Wireshark intro answers
Author: golan matuf date: 14.11.2021

1:

The client ip is 192.168.1.72

Source	Destination	Protocol	Length	Info
192.168.1.72	192.168.1.254	DNS	85	Standard query 0x5197 A www.wire

2:

Dns server ip is 192.168.1.254

Source	Destination	Protocol	Length	Info
192.168.1.254	192.168.1.72	DNS	145	Standard query response 0x5197 A www.wiresha

3:

The dns response time is 0.256361

Time	Source	Destination	Protocol	Length	Info
0.000000	192.168.1.72	192.168.1.254	DNS	85	Standard query 0x5197 A www.
0.256361	192.168.1.254	192.168.1.72	DNS	145	Standard query response 0x51

4:

This trace was taken Closer to the client because we see the largest gap is while waiting to the server response. While the client response is faster

Time	Source	Destination	Protocol	Length	Info
4.095223	192.168.1.72	98.136.187.13	TCP	66	6128 → 80 [SYN]
4.095921	192.168.1.72	98.136.187.13	TCP	66	6129 → 80 [SYN]
4.144822	98.136.187.13	192.168.1.72	TCP	66	80 → 6128 [SYN,
4.145175	192.168.1.72	98.136.187.13	TCP	54	6128 → 80 [ACK]
4.145956	98.136.187.13	192.168.1.72	TCP	66	80 → 6129 [SYN,
4.146032	192.168.1.72	98.136.187.13	TCP	54	6129 → 80 [ACK]
4.156320	192.168.1.72	98.136.187.13	HTTP	322	GET / HTTP/1.1
4.203964	98.136.187.13	192.168.1.72	TCP	60	80 → 6128 [ACK]
4.212728	98.136.187.13	192.168.1.72	TCP	1514	80 → 6128 [ACK]

Wireshark intro answers
Author: golan matuf date: 14.11.2021

5:

Connected to 92.136.189.13 and 98.139.206.151 succesfuly

But in the end failed with the 92.136.189.13 one

Time	Source	Destination	Protocol	Length	Info
4.261482	98.136.187.13	192.168.1.72	HTTP	358	HTTP/1.1 200 OK (text/html)
5.649275	98.136.187.13	192.168.1.72	HTTP	792	HTTP/1.1 200 OK (PNG)
5.660720	98.136.187.13	192.168.1.72	HTTP	1166	HTTP/1.1 200 OK (JPEG JFIF image)
5.753769	98.136.187.13	192.168.1.72	HTTP	763	HTTP/1.1 200 OK (JPEG JFIF image)
5.802039	98.136.187.13	192.168.1.72	HTTP	72	HTTP/1.1 200 OK (JPEG JFIF image)
6.051696	98.136.187.13	192.168.1.72	HTTP	1055	HTTP/1.1 200 OK (text/css)
7.351740	98.136.187.13	192.168.1.72	HTTP	67	HTTP/1.1 200 OK (PNG)
7.353156	98.136.187.13	192.168.1.72	HTTP	376	HTTP/1.1 200 OK (PNG)
7.367530	98.136.187.13	192.168.1.72	HTTP	377	HTTP/1.1 200 OK (PNG)
7.502918	98.139.206.151	192.168.1.72	HTTP	343	HTTP/1.0 200 OK (GIF89a)
7.645942	98.136.187.13	192.168.1.72	HTTP	104	HTTP/1.1 200 OK (JPEG JFIF image)
8.111023	98.136.187.13	192.168.1.72	HTTP	548	HTTP/1.1 404 Not Found (text/html)

6:

www.wiresharktraining.com

```
Standard query 0x5197 A www.wiresharktraining.com
Standard query response 0x5197 A www.wiresharktraining.com CNAME sbsfe-p10.geo.mf0.yahoodns.net A 98.136.187.13
```

7:

8 total syn packet were sent by the client

tcp && ip.src == 192.168.1.72 && tcp.flags.syn == 1

No.	Time	Source	Destination	Protocol	Length	Info
3	4.095223	192.168.1.72	98.136.187.13	TCP	66	6128 → 80 [SYN] Seq=0 Wi
4	4.095921	192.168.1.72	98.136.187.13	TCP	66	6129 → 80 [SYN] Seq=0 Wi
22	5.553402	192.168.1.72	98.136.187.13	TCP	66	6130 → 80 [SYN] Seq=0 Wi
23	5.553690	192.168.1.72	98.136.187.13	TCP	66	6131 → 80 [SYN] Seq=0 Wi
91	7.283422	192.168.1.72	98.139.206.151	TCP	66	6136 → 80 [SYN] Seq=0 Wi
92	7.283422	192.168.1.72	98.139.206.151	TCP	66	6135 → 80 [SYN] Seq=0 Wi
234	8.008141	192.168.1.72	98.136.187.13	TCP	66	6141 → 80 [SYN] Seq=0 Wi
235	8.008738	192.168.1.72	98.136.187.13	TCP	66	6140 → 80 [SYN] Seq=0 Wi

8:

The first dns request www.wiresharktraining.com

9:

Only error code 40 showed up

http.response.code!=200

	Time	Source	Destination	Protocol	Length	Info
242	8.111023	98.136.187.13	192.168.1.72	HTTP	548	HTTP/1.1 404 Not Found (text/html)

Wireshark intro answers
Author: golan matuf date: 14.11.2021

10:

404 couldn't find favicon.ico

Wireshark · Follow HTTP Stream (tcp.stream eq 7) · wwb001-http.pcapng

```
GET /favicon.ico HTTP/1.1
Accept: */*
UA-CPU: AMD64
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko
Host: www.wiresharktraining.com
DNT: 1
Connection: Keep-Alive
Cookie: BX=bh6dgsp87hbvb&b=3&s=8s

HTTP/1.1 404 Not Found
Date: Sun, 23 Feb 2014 21:03:35 GMT
P3P: policyref="http://info.yahoo.com/w3c/p3p.xml", CP="CAO DSP COR CUR ADM DEV TAI PSA
UNRi PUBi IND PHY ONL UNI PUR FIN COM NAV INT DEM CNT STA POL HEA PRE LOC GOV"
Content-Type: text/html; charset=iso-8859-1
Age: 0
Transfer-Encoding: chunked
Connection: keep-alive
Server: YTS/1.20.28

<h1 style='color:#497A97;font-size:12pt;font-weight:bold'>404 - Not Found
```

11:

The client opened port 6128 to communicate with the HTTP server

tcp.stream eq 0

	Time	Source	Destination	Protocol	Length	Info
3	4.095223	192.168.1.72	98.136.187.13	TCP	66	6128 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SA
5	4.144822	98.136.187.13	192.168.1.72	TCP	66	80 → 6128 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=14
6	4.145175	192.168.1.72	98.136.187.13	TCP	54	6128 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
9	4.156320	192.168.1.72	98.136.187.13	HTTP	322	GET / HTTP/1.1
10	4.203964	98.136.187.13	192.168.1.72	TCP	60	80 → 6128 [ACK] Seq=1 Ack=269 Win=6912 Len=0
11	4.212728	98.136.187.13	192.168.1.72	TCP	1514	80 → 6128 [ACK] Seq=1 Ack=269 Win=6912 Len=1460 [TCP s
12	4.213112	192.168.1.72	98.136.187.13	TCP	54	6128 → 80 [ACK] Seq=269 Ack=1461 Win=65700 Len=0
13	4.213932	98.136.187.13	192.168.1.72	TCP	1514	80 → 6128 [ACK] Seq=1461 Ack=269 Win=6912 Len=1460 [TC