

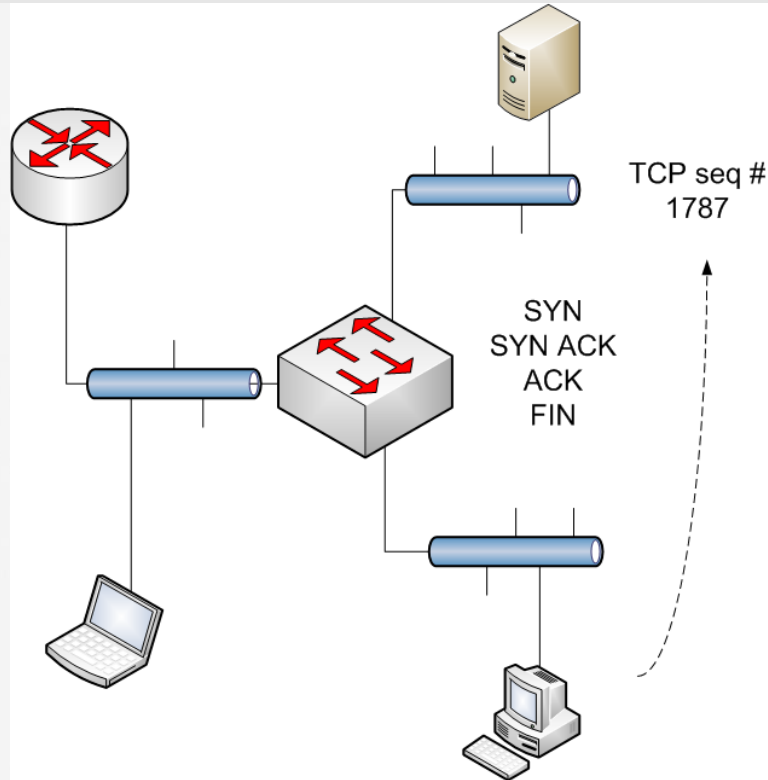


Capturing Client/Server Response

Client/Server Response

- » What is Client/Server communication?
- » How can I use Wireshark to capture and analyze this communication traffic?
 - Placement
 - Filters
- » What am I analyzing?
 - Communication patterns

Network Lab



Client/Server Response

» Wireshark can assist with

- Reviewing IP-based issues, TCP-based issues, UDP-based issues, and much more when analyzing client/server communications

» Available tools

- Capture window
- Filters
- Analysis tools (such as flow graph and I/O graph)
- More

Client/Server Response

No.	Time	Source	Destination	Protocol	Expert	Length	Info	Absolute time
352	58.249682000	192.168.1.13	74.125.228.52	TCP		54	49228 > https [ACK] Seq=16668 Ack=59857 win=111616 Len=0	2014-05-14
353	58.343208000	192.168.1.13	63.117.14.89	TCP		54	49234 > http [ACK] Seq=227 Ack=789 win=16640 Len=0	2014-05-14
354	58.405578000	192.168.1.13	63.117.14.151	TCP		54	49233 > https [ACK] Seq=864 Ack=3861 win=17152 Len=0	2014-05-14
355	58.416729000	63.117.14.151	192.168.1.13	TLSv1	Note	283	[TCP Retransmission] Application Data	2014-05-14
356	58.416944000	192.168.1.13	63.117.14.151	TCP	Note	66	[TCP Dup ACK 354#1] 49233 > https [ACK] Seq=864 Ack=3861 win=17152 Len=0 SLE=3632 S	2014-05-14
360	64.697323000	192.168.1.13	74.125.228.52	HTTP	Chat	1389	GET /url?sa=t&rc=t=j&q=&esrc=s&frm=1&source=web&cd=2&ved=0CC0QFjAB&url=http%3A%2F%2F	2014-05-14
361	64.734311000	74.125.228.52	192.168.1.13	HTTP	Chat	927	HTTP/1.1 200 OK (text/html)	2014-05-14
363	64.940529000	192.168.1.13	74.125.228.52	TCP		54	49229 > http [ACK] Seq=2027 Ack=1377 win=15616 Len=0	2014-05-14
365	64.946008000	192.168.1.13	162.159.241.165	TCP	Chat	66	49235 > http [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1	2014-05-14
366	64.946033000	192.168.1.13	162.159.241.165	TCP	Chat	66	49236 > http [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1	2014-05-14
367	64.946206000	74.125.228.52	192.168.1.13	HTTP	Chat	927	[TCP Retransmission] HTTP/1.1 200 OK (text/html)	2014-05-14
368	64.946450000	192.168.1.13	74.125.228.52	TCP	Note	66	[TCP Dup ACK 363#1] 49229 > http [ACK] Seq=2027 Ack=1377 win=15616 Len=0 SLE=504 SR	2014-05-14
369	64.958578000	162.159.241.165	192.168.1.13	TCP	Chat	66	http > 49236 [SYN, ACK] Seq=0 Ack=1 win=14600 Len=0 MSS=1460 SACK_PERM=1 WS=1024	2014-05-14
370	64.958945000	192.168.1.13	162.159.241.165	TCP		54	49236 > http [ACK] Seq=1 Ack=1 win=17408 Len=0	2014-05-14
371	64.959629000	192.168.1.13	162.159.241.165	HTTP	Chat	1382	GET /questions/12154/can-i-write-a-filter-to-locate-sequence-number-inconsistencies	2014-05-14
372	64.961379000	162.159.241.165	192.168.1.13	TCP	Chat	66	http > 49235 [SYN, ACK] Seq=0 Ack=1 win=14600 Len=0 MSS=1460 SACK_PERM=1 WS=1024	2014-05-14

Frame 368: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
Ethernet II, Src: IntelCor_3b:35:4c (6c:88:14:3b:35:4c), Dst: Actionte_44:de:b2 (00:26:b8:44:de:b2)
Internet Protocol Version 4, Src: 192.168.1.13 (192.168.1.13), Dst: 74.125.228.52 (74.125.228.52)
Transmission Control Protocol, Src Port: 49229 (49229), Dst Port: http (80), Seq: 2027, Ack: 1377, Len: 0

Questions?