Yusuf Ziya Dilek
ID: 21501462
CS-421

Computer Assignment 1

1-) *Listing 10 different protocols that appeared in protocol column.*

TCP, UDP, ARP, MDNS, SSDP, TLSv1.2, IGMPv.2, ICMPv6, DHCPv6, STP.

2-) *How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received?*

Starts: 21:34:39

Ends: 21:34:40

3-) *What is the Internet address of the gaia.cs.umass.edu? What is the Internet address of your computer?*

Their IP: 128.119.245.12

My IP: 139.179.202.36

4-) *Print the two HTTP messages displayed in step 9 above.*

```
No.     Time               Source                Destination           Protocol Length Info
  11901 21:34:39.821817    139.179.202.36        128.119.245.12        HTTP     535    GET /wireshark-labs/INTRO-wireshark-
file1.html HTTP/1.1
Frame 11901: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface 0
Ethernet II, Src: CompalIn_22:dc:86 (1c:39:47:22:dc:86), Dst: SuperMic_8e:b3:6f (0c:c4:7a:8e:b3:6f)
Internet Protocol Version 4, Src: 139.179.202.36, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 55965 (55965), Dst Port: http (80), Seq: 1, Ack: 1, Len: 481
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: tr-TR,tr;q=0.9,en-US;q=0.8,en;q=0.7\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
    [HTTP request 1/2]
    [Response in frame: 11904]
    [Next request in frame: 13280]
```

Wireshark Lab: HTTP

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

Request version: HTTP/1.1 →Info line

HTTP 1.1

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

Yusuf Ziya Dilek
ID: 21501462
CS-421

Accept-Language: tr-TR,tr;q=0.9,en-US;q=0.8,en;q=0.7 →Code line

Turkish and English.

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

Their IP: 128.119.245.12 -> Destination of GET message

My IP: 139.179.202.36 -> Source of GET message

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

Status Code: 200 →Info line

Status Code Description: OK →Info line

Code is 200 (OK code that indicates the request is successful)

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

Last-Modified: Tue, 22 Oct 2019 05:59:03 GMT\r\n →Info line

22 October Tuesday at 05:59:03

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

File Data: 128 bytes →Info line

128 bytes of data is returned

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

Accept-Ranges: bytes

Content-Length: 128

Keep-Alive: timeout=5, max=100

Connection: Keep-Alive

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

<html>

Yusuf Ziya Dilek
ID: 21501462
CS-421

Congratulations. You've downloaded the file

http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html!

</html>

These are some examples.

2. The HTTP CONDITIONAL GET/response interaction

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?

In the first GET request there is no If-Modified-Since.

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

In the first GET, **Status code is 200**. The File Data: 371 bytes is returned but in the second time it returns **Status Code: 304** which means the file is not modified so file data did not sent again.

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-Modified-Since: Tue, 22 Oct 2019 05:59:03 GMT\r\n → this is the line that appears in second GET request

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.

Status Code: 304

Status Code Description: Not Modified

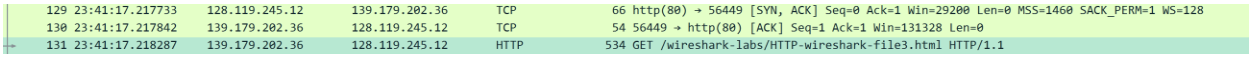
Response Phrase: Not Modified

Status Code: 304 which means the file is not modified. Because of that there is no file data is sent back in response to the second GET request.

Yusuf Ziya Dilek
ID: 21501462
CS-421

3. Retrieving Long Documents

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



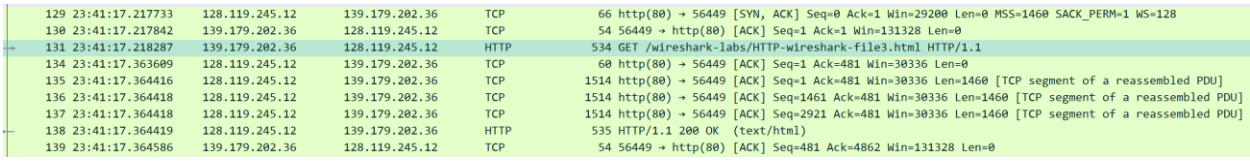
As we can see After [SYN,ACK] and [ACK] sequence there is singular GET request for this long file.

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

```
[4 Reassembled TCP Segments (4861 bytes): #135(1460), #136(1460), #137(1460), #138(481)]
    [Frame: 135, payload: 0-1459 (1460 bytes)]
    [Frame: 136, payload: 1460-2919 (1460 bytes)]
    [Frame: 137, payload: 2920-4379 (1460 bytes)]
    [Frame: 138, payload: 4380-4860 (481 bytes)]
    [Segment count: 4]
    [Reassembled TCP length: 4861]
    [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a2054…]
```

From here we can see that the response is broken into 4 segments.

This is the whole story:



As you can see there is 4 TCP connection between GET and the response.

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

```
Response Version: HTTP/1.1
Status Code: 200
[Status Code Description: OK]
Response Phrase: OK
```

Status code is 200.

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

I could not see any status line in the HTTP code itself that indicates "*Continuation*". It is the regular Status code 200.

Yusuf Ziya Dilek
ID: 21501462
CS-421

4. HTML Documents with Embedded Objects

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

106	00:19:55.053140	139.179.202.36	128.119.245.12	HTTP	534 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
111	00:19:55.205194	128.119.245.12	139.179.202.36	HTTP	1127 HTTP/1.1 200 OK (text/html)
113	00:19:55.278509	139.179.202.36	128.119.245.12	HTTP	472 GET /pearson.png HTTP/1.1
137	00:19:55.433625	128.119.245.12	139.179.202.36	HTTP	745 HTTP/1.1 200 OK (PNG)
156	00:19:55.477046	139.179.202.36	128.119.245.12	HTTP	486 GET /~kurose/cover_5th_ed.jpg HTTP/1.1
269	00:19:55.932599	128.119.245.12	139.179.202.36	HTTP	632 HTTP/1.1 200 OK (JPEG JFIF image)

There is 3 HTTP GET request messages were sent. 1 for base HTML and 2 for the PNG and JPEG files.

Host: gaia.cs.umass.edu\r\n →First GET

Host: www.aw-bc.com\r\n →Second GET

Host: manic.cs.umass.edu\r\n →Third GET

The last to GET messages have this extra line:

Referer: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html\r\n

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.

They are not parallel because the browser sends GET message for the first picture then waits for the response and gets the data, only after that sends the second GET message for the second picture. We can see this by looking at the time column.

5. HTTP Authentication

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

Status Code: 401

Status Code Description: Unauthorized

Response Phrase: 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?

This line is included:

Yusuf Ziya Dilek
ID: 21501462
CS-421

Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n

DNS

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

```
PS C:\Windows\system32> nslookup www.korea.edu
Server:  manyas.bcc.bilkent.edu.tr
Address:  139.179.30.24

Non-authoritative answer:
Name:    www.korea.edu.bilkent.edu.tr
Address:  139.179.10.34
```

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

```
PS C:\Users\Dilek> nslookup -type=NS www.cam.ac.uk
Server:  dns.google
Address:  8.8.8.8

bilkent.edu.tr
        primary name server = firat.bcc.bilkent.edu.tr
        responsible mail addr = hostmaster.bilkent.edu.tr
        serial  = 2019101503
        refresh = 43200 (12 hours)
        retry   = 7200 (2 hours)
        expire  = 604800 (7 days)
        default TTL = 300 (5 mins)
```

It always gives the Bilkent DNS servers as authoritative DNS servers for some reason.

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

```
PS C:\Users\Dilek> nslookup firat.bcc.bilkent.edu.tr mail.yahoo.com
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  87.248.118.22

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\Dilek>
```

IP is = 87.248.118.22

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

```
User Datagram Protocol, Src Port: 56737 (56737), Dst Port: domain (53)
    Source Port: 56737 (56737)
    Destination Port: domain (53)
    Length: 38
    Checksum: 0x012f [unverified]
    [Checksum Status: Unverified]
    [Stream index: 6]
  > [Timestamps]
Domain Name System (query)
    Transaction ID: 0xfeb3
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  > Queries
    [Response In: 66]
```

It is sent by user datagram protocol (UDP).

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

Standard query:

```
User Datagram Protocol, Src Port: 56737 (56737), Dst Port: domain (53)
    Source Port: 56737 (56737)
    Destination Port: domain (53)
```

Standard query response:

```
User Datagram Protocol, Src Port: domain (53), Dst Port: 56737 (56737)
    Source Port: domain (53)
    Destination Port: 56737 (56737)
```

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?

From ipconfig:

DNS Servers . . . . . : 139.179.30.24

139.179.10.13

```
51 21:53:55.097468 139.179.202.36    139.179.30.24    DNS    72 Standard query 0xfeb3 A www.ietf.org
```

We can see that DNS address acquired from ipconfig and standard DNS query destination address matches. Both of them are 139.179.30.24

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

```
Queries
  > www.ietf.org: type A, class IN
[Response In: 66]
```

Type A query with no answers.

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

```
Questions: 1
Answer RRs: 3
Authority RRs: 5
Additional RRs: 0
▾ Queries
  › www.ietf.org: type A, class IN
▾ Answers
  ▾ www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
      Name: www.ietf.org
      Type: CNAME (Canonical NAME for an alias) (5)
      Class: IN (0x0001)
      Time to live: 300
      Data length: 33
      CNAME: www.ietf.org.cdn.cloudflare.net
  › www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.1.85
  › www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.0.85
```

3 answers are given. The answers contain the address of the websites and dns servers that are queried from. 104.20.1.85 and 104.20.0.85 are returned from cloudflare.

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?

```
68 21:53:55.453749 104.20.1.85    139.179.202.36   TCP   66 http(80) → 58933 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400 SACK_PERM=1 WS=1024
```

SYN, ACK destination is 104.20.1.85, same address from before.

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

```
 51 21:53:55.097468 139.179.202.36  139.179.30.24   DNS   72 Standard query 0xfeb3 A www.ietf.org
 66 21:53:55.442817 139.179.30.24   139.179.202.36  DNS   239 Standard query response 0xfeb3 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.20.1.85 A 104.20.0.85 NS ns3.cl…
178 21:53:56.212656 139.179.202.36  139.179.30.24   DNS   79 Standard query 0xff8c A clients4.google.com
179 21:53:56.213727 139.179.30.24   139.179.202.36  DNS   119 Standard query response 0xff8c A clients4.google.com CNAME clients.l.google.com A 172.217.169.206
399 21:53:56.568523 139.179.202.36  139.179.30.24   DNS   87 Standard query 0xce4e A safebrowsing.googleapis.com
400 21:53:56.569695 139.179.30.24   139.179.202.36  DNS   182 Standard query response 0xce4e A safebrowsing.googleapis.com A 216.58.212.10 NS ns2.google.com NS ns3.google.com NS ns4.g…
```

These are all DNS queries. My host does not seem to be issue new DNS queries for each image.

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

DNS query response:

```
▾ User Datagram Protocol, Src Port: 64770 (64770), Dst Port: domain (53)
    Source Port: 64770 (64770)
    Destination Port: domain (53)
```

Destination port is 53. Source is 64770.

Yusuf Ziya Dilek
ID: 21501462
CS-421

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

```
PS C:\Windows\system32> nslookup firat.bcc.bilkent.edu.tr
Server:  manyas.bcc.bilkent.edu.tr
Address:  139.179.30.24
```

```
36 22:24:26.302932 139.179.202.36  139.179.30.24  DNS  94 Standard query 0x0002 A www.mit.edu.dormnet.bilkent.edu.tr
```

DNS query message is sent to my default local DNS server as we can see. 139.179.30.24

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

24.30.179.139.in-addr.arpa: type PTR, class IN

It is type PTR.

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

First response contains only one answer.

15. Provide a screenshot.

No.	Time	Source	Destination	Protocol	Length	Info
33	22:24:26.300558	139.179.202.36	139.179.30.24	DNS	86	Standard query 0x0001 PTR 24.30.179.139.in-addr.arpa
34	22:24:26.301406	139.179.30.24	139.179.202.36	DNS	197	Standard query response 0x0001 PTR 24.30.179.139.in-addr.arpa PTR manyas.bcc.bilkent.edu.tr NS dicle.bcc.bilkent.edu.tr N…
36	22:24:26.302932	139.179.202.36	139.179.30.24	DNS	94	Standard query 0x0002 A www.mit.edu.dormnet.bilkent.edu.tr
37	22:24:26.319385	139.179.30.24	139.179.202.36	DNS	151	Standard query response 0x0002 No such name A www.mit.edu.dormnet.bilkent.edu.tr SOA firat.bcc.bilkent.edu.tr
38	22:24:26.319638	139.179.202.36	139.179.30.24	DNS	94	Standard query 0x0003 AAAA www.mit.edu.dormnet.bilkent.edu.tr
39	22:24:26.321048	139.179.30.24	139.179.202.36	DNS	151	Standard query response 0x0003 No such name AAAA www.mit.edu.dormnet.bilkent.edu.tr SOA firat.bcc.bilkent.edu.tr
40	22:24:26.321318	139.179.202.36	139.179.30.24	DNS	86	Standard query 0x0004 A www.mit.edu.bilkent.edu.tr
41	22:24:26.322723	139.179.30.24	139.179.202.36	DNS	212	Standard query response 0x0004 A www.mit.edu.bilkent.edu.tr A 139.179.10.34 NS dicle.bcc.bilkent.edu.tr NS ns3.bilkent.ed…
42	22:24:26.326591	139.179.202.36	139.179.30.24	DNS	86	Standard query 0x0005 AAAA www.mit.edu.bilkent.edu.tr
43	22:24:26.327854	139.179.30.24	139.179.202.36	DNS	143	Standard query response 0x0005 AAAA www.mit.edu.bilkent.edu.tr SOA firat.bcc.bilkent.edu.tr

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

Destination IP is 139.179.30.24 – which is my default local DNS server.

Yusuf Ziya Dilek
ID: 21501462
CS-421

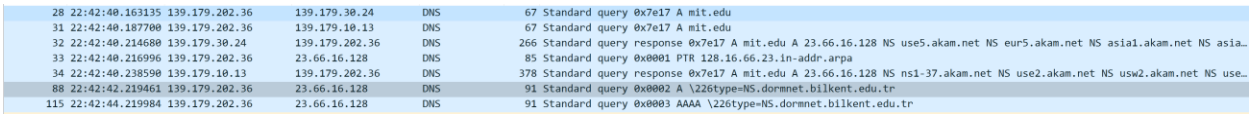
17. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?

Type NS DNS query that contains no answers.

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?

First it asks 139.179.30.24 which is my local DNS server then as a response we get mit.edu 23.66.16.128 address. A standard query is sent to this adress.

19. Provide a screenshot.



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?

It is 18.0.72.3 – it is not my default local DNS server

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

DNS query message type is PTR. Contains no answers.

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

There is no response message here.

23. Provide a screenshot.

Yusuf Ziya Dilek
ID: 21501462
CS-421