

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

| Time       | Source        | Destination   | Protocol | Length | Info                    |
|------------|---------------|---------------|----------|--------|-------------------------|
| 1 0.000000 | 192.168.1.72  | 192.168.1.254 | DNS      | 85     | Standard query          |
| 2 0.256361 | 192.168.1.254 | 192.168.1.72  | DNS      | 145    | Standard query response |
| 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

| Time       | Source        | Destination   | Protocol | Length | Info                    |
|------------|---------------|---------------|----------|--------|-------------------------|
| 1 0.000000 | 192.168.1.72  | 192.168.1.254 | DNS      | 85     | Standard query          |
| 2 0.256361 | 192.168.1.254 | 192.168.1.72  | DNS      | 145    | Standard query response |

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]
```

| 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      |

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

> Flags: 0x4000, Don't fragment  
...0 0000 0000 0000 = Fragment offset: 0  
Time to live: 128  
Protocol: TCP (6)  
Header checksum: 0x0000 [validation disabled]  
[Header checksum status: Unverified]  
Source: 192.168.1.72  
Destination: 98.139.206.151  
Transmission Control Protocol, Src Port: 6136, Dst Port: 80  
Hypertext Transfer Protocol

> Differentiated Services Field: 0x00 (DSCP: CS0)  
Total Length: 329  
Identification: 0x9409 (37897)  
> Flags: 0x4000, Don't fragment  
...0 0000 0000 0000 = Fragment offset: 0  
Time to live: 45  
Protocol: TCP (6)  
Header checksum: 0xc592 [validation disabled]  
[Header checksum status: Unverified]  
Source: 98.139.206.151  
Destination: 192.168.1.72  
> Transmission Control Protocol, Src Port: 80, Dst Port: 6136  
Hypertext Transfer Protocol

...0 0000 0000 0000 = Fragment offset: 0  
Time to live: 46  
Protocol: TCP (6)  
Header checksum: 0x64c2 [validation disabled]  
[Header checksum status: Unverified]  
Source: 98.136.187.13  
Destination: 192.168.1.72  
> Transmission Control Protocol, Src Port: 80, Dst Port: 6136  
[5 Reassembled TCP Segments (6144 bytes): #11(146)  
> Hypertext Transfer Protocol  
> Line-based text data: text/html (71 lines)

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)

| No. | Time     | Source         | Destination    | Protocol | Length | Info   |
|-----|----------|----------------|----------------|----------|--------|--|
| 9   | 4.156320 | 192.168.1.72   | 98.136.187.13  | HTTP     | 322    | GET / HTTP/1.1                               |
| 18  | 4.261482 | 98.136.187.13  | 192.168.1.72   | HTTP     | 358    | HTTP/1.1 200 OK (text/html)                  |
| 20  | 5.552760 | 192.168.1.72   | 98.136.187.13  | HTTP     | 430    | GET /images/logo2.png HTTP/1.1               |
| 21  | 5.553211 | 192.168.1.72   | 98.136.187.13  | HTTP     | 433    | GET /images/sample1b.jpg HTTP/1.1            |
| 32  | 5.605970 | 192.168.1.72   | 98.136.187.13  | HTTP     | 433    | GET /images/sample2b.jpg HTTP/1.1            |
| 39  | 5.620223 | 192.168.1.72   | 98.136.187.13  | HTTP     | 433    | GET /images/101small.jpg HTTP/1.1            |
| 40  | 5.649275 | 98.136.187.13  | 192.168.1.72   | HTTP     | 792    | HTTP/1.1 200 OK (PNG)                        |
| 46  | 5.660720 | 98.136.187.13  | 192.168.1.72   | HTTP     | 1166   | HTTP/1.1 200 OK (JPEG JFIF image)            |
| 67  | 5.753769 | 98.136.187.13  | 192.168.1.72   | HTTP     | 763    | HTTP/1.1 200 OK (JPEG JFIF image)            |
| 79  | 5.802039 | 98.136.187.13  | 192.168.1.72   | HTTP     | 72     | HTTP/1.1 200 OK (JPEG JFIF image)            |
| 81  | 5.994467 | 192.168.1.72   | 98.136.187.13  | HTTP     | 387    | GET /styles.css HTTP/1.1                     |
| 89  | 6.051696 | 98.136.187.13  | 192.168.1.72   | HTTP     | 1055   | HTTP/1.1 200 OK (text/css)                   |
| 93  | 7.302416 | 192.168.1.72   | 98.136.187.13  | HTTP     | 432    | GET /images/body-bg.png HTTP/1.1             |
| 94  | 7.303009 | 192.168.1.72   | 98.136.187.13  | HTTP     | 433    | GET /images/nav-left.png HTTP/1.1            |
| 95  | 7.303586 | 192.168.1.72   | 98.136.187.13  | HTTP     | 434    | GET /images/nav-right.png HTTP/1.1           |
| 96  | 7.304236 | 192.168.1.72   | 98.136.187.13  | HTTP     | 433    | GET /images/featureb.jpg HTTP/1.1            |
| 100 | 7.351740 | 98.136.187.13  | 192.168.1.72   | HTTP     | 67     | HTTP/1.1 200 OK (PNG)                        |
| 104 | 7.353156 | 98.136.187.13  | 192.168.1.72   | HTTP     | 376    | HTTP/1.1 200 OK (PNG)                        |
| 114 | 7.367530 | 98.136.187.13  | 192.168.1.72   | HTTP     | 377    | HTTP/1.1 200 OK (PNG)                        |
| 118 | 7.393418 | 192.168.1.72   | 98.139.206.151 | HTTP     | 735    | GET /visit.gif?&r=&b=Metscape%205.0 HTTP/1.1 |
| 156 | 7.502918 | 98.139.206.151 | 192.168.1.72   | HTTP     | 343    | HTTP/1.0 200 OK (GIF89a)                     |
| 232 | 7.645942 | 98.136.187.13  | 192.168.1.72   | HTTP     | 104    | HTTP/1.1 200 OK (JPEG JFIF image)            |
| 238 | 8.058070 | 192.168.1.72   | 98.136.187.13  | HTTP     | 330    | GET /favicon.ico HTTP/1.1                    |
| 242 | 8.111023 | 98.136.187.13  | 192.168.1.72   | HTTP     | 548    | HTTP/1.1 404 Not Found (text/html)           |

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

|  |  |
|--|--|
| Accept: image/png, image/svg+xml, image/*;q=0.8, */*;q=0.5\r\n             | Accept: */*\r\n  |
| Referer: http://www.wiresharktraining.com/\r\n                             | UA-CPU: AMD64\r\n  |
| Accept-Language: en-US\r\n   | Accept-Encoding: gzip, deflate\r\n   |
| User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like | User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like |
| Accept-Encoding: gzip, deflate\r\n   | Host: www.wiresharktraining.com\r\n  |
| Host: visit.webhosting.yahoo.com\r\n                                       | DNT: 1\r\n   |
| DNT: 1\r\n   | Connection: Keep-Alive\r\n   |

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

Answer:

8

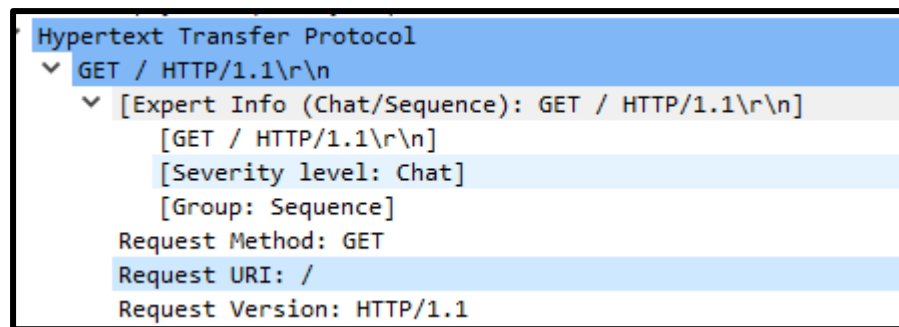
(filter used are shown in the screenshot I could have also added tcp.flags.ack == 0)

| 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 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1 |
| 4   | 4.095921 | 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=1 |
| 22  | 5.553402 | 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=1 |
| 23  | 5.553690 | 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=1 |
| 91  | 7.283422 | 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=1 |
| 92  | 7.283422 | 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=1 |
| 234 | 8.008141 | 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=1 |
| 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=1 |

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

|     |          |               |               |      |     |                                    |
|-----|----------|---------------|---------------|------|-----|------------------------------------|
| 238 | 8.058070 | 192.168.1.72  | 98.136.187.13 | HTTP | 330 | GET /favicon.ico HTTP/1.1          |
| 242 | 8.111023 | 98.136.187.13 | 192.168.1.72  | HTTP | 548 | HTTP/1.1 404 Not Found (text/html) |

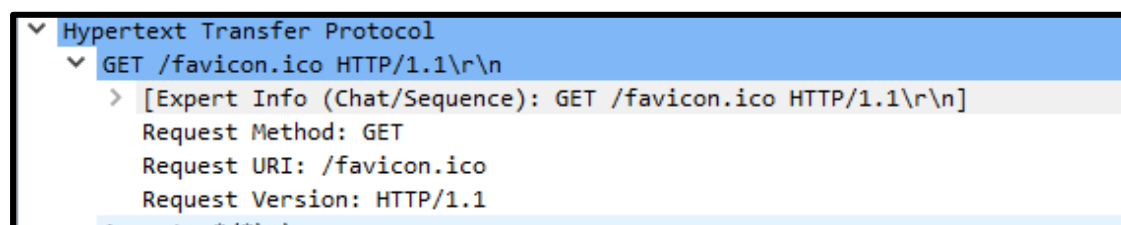
Answer:

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

Answer:

favicon.ico, filter used: http

|     |          |               |               |      |     |                                    |
|-----|----------|---------------|---------------|------|-----|------------------------------------|
| 238 | 8.058070 | 192.168.1.72  | 98.136.187.13 | HTTP | 330 | GET /favicon.ico HTTP/1.1          |
| 242 | 8.111023 | 98.136.187.13 | 192.168.1.72  | HTTP | 548 | HTTP/1.1 404 Not Found (text/html) |



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

|                      |                      |                      |
|----------------------|----------------------|----------------------|
| Source Port: 6128    | Source Port: 6129    | Source Port: 6130    |
| Destination Port: 80 | Destination Port: 80 | Destination Port: 80 |
| Source Port: 6131    | Source Port: 6136    | Source Port: 6140    |
| Destination Port: 80 | Destination Port: 80 | Destination Port: 80 |

תודה לבדיקה!