



Capturing HTTP

Capturing HTTP

» What is HTTP?

» Common issues with HTTP

- Slow response times
- Error codes (404, 501, etc.)
- No page returned

» Using Wireshark to troubleshoot issues

- You can use Wireshark to find broken websites

Capturing HTTP

34	4.496465	65.208.228.223	145.254.160.237	TCP		1434 [TCP segment of a reassembled PDU]
35	4.496465	145.254.160.237	65.208.228.223	TCP		54 tip2 > http [ACK] Seq=480 Ack=17941 win=9660 Len=0
36	4.776868	216.239.59.99	145.254.160.237	TCP	Note	1484 [TCP Retransmission] http > 3371 [PSH, ACK] Seq=1 Ack=722 win=31460
37	4.776868	145.254.160.237	216.239.59.99	TCP	Note	54 [TCP Dup ACK 28#1] 3371 > http [ACK] Seq=722 Ack=1591 win=8760 Len=0
38	4.846969	65.208.228.223	145.254.160.237	HTTP/X-Chat		478 HTTP/1.1 200 OK
39	5.017214	145.254.160.237	65.208.228.223	TCP		54 tip2 > http [ACK] Seq=480 Ack=18365 win=9236 Len=0
40	17.905747	65.208.228.223	145.254.160.237	TCP	Chat	54 http > tip2 [FIN, ACK] Seq=18365 Ack=480 win=6432 Len=0
41	17.905747	145.254.160.237	65.208.228.223	TCP		54 tip2 > http [ACK] Seq=480 Ack=18366 win=9236 Len=0
42	30.063228	145.254.160.237	65.208.228.223	TCP	Chat	54 tip2 > http [FIN, ACK] Seq=480 Ack=18366 win=9236 Len=0
43	30.393704	65.208.228.223	145.254.160.237	TCP		54 http > tip2 [ACK] Seq=18366 Ack=481 win=6432 Len=0

[Calculated window size: 31460]

[window size scaling factor: -1 (unknown)]

⊕ Checksum: 0xacd9 [validation disabled]

⊖ [SEQ/ACK analysis]

[Bytes in flight: 1430]

⊖ [TCP Analysis Flags]

⊖ [This frame is a (suspected) retransmission]

⊖ [Expert Info (Note/Sequence): Retransmission (suspected)]

[Message: Retransmission (suspected)]

[Severity level: Note]

[Group: Sequence]

[The RTO for this segment was: 0.821180000 seconds]

[\[RTO based on delta from frame: 27\]](#)

⊖ [Timestamps]

[Time since first frame in this TCP stream: 1.792577000 seconds]

[Time since previous frame in this TCP stream: 0.821180000 seconds]

Retransmitted TCP segment data (1430 bytes)

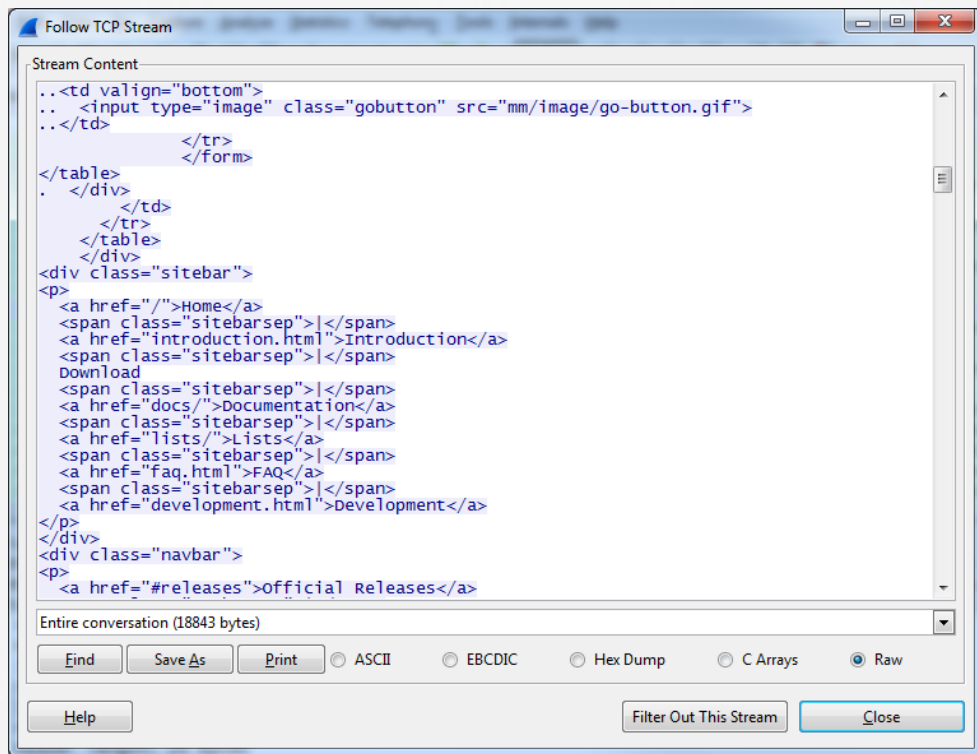
Capturing HTTP

» Using tools to find problems with HTTP

» Following the TCP stream

- You can filter out the conversation and view the TCP stream
- This allows you to see problems with the pages you are viewing

Capturing HTTP



Questions?