CENG 435 - Data Communications and Networking
2023-1
Wireshark Assignment 1

Anıl Eren Göçer
e2448397@ceng.metu.edu.tr

October 18, 2023

---

1. I have sorted my trace file with respect to "Protocol" column in order see clearly. I have seen that my trace file includes the following protocols:

   - DNS
   - HTTP
   - TCP
   - TLSv1.2
   - UDP

   Here are the screenshots, that helped me to detect protocols, from my trace file. I have looked at the "Protocol" column in the following screenshots.

284	3.605871	144.122.4.119	144.122.199.90	DNS	77	Standard query 0x14dd A gaia.cs.umass.edu
285	3.606029	144.122.4.119	144.122.199.90	DNS	77	Standard query 0x3509 HTTPS gaia.cs.umass.edu
291	3.607869	144.122.199.90	144.122.4.119	DNS	93	Standard query response 0x14dd A gaia.cs.umass.edu A 128.119.245.12
292	3.607869	144.122.199.90	144.122.4.119	DNS	130	Standard query response 0x3509 HTTPS gaia.cs.umass.edu SOA unix1.cs.umass.edu

Figure 1: DNS packet samples

323	3.755927	144.122.4.119	128.119.245.12	HTTP	647	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
337	3.909150	128.119.245.12	144.122.4.119	HTTP	293	HTTP/1.1 304 Not Modified

Figure 2: HTTP packet samples

38	0.397408	144.122.4.119	142.251.141.46	TCP	55	50983 → 443 [ACK] Seq=1 Ack=1 Win=256 Len=1 [TCP segment of a reassembled PDU]
41	0.414590	142.251.141.46	144.122.4.119	TCP	66	443 → 50983 [ACK] Seq=1 Ack=2 Win=466 Len=0 SLE=1 SRE=2
142	1.985525	144.122.4.119	35.186.224.25	TCP	55	50958 → 443 [ACK] Seq=1 Ack=1 Win=509 Len=1 [TCP segment of a reassembled PDU]
143	2.005490	35.186.224.25	144.122.4.119	TCP	66	443 → 50958 [ACK] Seq=1 Ack=2 Win=1021 Len=0 SLE=1 SRE=2

Figure 3: TCP packet samples

193	2.814580	144.122.4.119	35.186.224.25	TLSv1.2	2005	Application Data
201	2.833453	35.186.224.25	144.122.4.119	TLSv1.2	93	Application Data
207	2.892629	35.186.224.25	144.122.4.119	TLSv1.2	121	Application Data
208	2.892629	35.186.224.25	144.122.4.119	TLSv1.2	299	Application Data
209	2.892629	35.186.224.25	144.122.4.119	TLSv1.2	318	Application Data

Figure 4: TLSv1.2 packet samples

1	0.000000	144.122.226.246	144.122.227.255	UDP	62	2008 → 2008 Len=20
2	0.001072	144.122.226.246	144.122.227.255	UDP	62	2007 → 2007 Len=20
9	0.116027	144.122.226.246	144.122.227.255	UDP	62	2008 → 2008 Len=20
10	0.117104	144.122.226.246	144.122.227.255	UDP	62	2007 → 2007 Len=20
16	0.217531	144.122.226.246	144.122.227.255	UDP	62	2008 → 2008 Len=20
17	0.218591	144.122.226.246	144.122.227.255	UDP	62	2007 → 2007 Len=20

Figure 5: UDP packet samples

2. I have calculated the time passed between sending HTTP request and HTTP response by subtracting the time request was sent from the time the response was received.

No.	Time	Source	Destination	Protocol	Length	Info
323	3.755927	144.122.4.119	128.119.245.12	HTTP	647	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
337	3.909150	128.119.245.12	144.122.4.119	HTTP	293	HTTP/1.1 304 Not Modified

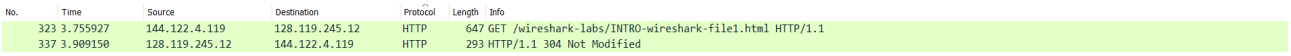
Figure 6: HTTP GET request and HTTP OK response

By looking at the "Time" column, we obtain $t_{sent} = 3.755927$ seconds and $t_{received} = 3.909150$ seconds.

$$t_{passed} = t_{received} - t_{sent} = 0.153223 \text{ seconds}$$

If we round it, we get 0.153 seconds.

3. The packet with no 323 is the request which is sent from my computer to the server and the packet with 337 is the response sent from the servers to my computer. (Please, look at "No" column in the below figure.)



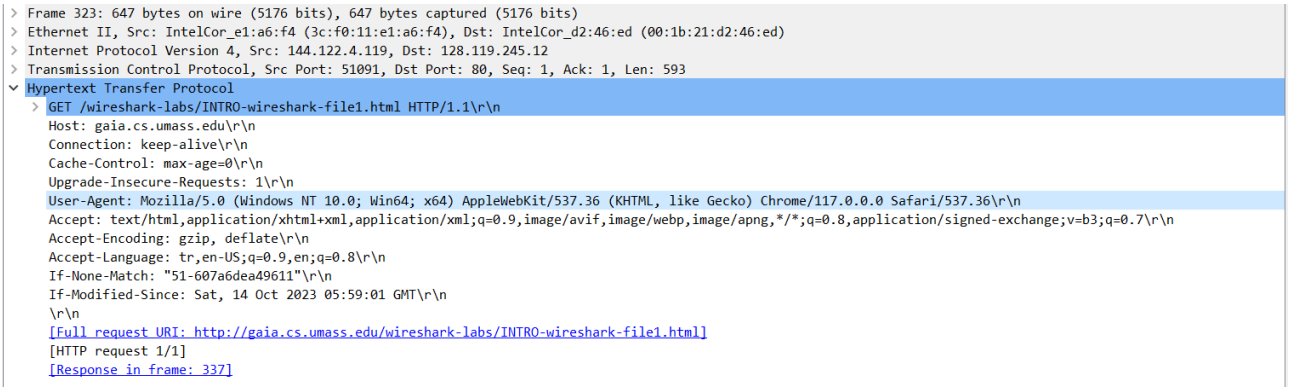
No.	Time	Source	Destination	Protocol	Length	Info
323	3.755927	144.122.4.119	128.119.245.12	HTTP	647	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
337	3.909150	128.119.245.12	144.122.4.119	HTTP	293	HTTP/1.1 304 Not Modified

Figure 7: HTTP GET request and HTTP OK response

Therefore, for the packet with no 323, my computer is source and the server is the destination. For the packet with no 337, my computer is destination and the server is source. By looking at the "Source" and "Destination" columns, I understood that:

Internet address of gaia.cs.umass.edu: 128.119.245.12
Internet address of my computer: 144.122.4.119

4. In order to learn type of Web browser issued the HTTP request, I used the Hypertext Transfer Protocol section of the HTTP GET request (packet with no 323).



```
> Frame 323: 647 bytes on wire (5176 bits), 647 bytes captured (5176 bits)
> Ethernet II, Src: IntelCor_e1:a6:f4 (3c:f0:11:e1:a6:f4), Dst: IntelCor_d2:46:ed (00:1b:21:d2:46:ed)
> Internet Protocol Version 4, Src: 144.122.4.119, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 51091, Dst Port: 80, Seq: 1, Ack: 1, Len: 593
v 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
    Cache-Control: max-age=0\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/117.0.0.0 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,application/signed-exchange;v=b3;q=0.7\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: tr,en-US;q=0.9,en;q=0.8\r\n
    If-None-Match: "51-607a6dea49611"\r\n
    If-Modified-Since: Sat, 14 Oct 2023 05:59:01 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: 337]
```

Figure 8: Hypertext Transfer Protocol details

I looked at the User-Agent information. It includes the value **Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/117.0.0.0 Safari/537.36**. In the beginning, I was confused since this value includes multiple browser names although I used Google Chrome to send this request. Then, I referred to the following source:

https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/User-Agent

As a result, I confirmed that this value corresponds to Chrome which is my browser.

Hence, the browser type that issued the HTTP request is **Chrome** (corresponds to "None of these answers." option in the quiz).

5. In order to find out destination port number, I looked at details of Transmission Control Protocol segment carrying this HTTP request (packet with no 323). There was a information **"Destination Port"** and it has value **80**.

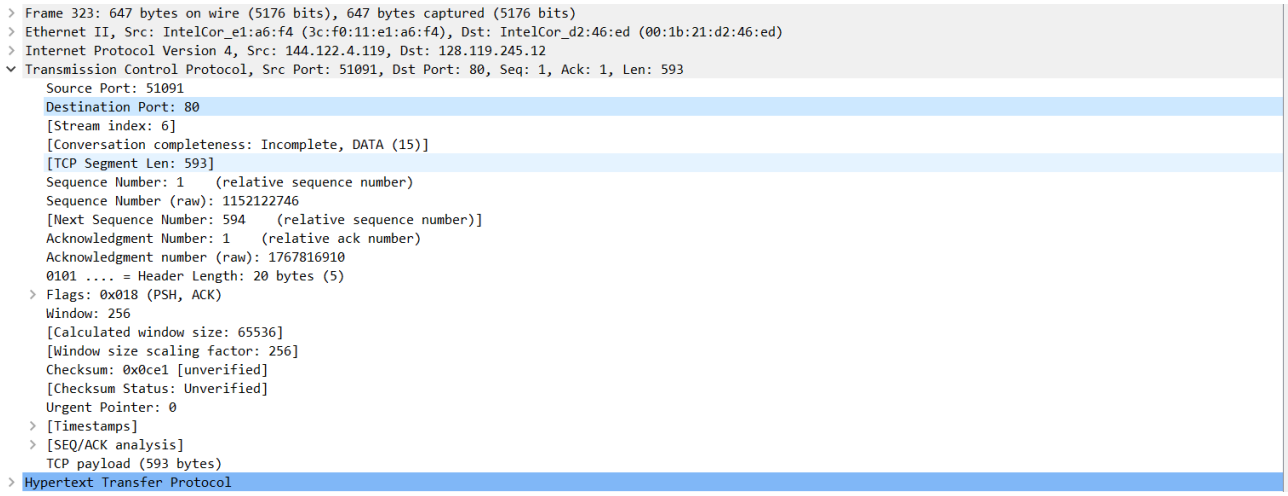


Figure 9: Transmission Control Protocol details

Hence, the destination port number was **80**.