1.what is the ip address of the dns/http client in the trace file?

Answer:

192.168.1.72 same in http and dns , no filter used

1	0.000000	192.168.1.72	192.168.1.254	DNS	85 Standard qu
2	0.256361	192.168.1.254	192.168.1.72	DNS	145 Standard qu
3	4.095223	192.168.1.72	98.136.187.13	TCP	66 6128 → 80 [
4	4.095921	192.168.1.72	98.136.187.13	TCP	66 6129 → 80 [
5	4.144822	98.136.187.13	192.168.1.72	TCP	66 80 → 6128 [
6	4.145175	192.168.1.72	98.136.187.13	TCP	54 6128 → 80 [
7	4.145956	98.136.187.13	192.168.1.72	TCP	66 80 → 6129 [
8	4.146032	192.168.1.72	98.136.187.13	TCP	54 6129 → 80 [
9	4.156320	192.168.1.72	98.136.187.13	HTTP	322 GET / HTTP/

2. what is the ip address of the dns server?

Answer:

192.168.1.254, filter used: dns

1	0.000000	192.168.1.72	192.168.1.254	DNS	85 Standard qu
2	0.256361	192.168.1.254	192.168.1.72	DNS	145 Standard qu

3.what dns response time is seen in this trace file?

Answer:

0.256361 seconds, filter used: dns

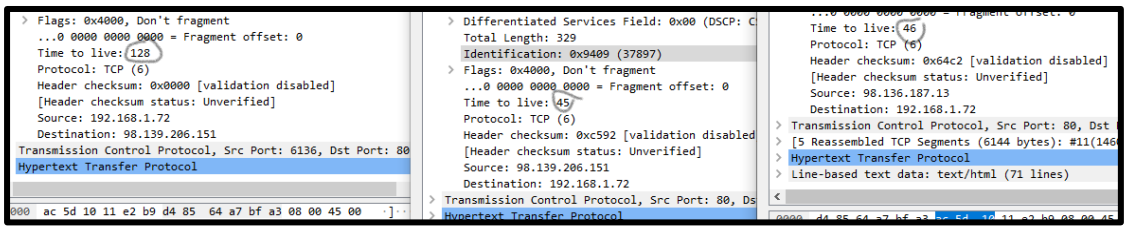
```
[Time delta from previous captured frame: 0.256361000 seconds]
[Time delta from previous displayed frame: 0.256361000 seconds]
[Time since reference or first frame: 0.256361000 seconds]
```

1	0.000000	192.168.1.72	192.168.1.254	DNS
2	0.256361	192.168.1.254	192.168.1.72	DNS

4.Do you think this trace was taken closer to the http client or closer to the http servers?

Answer:

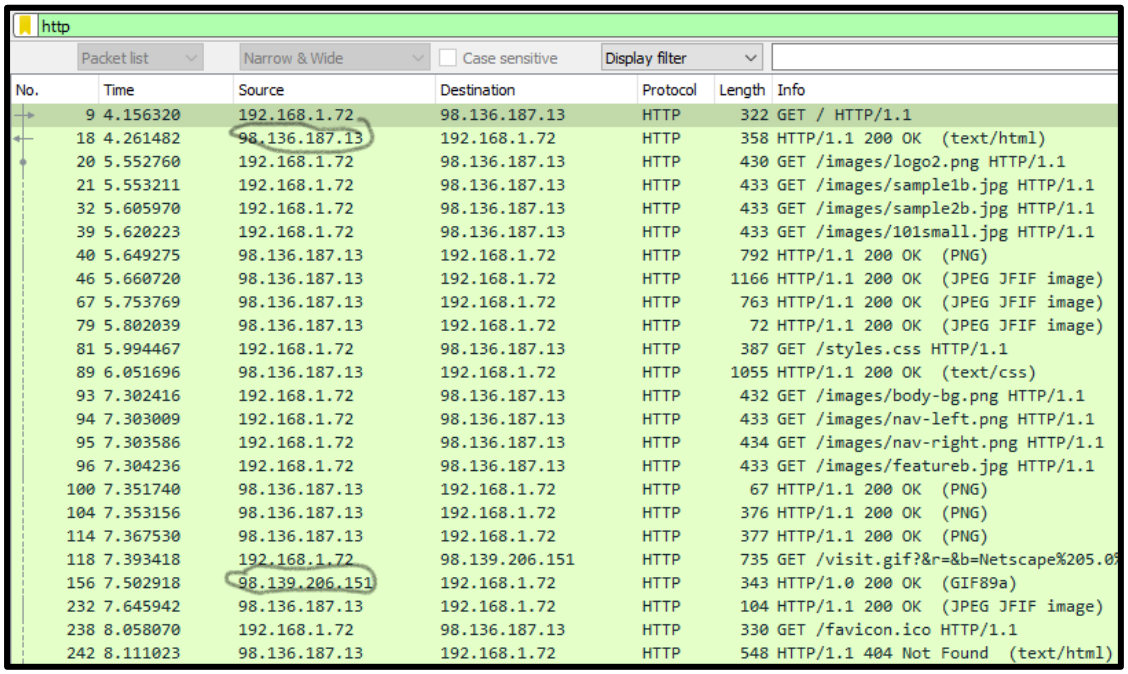
http client was taken closer, the TTL of the client is higher 128 then the servers which are 45 and 46, filter used :http



5. what are the IP addresses of the http servers to which the client successfully connected?

Answer:

98.136.187.13 and 98.139.206.151 (filter shown in screenshot)

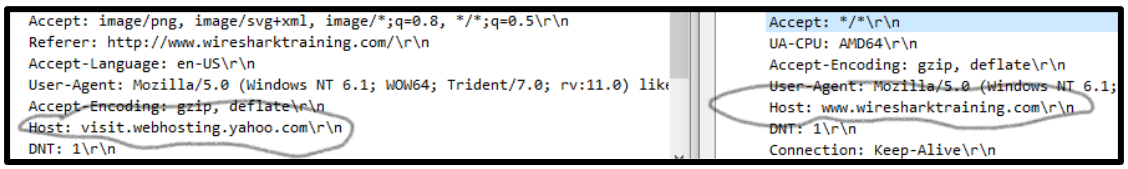


6. what are the http host names of the target http servers?

Answer:

visit.webhosting.yahoo.com\r\n (98.139.206.151)

www.wiresharktraining.com\r\n (98.136.187.13), filter used: http.host

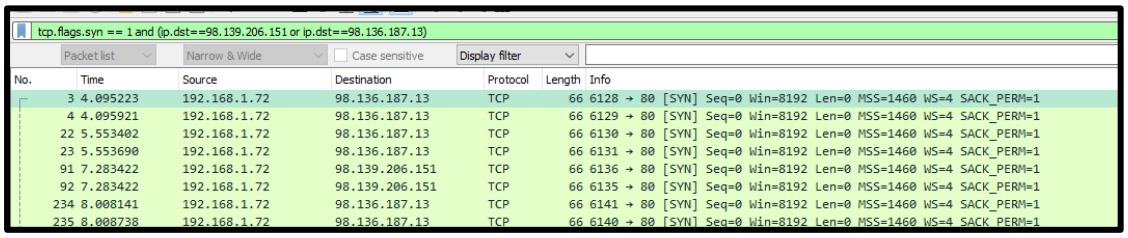


7.how many tcp syn packet did the client send to the http servers?

Answer:

8

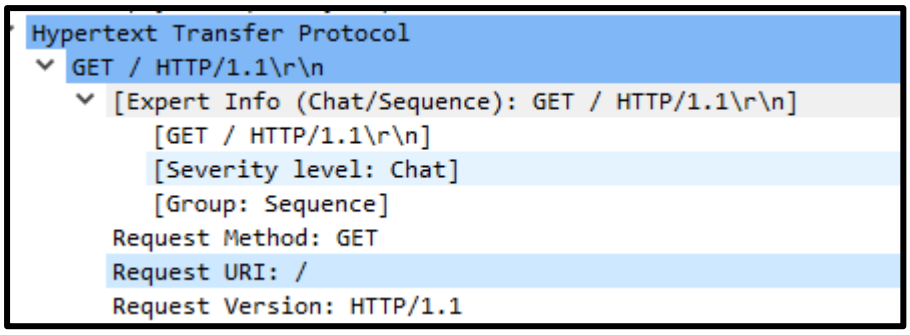
(filter used are shown in the screenshot I could have also added tcp.flags.ack == 0)



8.what uniform resource identifier (URI) does the client request first in this trace file?

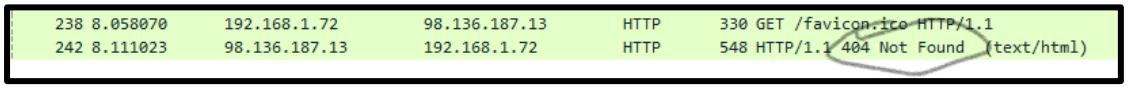
Answer:

HTTP/1.1\r\n, filter used: http



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

404 Not found, filter used: http

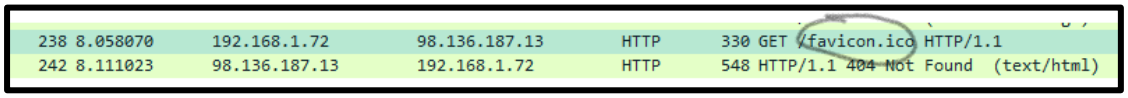


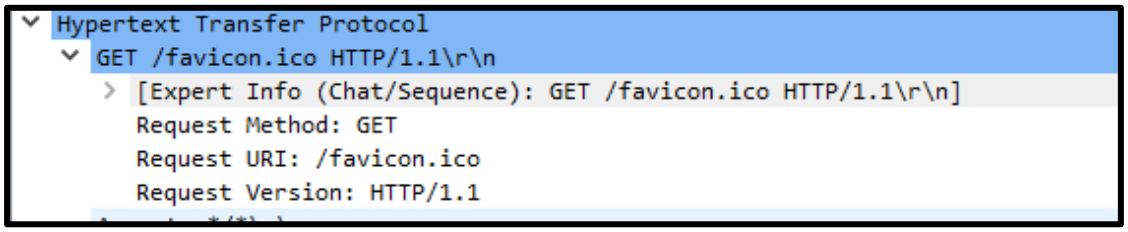
Answer:

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

Answer:

favicon.ico, filter used: http

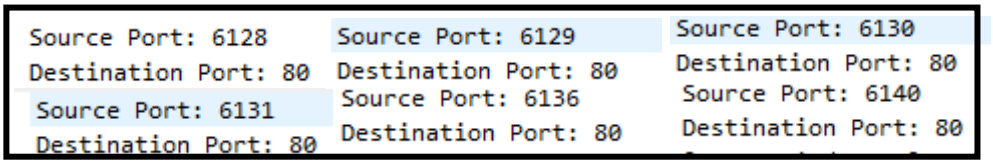




11.what TCP port numbers did the client open to communicate with the HTTP server

Answer:

6128, 6129, 6130, 6131, 6136, 6140, filter used: http



תודה לבדיקה!