Name: Yehuda Gurovich I.D.: 44184491

בס"ד

Date: 5/5/2024

Advanced Computer Networks – רשתות מחשבים מתקדם

Laboratory 01 - Wireshark Exercise:

Image for 1-3:

dns

	Time	Source	Destination	Protocol
1	0.000000	192.168.1.72	192.168.1.254	DNS
2	0.256361	192.168.1.254	192.168.1.72	DNS

1. **What is the IP address of the DNS/HTTP client in the trace file *wwb001-http.pcapng*?**

   192.168.1.72

2. **What is the IP address of the DNS server?**

   192.168.1.254

3. **What DNS response time is seen in the trace file?**

   0.256361 seconds

4. **Do you think that this trace was taken (captured) closer to the HTTP client or closer to the HTTP server?**

   Closer to the server. We can see in time from previous packet mode that the time between 2 packets from same source to destination is generally smaller in the server.

17	0.000840	98.136.187.13	192.168.1.72	TCP
18	0.000004	98.136.187.13	192.168.1.72	HTTP
19	0.000675	192.168.1.72	98.136.187.13	TCP
20	1.290603	192.168.1.72	98.136.187.13	HTTP
21	0.000451	192.168.1.72	98.136.187.13	HTTP
22	0.000191	192.168.1.72	98.136.187.13	TCP
23	0.000288	192.168.1.72	98.136.187.13	TCP
24	0.046317	98.136.187.13	192.168.1.72	TCP
25	0.000461	192.168.1.72	98.136.187.13	TCP
26	0.001578	98.136.187.13	192.168.1.72	TCP
27	0.000875	98.136.187.13	192.168.1.72	TCP
28	0.000011	98.136.187.13	192.168.1.72	TCP
29	0.000004	98.136.187.13	192.168.1.72	TCP
30	0.002033	192.168.1.72	98.136.187.13	TCP
31	0.000092	192.168.1.72	98.136.187.13	TCP
32	0.000909	192.168.1.72	98.136.187.13	HTTP

Homework:

5. **What are the IP addresses of the HTTP servers to which the client successfully connected?**

   - 98.136.187.13
   - 98.139.206.151

tcp && ip.src==192.168.1.72

o.	Time	Source	Destination	Protocol	Len
80	0.000306	192.168.1.72	98.136.187.13	TCP	
81	0.192122	192.168.1.72	98.136.187.13	HTTP	
83	0.000316	192.168.1.72	98.136.187.13	TCP	
86	0.000185	192.168.1.72	98.136.187.13	TCP	
90	0.000128	192.168.1.72	98.136.187.13	TCP	
91	1.231598	192.168.1.72	98.139.206.151	TCP	
92	0.000000	192.168.1.72	98.139.206.151	TCP	
93	0.018994	192.168.1.72	98.136.187.13	HTTP	
94	0.000593	192.168.1.72	98.136.187.13	HTTP	
95	0.000577	192.168.1.72	98.136.187.13	HTTP	
96	0.000650	192.168.1.72	98.136.187.13	HTTP	
98	0.000330	192.168.1.72	98.136.187.13	TCP	
101	0.000606	192.168.1.72	98.136.187.13	TCP	
106	0.001113	192.168.1.72	98.136.187.13	TCP	
107	0.000044	192.168.1.72	98.136.187.13	TCP	
110	0.000164	192.168.1.72	98.136.187.13	TCP	
112	0.000308	192.168.1.72	98.136.187.13	TCP	
115	0.000756	192.168.1.72	98.136.187.13	TCP	
117	0.000167	192.168.1.72	98.139.206.151	TCP	
118	0.000718	192.168.1.72	98.139.206.151	HTTP	
120	0.000140	192.168.1.72	98.139.206.151	TCP	
122	0.000201	192.168.1.72	98.136.187.13	TCP	

We see the 2 different destination addresses.

6. **What are the HTTP host names of the target HTTP servers?**

   - http://www.wiresharktraining.com/
   - http://visit.webhosting.yahoo.com/visit.gif?&r=&b=Netscape%205.0%20%28Windows%20NT%206.1%3B%20WOW64%3B%20Trident/7.0%3B%20SLCC2%3B%20.NET%20CLR%202.0.50727%3B%20.NET%20CLR%203.5.30729%3B%20.NET%20CLR%203.0.307]

   Checking the HTTP packets from the 2 different sources in question 5 we obtain these 2 host names.

7. **How many TCP SYN packets did the client send to the HTTP servers?**

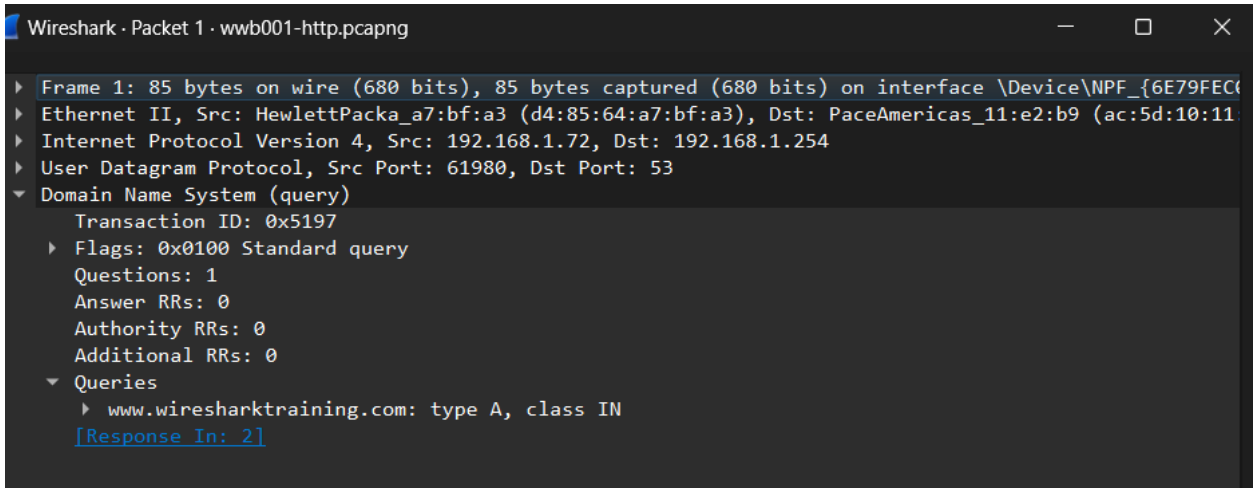
   8

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

o.	Time	Source	Destination	Protocol	Length	Info
3	3.838862	192.168.1.72	98.136.187.13	TCP	66	6128 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM
4	0.000698	192.168.1.72	98.136.187.13	TCP	66	6129 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM
22	0.000191	192.168.1.72	98.136.187.13	TCP	66	6130 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM
23	0.000288	192.168.1.72	98.136.187.13	TCP	66	6131 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM
91	1.231598	192.168.1.72	98.139.206.151	TCP	66	6136 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM
92	0.000000	192.168.1.72	98.139.206.151	TCP	66	6135 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM
234	0.362137	192.168.1.72	98.136.187.13	TCP	66	6141 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM
235	0.000597	192.168.1.72	98.136.187.13	TCP	66	6140 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM

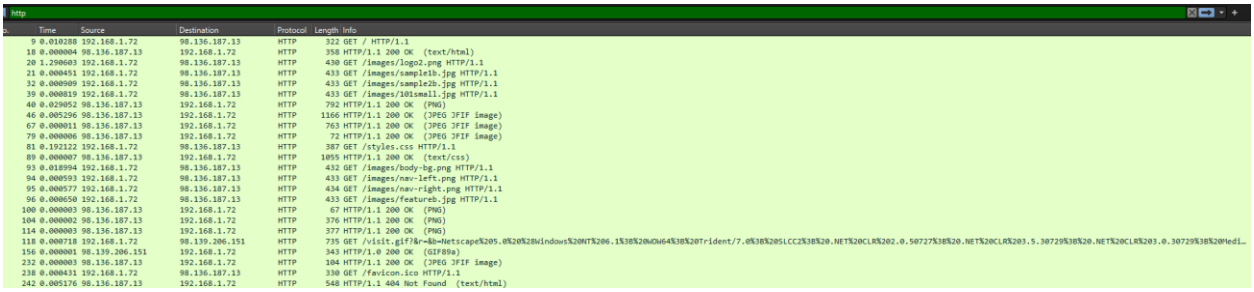
8. **What Uniform Resource Identifier (URI) does the client request first in this trace file?**

   http://www.wiresharktraining.com/



9. **What HTTP error response(s) are seen in this trace file?**

    - 200 OK
    - 404 Not Found



#	Time	Source	Destination	Protocol	Length	Info
9	0.010288	192.168.1.72	98.136.187.13	HTTP	322	GET / HTTP/1.1
18	0.000004	98.136.187.13	192.168.1.72	HTTP	358	HTTP/1.1 200 OK (text/html)
20	1.290603	192.168.1.72	98.136.187.13	HTTP	430	GET /images/logo2.png HTTP/1.1
21	0.000451	192.168.1.72	98.136.187.13	HTTP	433	GET /images/sample1b.jpg HTTP/1.1
32	0.000909	192.168.1.72	98.136.187.13	HTTP	433	GET /images/sample2b.jpg HTTP/1.1
39	0.000819	192.168.1.72	98.136.187.13	HTTP	433	GET /images/101small.jpg HTTP/1.1
40	0.029052	98.136.187.13	192.168.1.72	HTTP	792	HTTP/1.1 200 OK (PNG)
46	0.005296	98.136.187.13	192.168.1.72	HTTP	1166	HTTP/1.1 200 OK (JPEG JFIF image)
67	0.000011	98.136.187.13	192.168.1.72	HTTP	763	HTTP/1.1 200 OK (JPEG JFIF image)
79	0.000006	98.136.187.13	192.168.1.72	HTTP	72	HTTP/1.1 200 OK (JPEG JFIF image)
81	0.192122	192.168.1.72	98.136.187.13	HTTP	387	GET /styles.css HTTP/1.1
89	0.000007	98.136.187.13	192.168.1.72	HTTP	1055	HTTP/1.1 200 OK (text/css)
93	0.018994	192.168.1.72	98.136.187.13	HTTP	432	GET /images/body-bg.png HTTP/1.1
94	0.000593	192.168.1.72	98.136.187.13	HTTP	433	GET /images/nav-left.png HTTP/1.1
95	0.000577	192.168.1.72	98.136.187.13	HTTP	434	GET /images/nav-right.png HTTP/1.1
96	0.000650	192.168.1.72	98.136.187.13	HTTP	433	GET /images/featureb.jpg HTTP/1.1
100	0.000003	98.136.187.13	192.168.1.72	HTTP	67	HTTP/1.1 200 OK (PNG)
104	0.000002	98.136.187.13	192.168.1.72	HTTP	376	HTTP/1.1 200 OK (PNG)
114	0.000003	98.136.187.13	192.168.1.72	HTTP	377	HTTP/1.1 200 OK (PNG)
118	0.000718	192.168.1.72	98.139.206.151	HTTP	735	GET /visit.gif?&r=&b=Netscape%205.0%20%28Windows%20NT%206.1%38%20WOW64%38%20Trident/7.0%3B%20SLCC2%38%20.NET%20CLR%202.0.50727%3B%20.NET%20CLR%203.5.30729%3B%20.NET%20CLR%203.0.30729%3B%20Medi…
156	0.000001	98.139.206.151	192.168.1.72	HTTP	343	HTTP/1.0 200 OK (GIF89a)
232	0.000003	98.136.187.13	192.168.1.72	HTTP	104	HTTP/1.1 200 OK (JPEG JFIF image)
238	0.000431	192.168.1.72	98.136.187.13	HTTP	330	GET /favicon.ico HTTP/1.1
242	0.005176	98.136.187.13	192.168.1.72	HTTP	548	HTTP/1.1 404 Not Found (text/html)

10. **What requested web object could not be found on the HTTP server?**

    As we see in the bottom of the image in question 9 we see the GET request to http://www.wiresharktraining.com/favicon.ico gets a response of 404 Not Found

11. **What TCP port numbers did the client open to communicate with the HTTP server?**

    - 6128
    - 6129
    - 6130
    - 6131
    - 6136
    - 6140

```
▸ Internet Protocol Version 4, Src: 192.168.1.72, Dst: 98.136.187.13
▾ Transmission Control Protocol, Src Port: 6128, Dst Port: 80, Seq: 269, Ack: 6145, Len: 0
    Source Port: 6128
    Destination Port: 80
    [Stream index: 0]
  ▸ [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 0]
    Sequence Number: 269    (relative sequence number)
    Sequence Number (raw): 611442013
    [Next Sequence Number: 269    (relative sequence number)]
    Acknowledgment Number: 6145    (relative ack number)
    Acknowledgment number (raw): 581500344
    0101 .... = Header Length: 20 bytes (5)
  ▸ Flags: 0x010 (ACK)
    Window: 16425
    [Calculated window size: 65700]
    [Window size scaling factor: 4]
    Checksum: 0xdfa0 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  ▸ [Timestamps]
  ▸ [SEQ/ACK analysis]
```

We go over all the TCP packets where the source is the client and check the different opened ports

12. What TCP options are supported by the client?

- MSS
- Window scale
- SACK permitted

```
Wireshark · Packet 23 · wwb001-http.pcapng
▸ Frame 23: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{6E79FEC0-FF79-4970-96E4-EEFF300A9B9F}, id 0
▸ Ethernet II, Src: HewlettPacka_a7:bf:a3 (d4:85:64:a7:bf:a3), Dst: PaceAmericas_11:e2:b9 (ac:5d:10:11:e2:b9)
▸ Internet Protocol Version 4, Src: 192.168.1.72, Dst: 98.136.187.13
▾ Transmission Control Protocol, Src Port: 6131, Dst Port: 80, Seq: 0, Len: 0
    Source Port: 6131
    Destination Port: 80
    [Stream index: 3]
  ▸ [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 345071414
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 0
    Acknowledgment number (raw): 0
    1000 .... = Header Length: 32 bytes (8)
  ▾ Flags: 0x002 (SYN)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Accurate ECN: Not set
      .... 0... .... = Congestion Window Reduced: Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...0 .... = Acknowledgment: Not set
      .... .... 0... = Push: Not set
      .... .... .0.. = Reset: Not set
    ▸ .... .... ..1. = Syn: Set
      .... .... ...0 = Fin: Not set
      [TCP Flags: ······· S ·]
    Window: 8192
    [Calculated window size: 8192]
    Checksum: 0xdfac [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  ▾ Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), SACK permitted
    ▸ TCP Option - Maximum segment size: 1460 bytes
    ▸ TCP Option - No-Operation (NOP)
    ▸ TCP Option - Window scale: 2 (multiply by 4)
    ▸ TCP Option - No-Operation (NOP)
    ▸ TCP Option - No-Operation (NOP)
    ▸ TCP Option - SACK permitted
  ▸ [Timestamps]
```

We see at the bottom the options that are available.

13. What words are seen in the featureb.jpg image?

Get Deep

14. What is the average throughput rate (bits per second) in this trace file?

37k bits/second as we see below, from statistics -> Capture Files Properties.

Statistics

Measurement	Captured	Displayed	Marked
Packets	273	273 (100.0%)	—
Time span, s	38.351	38.351	—
Average pps	7.1	7.1	—
Average packet size, B	662	662	—
Bytes	180655	180655 (100.0%)	0
Average bytes/s	4710	4710	—
Average bits/s	37 k	37 k	—

15. How many UDP streams are in the trace file?

0 because there are no handshakes established with UDP protocol

16. What is the purpose of TCP stream 7?

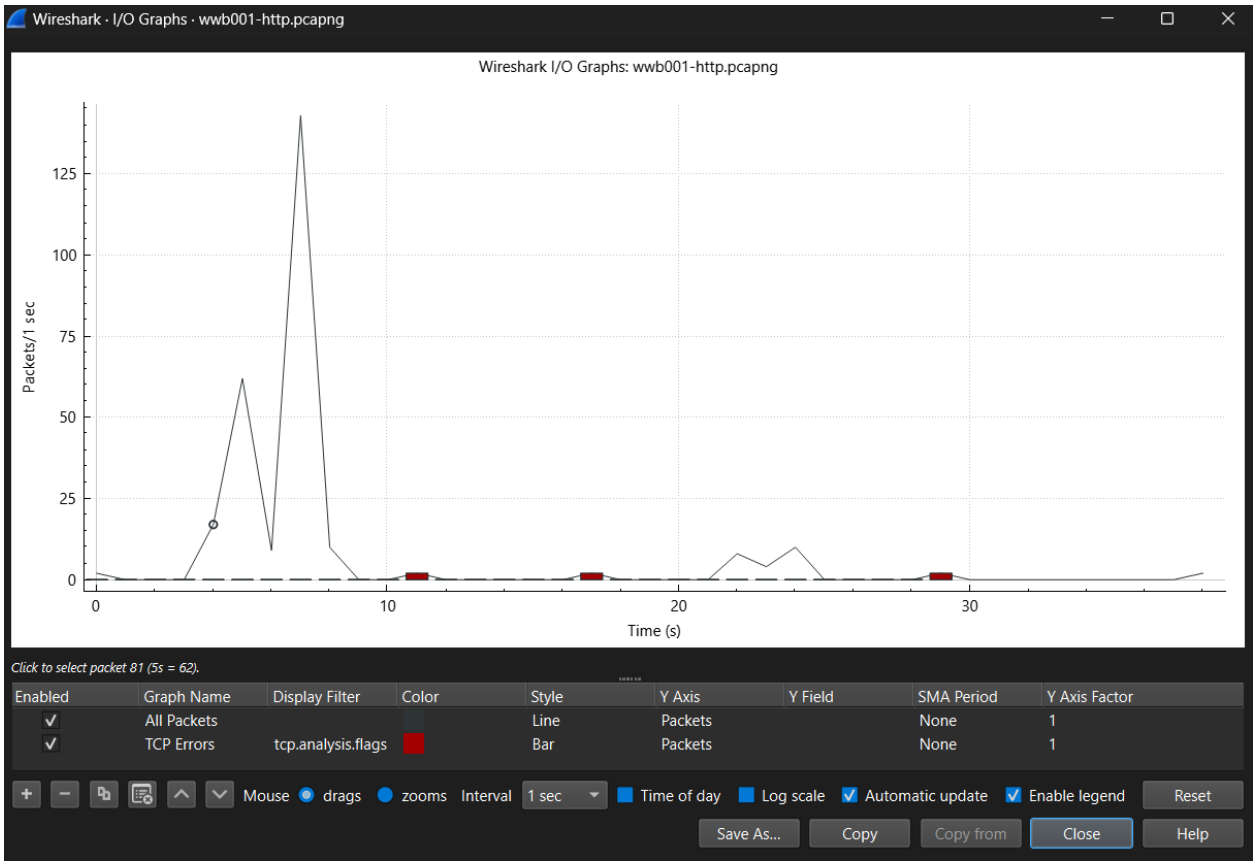
tcp.stream eq 7

No.	Time	Source	Destination	Protocol	Length	Info
235	8.008738	192.168.1.72	98.136.187.13	TCP	66	6140 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM
236	8.057195	98.136.187.13	192.168.1.72	TCP	66	80 → 6140 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM WS=256
237	8.057639	192.168.1.72	98.136.187.13	TCP	54	6140 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
238	8.058070	192.168.1.72	98.136.187.13	HTTP	330	GET /favicon.ico HTTP/1.1
241	8.105847	98.136.187.13	192.168.1.72	TCP	60	80 → 6140 [ACK] Seq=1 Ack=277 Win=6912 Len=0
242	8.111023	98.136.187.13	192.168.1.72	HTTP	548	HTTP/1.1 404 Not Found (text/html)
243	8.111276	192.168.1.72	98.136.187.13	TCP	54	6140 → 80 [ACK] Seq=277 Ack=495 Win=65204 Len=0
256	23.109916	98.136.187.13	192.168.1.72	TCP	60	80 → 6140 [FIN, ACK] Seq=495 Ack=277 Win=6912 Len=0
257	23.110012	192.168.1.72	98.136.187.13	TCP	54	6140 → 80 [ACK] Seq=277 Ack=496 Win=65204 Len=0
272	38.351045	192.168.1.72	98.136.187.13	TCP	54	6140 → 80 [RST, ACK] Seq=277 Ack=496 Win=0 Len=0

It's a GET request to http://www.wiresharktraining.com/favicon.ico but it gets a response HTTP message of 404 Not Found

17. How many times does the packets per second rate reach over 125 in this trace file?

1 time. We can see that in the graph below that the 125 packets/s gets crossed only once.


Wireshark · I/O Graphs · wwb001-http.pcapng
Wireshark I/O Graphs: wwb001-http.pcapng
Packets/1 sec
125
100
75
50
25
0
0
10
20
30
Time (s)
Click to select packet 81 (5s = 62).
Enabled
Graph Name
Display Filter
Color
Style
Y Axis
Y Field
SMA Period
Y Axis Factor
All Packets
Line
Packets
None
1
TCP Errors
tcp.analysis.flags
Bar
Packets
None
1
Mouse
drags
zooms
Interval
1 sec
Time of day
Log scale
Automatic update
Enable legend
Reset
Save As...
Copy
Copy from
Close
Help