

1. Работа в Wireshark. Запустить Wireshark, выбрать любой веб-сайт, определить IP-адрес сервера, отфильтровать в Wireshark трафик по этому IP-адресу. Набрать адрес сервера в строке браузера. Сколько TCP-соединений было открыто и почему. В работе можно использовать источник 1 из списка дополнительных материалов.

Для теста используем: [https://geekbrains.ru\(178.248.232.209:443\)](https://geekbrains.ru(178.248.232.209:443))

При анализе соединений в WireShark видим сразу 1-ю «тройку рукопожатий»

С моего внешнего IP 192.168.0.4 с динамическим портом 60501 к серверу GeekBrains 178.248.232.209 (443 порт) соединение защищенное https.

No.	Time	Source	Destination	Protocol	Length	Info
83	2.636728	192.168.0.164	178.248.232.209	TCP	78	60501 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=2858448904
84	2.648775	178.248.232.209	192.168.0.164	TCP	74	443 → 60501 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1
85	2.648850	192.168.0.164	178.248.232.209	TCP	66	60501 → 443 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=2858448916 TSecr=4

В ходе изучения «Дампа», можно судить что через определенный timeout происходят повторные соединения с сервером (ip 178.248.232.209:443) с других динамических портов моего хоста включая окончание сессии(передача FIN параметра):

90	2.671227	192.168.0.164	178.248.232.209	TLSv1...	130	Change Cipher Spec, Application Data
93	2.683488	178.248.232.209	192.168.0.164	TLSv1...	337	Application Data
94	2.683586	192.168.0.164	178.248.232.209	TCP	66	60501 → 443 [ACK] Seq=641 Ack=516 Win=131200 Len=0 TSval=2858448946 TSecr=4
124	2.850934	192.168.0.164	178.248.232.209	TCP	78	60502 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=2858449105
128	2.863413	178.248.232.209	192.168.0.164	TCP	74	443 → 60502 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1
129	2.863520	192.168.0.164	178.248.232.209	TCP	66	60502 → 443 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=2858449116 TSecr=4
130	2.864131	192.168.0.164	178.248.232.209	TLSv1...	583	Client Hello
300	3.862508	192.168.0.164	178.248.232.209	TCP	78	60506 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=2858450071
303	3.874943	178.248.232.209	192.168.0.164	TCP	74	443 → 60506 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1
304	3.875070	192.168.0.164	178.248.232.209	TCP	66	60506 → 443 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=2858450083 TSecr=4
305	3.877457	192.168.0.164	178.248.232.209	TLSv1...	639	Client Hello
379	4.107581	192.168.0.164	178.248.232.209	TCP	78	60508 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=2858450294
382	4.113567	178.248.232.209	192.168.0.164	TCP	66	443 → 60502 [ACK] Seq=38511 Ack=10848 Win=53760 Len=0 TSval=4205597144
388	4.117185	178.248.232.209	192.168.0.164	TCP	66	443 → 60506 [ACK] Seq=991 Ack=5817 Win=41984 Len=0 TSval=4205597148 TSecr=4
389	4.119734	178.248.232.209	192.168.0.164	TCP	74	443 → 60508 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1
390	4.119827	192.168.0.164	178.248.232.209	TCP	66	60508 → 443 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=2858450304 TSecr=4
391	4.120627	192.168.0.164	178.248.232.209	TLSv1...	639	Client Hello
409	4.170360	192.168.0.164	178.248.232.209	TCP	78	60509 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=2858450350
410	4.174319	192.168.0.164	178.248.232.209	TCP	78	60510 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=2858450353
411	4.175093	178.248.232.209	192.168.0.164	TLSv1...	541	Application Data
412	4.175184	192.168.0.164	178.248.232.209	TCP	66	60508 → 443 [ACK] Seq=3179 Ack=991 Win=130752 Len=0 TSval=2858450354 TSecr=4
413	4.179952	178.248.232.209	192.168.0.164	TCP	66	443 → 60506 [ACK] Seq=1466 Ack=8324 Win=48128 Len=0 TSval=4205597211 TSecr=4
414	4.182460	178.248.232.209	192.168.0.164	TCP	74	443 → 60509 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1
415	4.182550	192.168.0.164	178.248.232.209	TCP	66	60509 → 443 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=2858450360 TSecr=4
418	4.186485	178.248.232.209	192.168.0.164	TCP	74	443 → 60510 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1
419	4.186573	192.168.0.164	178.248.232.209	TCP	66	60510 → 443 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=2858450363 TSecr=4
420	4.186868	192.168.0.164	178.248.232.209	TLSv1...	639	Client Hello

Time	Source	Destination	Protocol	Length	Application Data
439	4.201989	178.248.232.209	192.168.0.164	TLSv1...	320 Application Data, Application Data
440	4.201990	178.248.232.209	192.168.0.164	TCP	74 443 → 60511 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1
441	4.202051	192.168.0.164	178.248.232.209	TCP	66 60510 → 443 [ACK] Seq=518 Ack=2897 Win=128832 Len=0 TSval=2858450377 TSecr=42
442	4.202051	192.168.0.164	178.248.232.209	TCP	66 60510 → 443 [ACK] Seq=518 Ack=3151 Win=128576 Len=0 TSval=2858450377 TSecr=42
443	4.202081	192.168.0.164	178.248.232.209	TCP	66 60511 → 443 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=2858450377 TSecr=42
444	4.203680	192.168.0.164	178.248.232.209	TLSv1...	583 Client Hello
1128	7.662604	178.248.232.209	192.168.0.164	TCP	66 443 → 60501 [FIN, ACK] Seq=540 Ack=641 Win=30720 Len=0 TSval=4205600693 TSecr=42
1129	7.662714	192.168.0.164	178.248.232.209	TCP	66 60501 → 443 [ACK] Seq=641 Ack=540 Win=131200 Len=0 TSval=2858453695 TSecr=42
1130	7.662790	192.168.0.164	178.248.232.209	TCP	66 60501 → 443 [ACK] Seq=641 Ack=541 Win=131200 Len=0 TSval=2858453695 TSecr=42
1131	7.663224	192.168.0.164	178.248.232.209	TLSv1...	90 Application Data
1132	7.663781	192.168.0.164	178.248.232.209	TCP	66 60501 → 443 [FIN, ACK] Seq=665 Ack=541 Win=131200 Len=0 TSval=2858453695 TSecr=42
1133	7.675489	178.248.232.209	192.168.0.164	TCP	54 443 → 60501 [RST] Seq=541 Win=0 Len=0

Могу предположить что такие соединения связаны с протоколом https.
Всего было открыто 6 TCP -соединений.