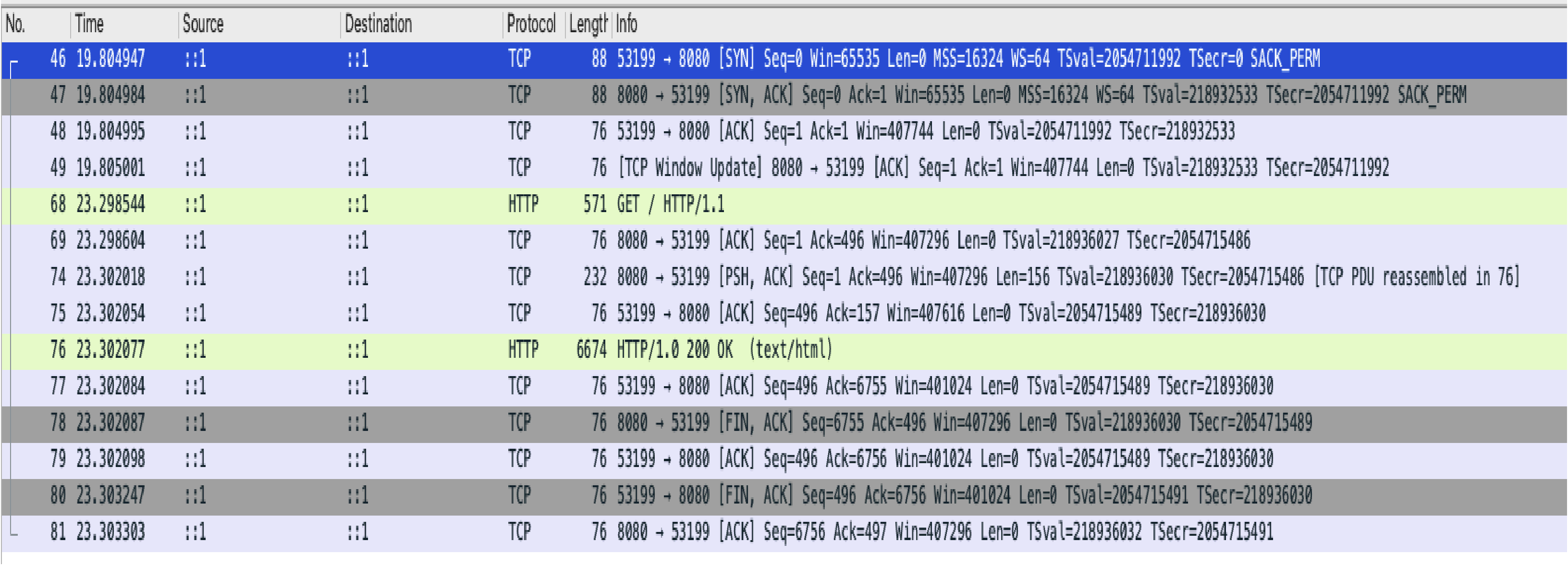
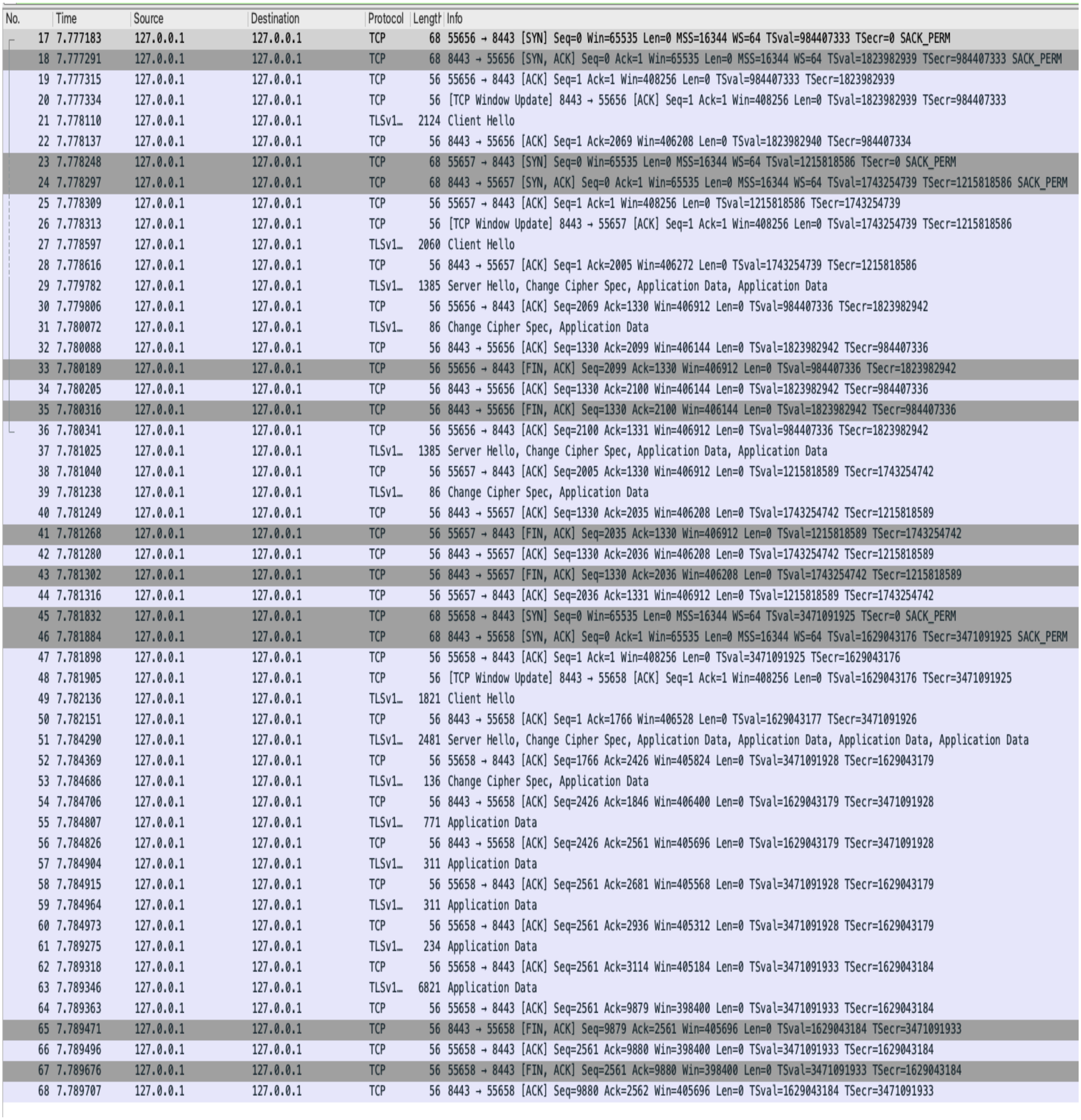
HTTP sends all of its data in plaintext between the client and the server. This is to say that it offers no encryption or authentication. So anyone with access to the network between the client and the server – like an eavesdropper with a network sniffer such as Wireshark – can read all of the traffic going to and from the server with no special key or password. So in the example above, the browser sends a request of GET / HTTP/1.1 to localhost:8080. When this happens, both the request and the response from the server can be seen as raw text on the network. The packet capture below in Wireshark shows exactly this happening. Anyone watching the traffic can see exactly which resources are being requested, any form data or cookies that are being sent, login info, and even the full contents of the HTML of the page. In the packet capture below, packet 68 shows the browser's GET / HTTP/1.1 request and packet 76 shows the server's HTTP/1.0 200 OK response with the full contents of the directory (i started the server in the root of my computer). Since there is no confidentiality or integrity with HTTP, it is open to attackers who can intercept or modify the data in transit.



No.	Time	Source	Destination	Protocol	Lengtl	Info
46	19.804947	::1	::1	TCP	88	53199 → 8080 [SYN] Seq=0 Win=65535 Len=0 MSS=16324 WS=64 TSval=2054711992 TSecr=0 SACK_PERM
47	19.804984	::1	::1	TCP	88	8080 → 53199 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=16324 WS=64 TSval=218932533 TSecr=2054711992 SACK_PERM
48	19.804995	::1	::1	TCP	76	53199 → 8080 [ACK] Seq=1 Ack=1 Win=407744 Len=0 TSval=2054711992 TSecr=218932533
49	19.805001	::1	::1	TCP	76	[TCP Window Update] 8080 → 53199 [ACK] Seq=1 Ack=1 Win=407744 Len=0 TSval=218932533 TSecr=2054711992
68	23.298544	::1	::1	HTTP	571	GET / HTTP/1.1
69	23.298604	::1	::1	TCP	76	8080 → 53199 [ACK] Seq=1 Ack=496 Win=407296 Len=0 TSval=218936027 TSecr=2054715486
74	23.302018	::1	::1	TCP	232	8080 → 53199 [PSH, ACK] Seq=1 Ack=496 Win=407296 Len=156 TSval=218936030 TSecr=2054715486 [TCP PDU reassembled in 76]
75	23.302054	::1	::1	TCP	76	53199 → 8080 [ACK] Seq=496 Ack=157 Win=407616 Len=0 TSval=2054715489 TSecr=218936030
76	23.302077	::1	::1	HTTP	6674	HTTP/1.0 200 OK (text/html)
77	23.302084	::1	::1	TCP	76	53199 → 8080 [ACK] Seq=496 Ack=6755 Win=401024 Len=0 TSval=2054715489 TSecr=218936030
78	23.302087	::1	::1	TCP	76	8080 → 53199 [FIN, ACK] Seq=6755 Ack=496 Win=407296 Len=0 TSval=218936030 TSecr=2054715489
79	23.302098	::1	::1	TCP	76	53199 → 8080 [ACK] Seq=496 Ack=6756 Win=401024 Len=0 TSval=2054715489 TSecr=218936030
80	23.303247	::1	::1	TCP	76	53199 → 8080 [FIN, ACK] Seq=496 Ack=6756 Win=401024 Len=0 TSval=2054715491 TSecr=218936030
81	23.303303	::1	::1	TCP	76	8080 → 53199 [ACK] Seq=6756 Ack=497 Win=407296 Len=0 TSval=218936032 TSecr=2054715491

The Wireshark capture below displays the HTTPS exchange between my browser and the local server on port 8443. As you can see, the HTTPS trace only contains TLS 1.3 handshake messages and encrypted "Application Data." The Client Hello and Server Hello packets set up encryption, and from then on the payloads are random binary instead of readable HTML. This is a strong benefit of HTTPS: it protects the confidentiality of the traffic such that no eavesdroppers can view or modify any part of the communication.



No.	Time	Source	Destination	Protocol	Length	Info
17	7.777183	127.0.0.1	127.0.0.1	TCP	68	55656 → 8443 [SYN] Seq=0 Win=65535 Len=0 MSS=16344 WS=64 TSval=984407333 TSecr=0 SACK_PERM
18	7.777291	127.0.0.1	127.0.0.1	TCP	68	8443 → 55656 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=16344 WS=64 TSval=1823982939 TSecr=984407333 SACK_PERM
19	7.777315	127.0.0.1	127.0.0.1	TCP	56	55656 → 8443 [ACK] Seq=1 Ack=1 Win=408256 Len=0 TSval=984407333 TSecr=1823982939
20	7.777334	127.0.0.1	127.0.0.1	TCP	56	[TCP Window Update] 8443 → 55656 [ACK] Seq=1 Ack=1 Win=408256 Len=0 TSval=1823982939 TSecr=984407333
21	7.778110	127.0.0.1	127.0.0.1	TLSv1…	2124	Client Hello
22	7.778137	127.0.0.1	127.0.0.1	TCP	56	8443 → 55656 [ACK] Seq=1 Ack=2069 Win=406208 Len=0 TSval=1823982940 TSecr=984407334
23	7.778248	127.0.0.1	127.0.0.1	TCP	68	55657 → 8443 [SYN] Seq=0 Win=65535 Len=0 MSS=16344 WS=64 TSval=1215818586 TSecr=0 SACK_PERM
24	7.778297	127.0.0.1	127.0.0.1	TCP	68	8443 → 55657 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=16344 WS=64 TSval=1743254739 TSecr=1215818586 SACK_PERM
25	7.778309	127.0.0.1	127.0.0.1	TCP	56	55657 → 8443 [ACK] Seq=1 Ack=1 Win=408256 Len=0 TSval=1215818586 TSecr=1743254739
26	7.778313	127.0.0.1	127.0.0.1	TCP	56	[TCP Window Update] 8443 → 55657 [ACK] Seq=1 Ack=1 Win=408256 Len=0 TSval=1743254739 TSecr=1215818586
27	7.778597	127.0.0.1	127.0.0.1	TLSv1…	2060	Client Hello
28	7.778616	127.0.0.1	127.0.0.1	TCP	56	8443 → 55657 [ACK] Seq=1 Ack=2005 Win=406272 Len=0 TSval=1743254739 TSecr=1215818586
29	7.779782	127.0.0.1	127.0.0.1	TLSv1…	1385	Server Hello, Change Cipher Spec, Application Data, Application Data
30	7.779806	127.0.0.1	127.0.0.1	TCP	56	55656 → 8443 [ACK] Seq=2069 Ack=1330 Win=406912 Len=0 TSval=984407336 TSecr=1823982942
31	7.780072	127.0.0.1	127.0.0.1	TLSv1…	86	Change Cipher Spec, Application Data
32	7.780088	127.0.0.1	127.0.0.1	TCP	56	8443 → 55656 [ACK] Seq=1330 Ack=2099 Win=406144 Len=0 TSval=1823982942 TSecr=984407336
33	7.780189	127.0.0.1	127.0.0.1	TCP	56	55656 → 8443 [FIN, ACK] Seq=2099 Ack=1330 Win=406912 Len=0 TSval=984407336 TSecr=1823982942
34	7.780205	127.0.0.1	127.0.0.1	TCP	56	8443 → 55656 [ACK] Seq=1330 Ack=2100 Win=406144 Len=0 TSval=1823982942 TSecr=984407336
35	7.780316	127.0.0.1	127.0.0.1	TCP	56	8443 → 55656 [FIN, ACK] Seq=1330 Ack=2100 Win=406144 Len=0 TSval=1823982942 TSecr=984407336
36	7.780341	127.0.0.1	127.0.0.1	TCP	56	55656 → 8443 [ACK] Seq=2100 Ack=1331 Win=406912 Len=0 TSval=984407336 TSecr=1823982942
37	7.781025	127.0.0.1	127.0.0.1	TLSv1…	1385	Server Hello, Change Cipher Spec, Application Data, Application Data
38	7.781040	127.0.0.1	127.0.0.1	TCP	56	55657 → 8443 [ACK] Seq=2005 Ack=1330 Win=406912 Len=0 TSval=1215818589 TSecr=1743254742
39	7.781238	127.0.0.1	127.0.0.1	TLSv1…	86	Change Cipher Spec, Application Data
40	7.781249	127.0.0.1	127.0.0.1	TCP	56	8443 → 55657 [ACK] Seq=1330 Ack=2035 Win=406208 Len=0 TSval=1743254742 TSecr=1215818589
41	7.781268	127.0.0.1	127.0.0.1	TCP	56	55657 → 8443 [FIN, ACK] Seq=2035 Ack=1330 Win=406912 Len=0 TSval=1215818589 TSecr=1743254742
42	7.781280	127.0.0.1	127.0.0.1	TCP	56	8443 → 55657 [ACK] Seq=1330 Ack=2036 Win=406208 Len=0 TSval=1743254742 TSecr=1215818589
43	7.781302	127.0.0.1	127.0.0.1	TCP	56	8443 → 55657 [FIN, ACK] Seq=1330 Ack=2036 Win=406208 Len=0 TSval=1743254742 TSecr=1215818589
44	7.781316	127.0.0.1	127.0.0.1	TCP	56	55657 → 8443 [ACK] Seq=2036 Ack=1331 Win=406912 Len=0 TSval=1215818589 TSecr=1743254742
45	7.781832	127.0.0.1	127.0.0.1	TCP	68	55658 → 8443 [SYN] Seq=0 Win=65535 Len=0 MSS=16344 WS=64 TSval=3471091925 TSecr=0 SACK_PERM
46	7.781884	127.0.0.1	127.0.0.1	TCP	68	8443 → 55658 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=16344 WS=64 TSval=1629043176 TSecr=3471091925 SACK_PERM
47	7.781898	127.0.0.1	127.0.0.1	TCP	56	55658 → 8443 [ACK] Seq=1 Ack=1 Win=408256 Len=0 TSval=3471091925 TSecr=1629043176
48	7.781905	127.0.0.1	127.0.0.1	TCP	56	[TCP Window Update] 8443 → 55658 [ACK] Seq=1 Ack=1 Win=408256 Len=0 TSval=1629043176 TSecr=3471091925
49	7.782136	127.0.0.1	127.0.0.1	TLSv1…	1821	Client Hello
50	7.782151	127.0.0.1	127.0.0.1	TCP	56	8443 → 55658 [ACK] Seq=1 Ack=1766 Win=406528 Len=0 TSval=1629043177 TSecr=3471091926
51	7.784290	127.0.0.1	127.0.0.1	TLSv1…	2481	Server Hello, Change Cipher Spec, Application Data, Application Data, Application Data, Application Data
52	7.784369	127.0.0.1	127.0.0.1	TCP	56	55658 → 8443 [ACK] Seq=1766 Ack=2426 Win=405824 Len=0 TSval=3471091928 TSecr=1629043179
53	7.784686	127.0.0.1	127.0.0.1	TLSv1…	136	Change Cipher Spec, Application Data
54	7.784706	127.0.0.1	127.0.0.1	TCP	56	8443 → 55658 [ACK] Seq=2426 Ack=1846 Win=406400 Len=0 TSval=1629043179 TSecr=3471091928
55	7.784807	127.0.0.1	127.0.0.1	TLSv1…	771	Application Data
56	7.784826	127.0.0.1	127.0.0.1	TCP	56	8443 → 55658 [ACK] Seq=2426 Ack=2561 Win=405696 Len=0 TSval=1629043179 TSecr=3471091928
57	7.784904	127.0.0.1	127.0.0.1	TLSv1…	311	Application Data
58	7.784915	127.0.0.1	127.0.0.1	TCP	56	55658 → 8443 [ACK] Seq=2561 Ack=2681 Win=405568 Len=0 TSval=3471091928 TSecr=1629043179
59	7.784964	127.0.0.1	127.0.0.1	TLSv1…	311	Application Data
60	7.784973	127.0.0.1	127.0.0.1	TCP	56	55658 → 8443 [ACK] Seq=2561 Ack=2936 Win=405312 Len=0 TSval=3471091928 TSecr=1629043179
61	7.789275	127.0.0.1	127.0.0.1	TLSv1…	234	Application Data
62	7.789318	127.0.0.1	127.0.0.1	TCP	56	55658 → 8443 [ACK] Seq=2561 Ack=3114 Win=405184 Len=0 TSval=3471091933 TSecr=1629043184
63	7.789346	127.0.0.1	127.0.0.1	TLSv1…	6821	Application Data
64	7.789363	127.0.0.1	127.0.0.1	TCP	56	55658 → 8443 [ACK] Seq=2561 Ack=9879 Win=398400 Len=0 TSval=3471091933 TSecr=1629043184
65	7.789471	127.0.0.1	127.0.0.1	TCP	56	8443 → 55658 [FIN, ACK] Seq=9879 Ack=2561 Win=405696 Len=0 TSval=1629043184 TSecr=3471091933
66	7.789496	127.0.0.1	127.0.0.1	TCP	56	55658 → 8443 [ACK] Seq=2561 Ack=9880 Win=398400 Len=0 TSval=3471091933 TSecr=1629043184
67	7.789676	127.0.0.1	127.0.0.1	TCP	56	55658 → 8443 [FIN, ACK] Seq=2561 Ack=9880 Win=398400 Len=0 TSval=3471091933 TSecr=1629043184
68	7.789707	127.0.0.1	127.0.0.1	TCP	56	8443 → 55658 [ACK] Seq=9880 Ack=2562 Win=405696 Len=0 TSval=1629043184 TSecr=3471091933