global.fastly.net

m.shared.global.fastly.net: type A, class IN, addr 151.101.241.178

Name: m.shared.global.fastly.net

Type: A (Host Address) (1)

Class: IN (0x0001)

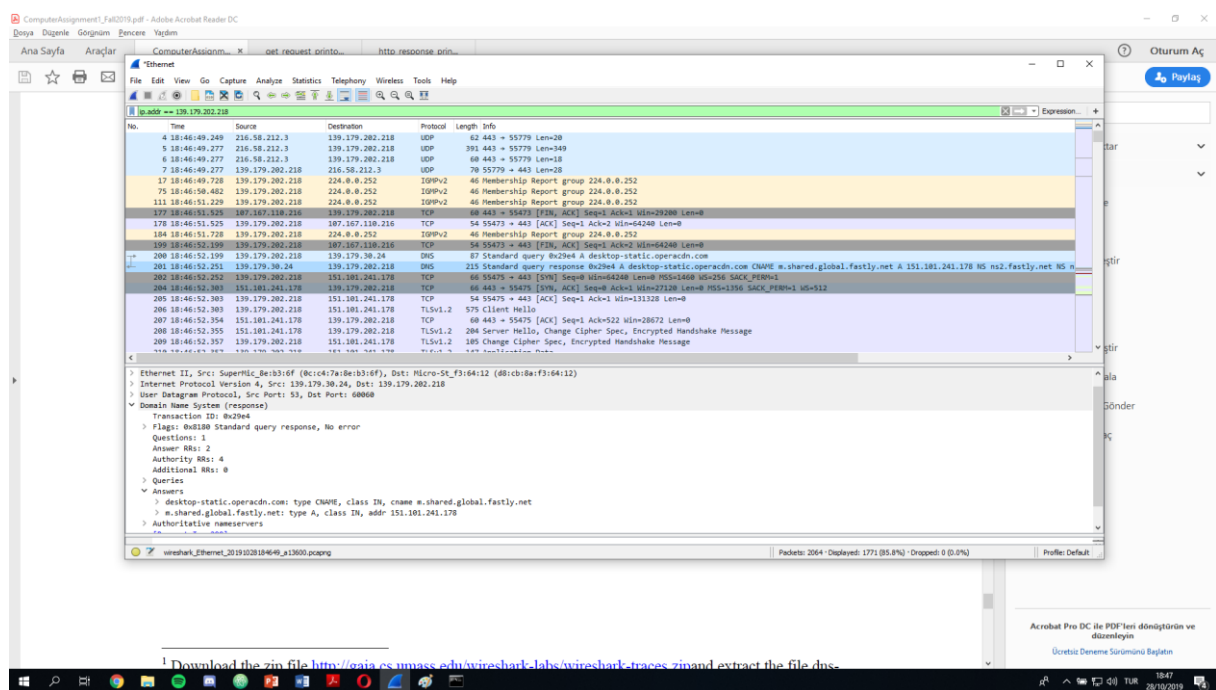
Time to live: 30

Data length: 4

Address: 151.101.241.178

9. Destination port of the SYN message is 443 which does not correspond to any of the source ports in the provided DNS message.

10. I could not understand if every image needs to precede a DNS query from this packet capture instance.



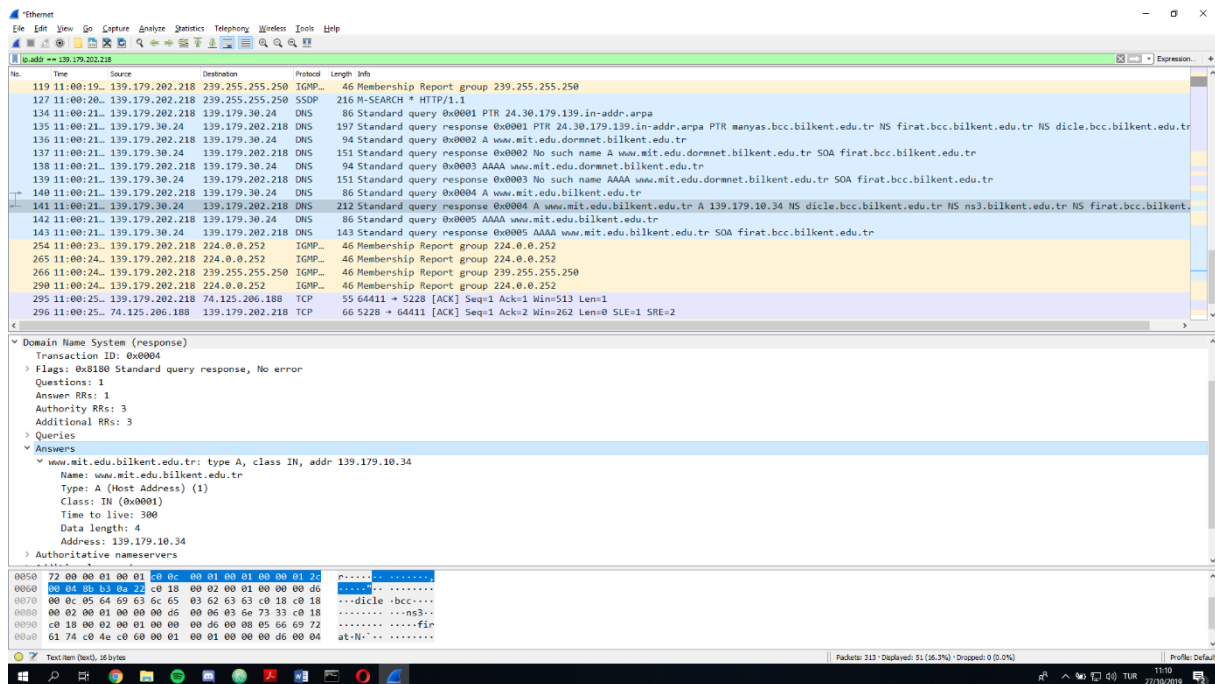
11. Destination port is 53. The source port of the response message is 53 as well.

12. The request is sent to 139.179.30.24. This is among my 2 dns servers. This is the first one listed, I guess it is the default one.

13. It is a Standard Query with no answers.

14. I've been looking at the request with a name 0x0004. So I will examine that particular answer. The answer contains a line: www.mit.edu.bilkent.edu.tr: type A, class IN, addr 139.179.30.24. Inside of the line, it contains type, class, time to live, data length and address.

15.



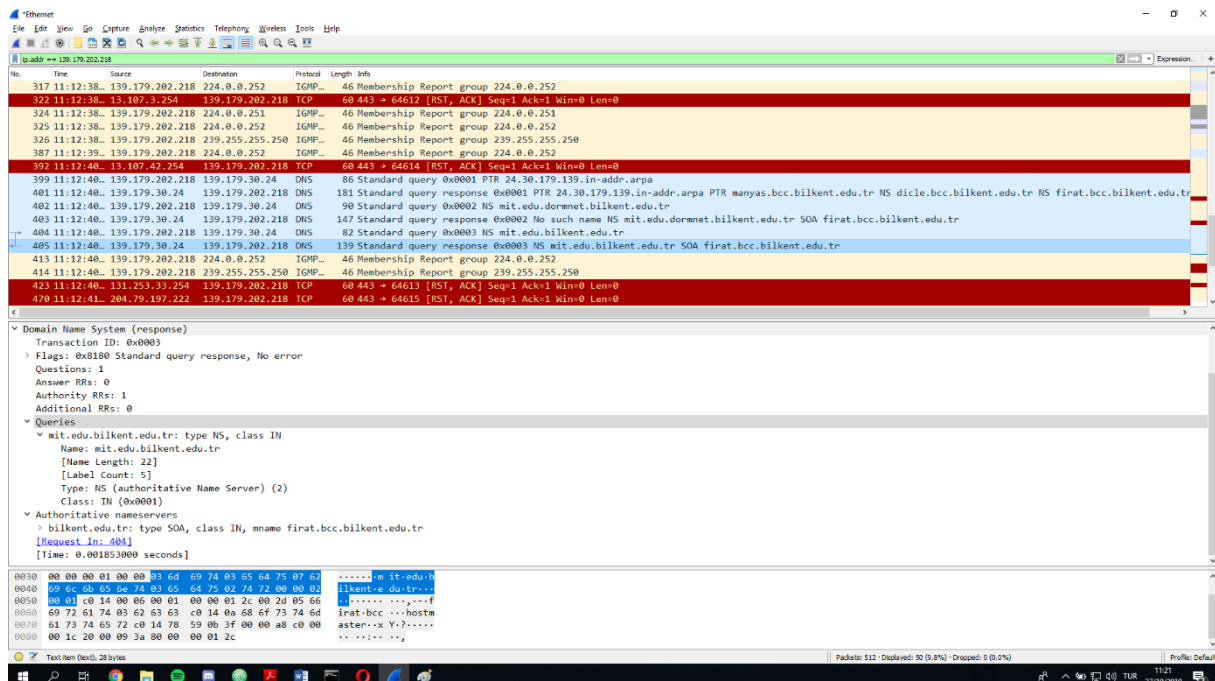
16. The destination IP address is still 139.179.30.24. So the query is sent to my local dns server.

17. No, there are no answers. All types are standard queries.

18. The response provides an mit name server such that its name is displayed as the following:

mit.edu.bilkent.edu.tr

19.



20. The DNS query message was sent to 139.179.30.24, which is my local dns server.

21. Again, all queries are standard queries. None of the DNS queries contain an answer.

22. There is only one DNS response message. The answer contains the following line:

bitsy.mit.edu: type A, class IN, addr 18.0.72.3

23.

The image shows a Wireshark packet capture of a network traffic. The top pane displays a list of packets. Packet 132 is selected, showing a DNS Standard query response from 139.179.202.218 to 139.179.30.24. The packet details pane shows the following information:

- Frame 132: 256 bytes on wire (2048 bits), 256 bytes captured (2048 bits) on interface 0
- Ethernet II, Src: SuperMic_8e:b3:6f (08:c4:7a:8e:b3:6f), Dst: Micro-St_f3:64:12 (d8:cb:8a:f3:64:12)
- Internet Protocol Version 4, Src: 139.179.30.24, Dst: 139.179.202.218
- User Datagram Protocol, Src Port: 53, Dst Port: 58627
- Domain Name System (response)
 - Transaction ID: 0xb818
 - Flags: 0xb180 Standard query response, No error
 - Questions: 1
 - Answer RRs: 1
 - Authority RRs: 0
 - Additional RRs: 0
 - Queries
 - Answers
 - bitsy.mit.edu: type A, class IN, addr 18.0.72.3
 - Name: bitsy.mit.edu
 - Type: A (Host Address) (1)
 - Class: IN (0x0001)
 - Time to live: 1771

The bottom pane shows the raw packet data in hexadecimal and ASCII format.