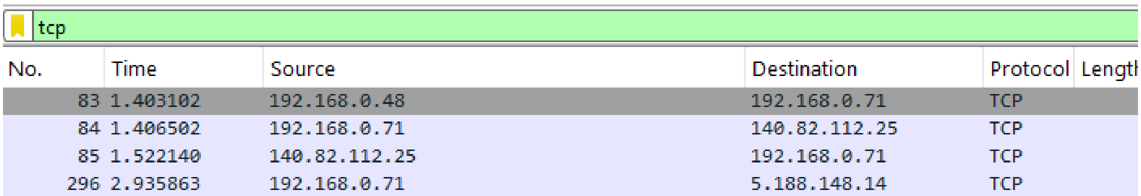
EJERCICIOS DE WIRESHARK

Protocolos

1. Todo el tráfico TCP:

Tcp

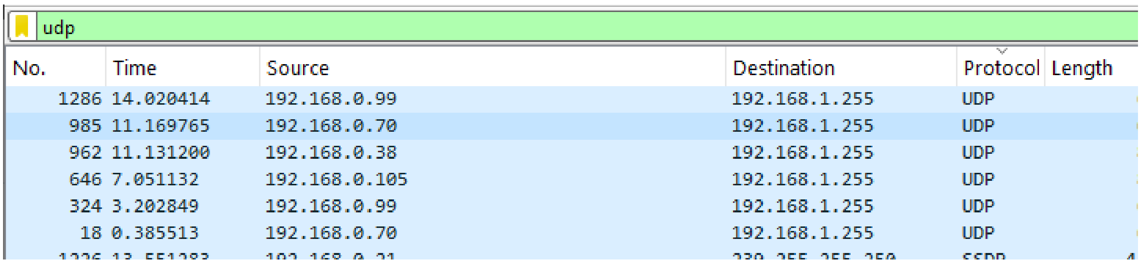


tcp

No.	Time	Source	Destination	Protocol	Length
83	1.403102	192.168.0.48	192.168.0.71	TCP	
84	1.406502	192.168.0.71	140.82.112.25	TCP	
85	1.522140	140.82.112.25	192.168.0.71	TCP	
296	2.935863	192.168.0.71	5.188.148.14	TCP	

2. Todo el tráfico UDP:

Udp

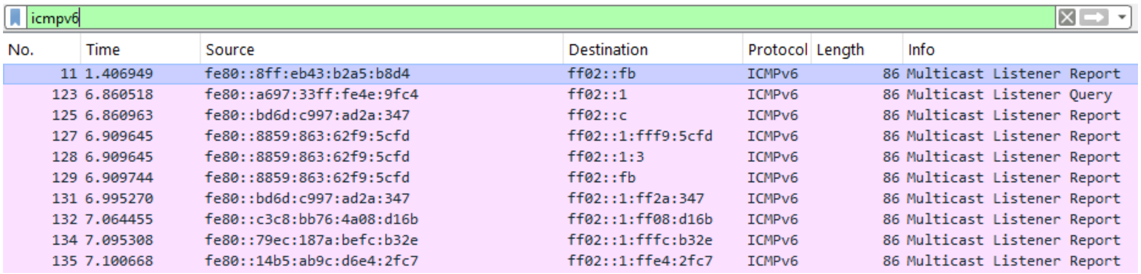


udp

No.	Time	Source	Destination	Protocol	Length
1286	14.020414	192.168.0.99	192.168.1.255	UDP	
985	11.169765	192.168.0.70	192.168.1.255	UDP	
962	11.131200	192.168.0.38	192.168.1.255	UDP	
646	7.051132	192.168.0.105	192.168.1.255	UDP	
324	3.202849	192.168.0.99	192.168.1.255	UDP	
18	0.385513	192.168.0.70	192.168.1.255	UDP	
1226	13.551283	192.168.0.21	239.255.255.250	SSDP	

3. Tráfico ICMP (ping):

Icmp

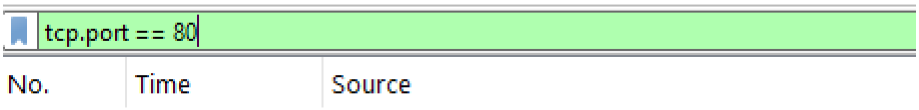


icmpv6

No.	Time	Source	Destination	Protocol	Length	Info
11	1.406949	fe80::8ff:eb43:b2a5:b8d4	ff02::fb	ICMPv6	86	Multicast Listener Report
123	6.860518	fe80::a697:33ff:fe4e:9fc4	ff02::1	ICMPv6	86	Multicast Listener Query
125	6.860963	fe80::bd6d:c997:ad2a:347	ff02::c	ICMPv6	86	Multicast Listener Report
127	6.909645	fe80::8859:863:62f9:5cfd	ff02::1:fff9:5cfd	ICMPv6	86	Multicast Listener Report
128	6.909645	fe80::8859:863:62f9:5cfd	ff02::1:3	ICMPv6	86	Multicast Listener Report
129	6.909744	fe80::8859:863:62f9:5cfd	ff02::fb	ICMPv6	86	Multicast Listener Report
131	6.995270	fe80::bd6d:c997:ad2a:347	ff02::1:ff2a:347	ICMPv6	86	Multicast Listener Report
132	7.064455	fe80::c3c8:bb76:4a08:d16b	ff02::1:ff08:d16b	ICMPv6	86	Multicast Listener Report
134	7.095308	fe80::79ec:187a:befc:b32e	ff02::1:fffc:b32e	ICMPv6	86	Multicast Listener Report
135	7.100668	fe80::14b5:ab9c:d6e4:2fc7	ff02::1:ffe4:2fc7	ICMPv6	86	Multicast Listener Report

4. Tráfico HTTP (puerto 80):

http

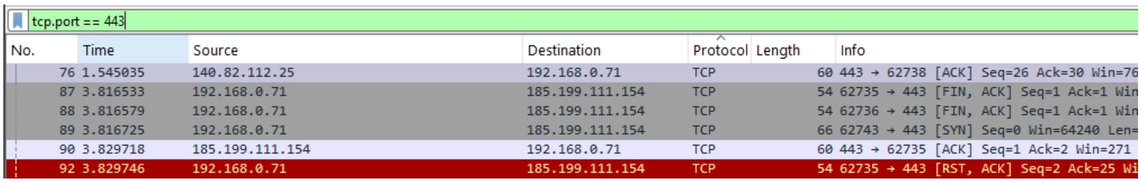


tcp.port == 80

No.	Time	Source

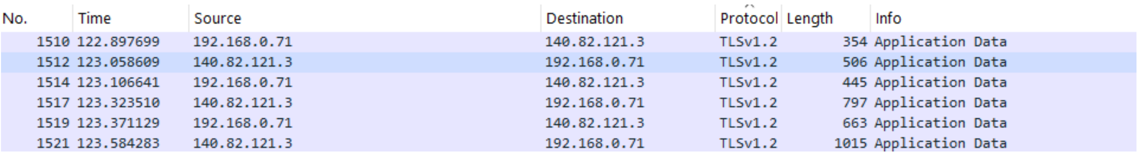
5. Tráfico HTTPS (TLS/SSL):

Tls



tcp.port == 443

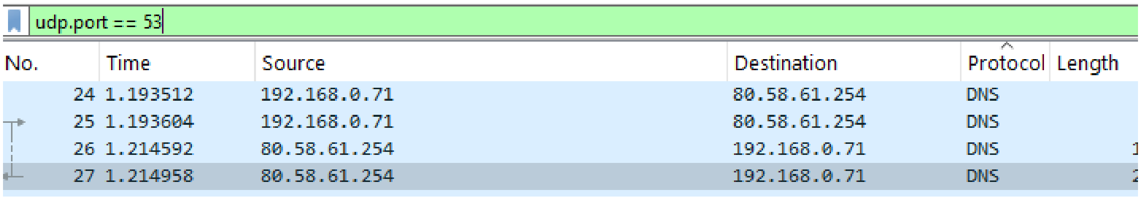
No.	Time	Source	Destination	Protocol	Length	Info
76	1.545035	140.82.112.25	192.168.0.71	TCP	60	443 → 62738 [ACK] Seq=26 Ack=30 Win=76
87	3.816533	192.168.0.71	185.199.111.154	TCP	54	62735 → 443 [FIN, ACK] Seq=1 Ack=1 Win
88	3.816579	192.168.0.71	185.199.111.154	TCP	54	62736 → 443 [FIN, ACK] Seq=1 Ack=1 Win
89	3.816725	192.168.0.71	185.199.111.154	TCP	66	62743 → 443 [SYN] Seq=0 Win=64240 Len=
90	3.829718	185.199.111.154	192.168.0.71	TCP	60	443 → 62735 [ACK] Seq=1 Ack=2 Win=271
92	3.829746	192.168.0.71	185.199.111.154	TCP	54	62735 → 443 [RST, ACK] Seq=2 Ack=25 Wi



No.	Time	Source	Destination	Protocol	Length	Info
1510	122.897699	192.168.0.71	140.82.121.3	TLSv1.2	354	Application Data
1512	123.058609	140.82.121.3	192.168.0.71	TLSv1.2	506	Application Data
1514	123.106641	192.168.0.71	140.82.121.3	TLSv1.2	445	Application Data
1517	123.323510	140.82.121.3	192.168.0.71	TLSv1.2	797	Application Data
1519	123.371129	192.168.0.71	140.82.121.3	TLSv1.2	663	Application Data
1521	123.584283	140.82.121.3	192.168.0.71	TLSv1.2	1015	Application Data

6. Tráfico DNS (puerto 53):

Dns

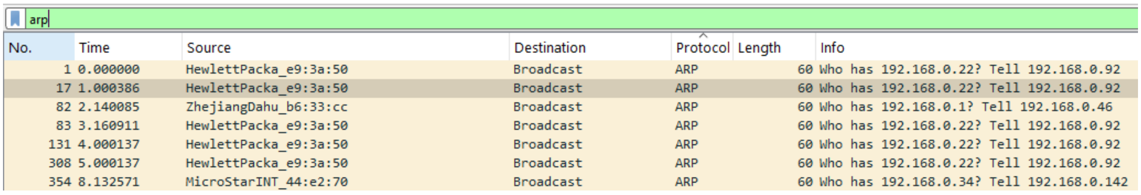


udp.port == 53

No.	Time	Source	Destination	Protocol	Length
24	1.193512	192.168.0.71	80.58.61.254	DNS	
25	1.193604	192.168.0.71	80.58.61.254	DNS	
26	1.214592	80.58.61.254	192.168.0.71	DNS	1
27	1.214958	80.58.61.254	192.168.0.71	DNS	2

7. Tráfico ARP:

Arp

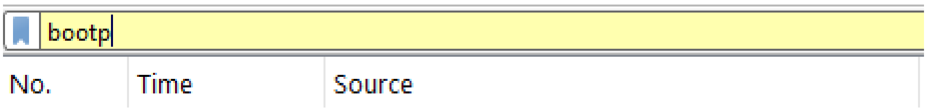


arp

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	HewlettPacka_e9:3a:50	Broadcast	ARP	60	Who has 192.168.0.22? Tell 192.168.0.92
17	1.000386	HewlettPacka_e9:3a:50	Broadcast	ARP	60	Who has 192.168.0.22? Tell 192.168.0.92
82	2.140085	ZhejiangDahu_b6:33:cc	Broadcast	ARP	60	Who has 192.168.0.1? Tell 192.168.0.46
83	3.160911	HewlettPacka_e9:3a:50	Broadcast	ARP	60	Who has 192.168.0.22? Tell 192.168.0.92
131	4.000137	HewlettPacka_e9:3a:50	Broadcast	ARP	60	Who has 192.168.0.22? Tell 192.168.0.92
308	5.000137	HewlettPacka_e9:3a:50	Broadcast	ARP	60	Who has 192.168.0.22? Tell 192.168.0.92
354	8.132571	MicroStarINT_44:e2:70	Broadcast	ARP	60	Who has 192.168.0.34? Tell 192.168.0.142

8. Tráfico DHCP:

Bootp

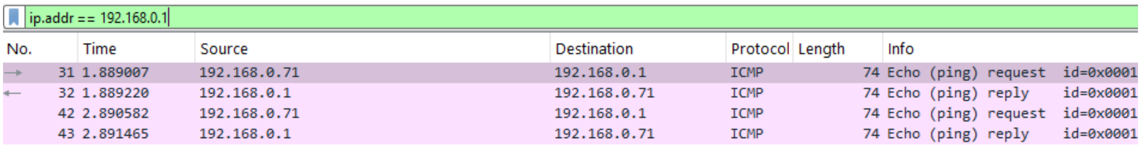


```
bootp
No.        Time              Source
```

IPs

9. Cualquier tráfico de una IP concreta:

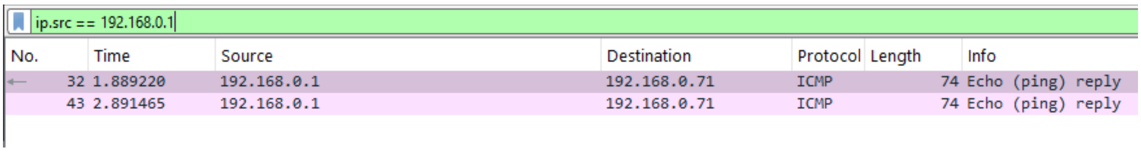
ip.addr == 192.168.1.10



```
ip.addr == 192.168.0.1
No.   Time        Source         Destination   Protocol Length  Info
   31 1.889007    192.168.0.71   192.168.0.1   ICMP         74 Echo (ping) request  id=0x0001
   32 1.889220    192.168.0.1    192.168.0.71  ICMP         74 Echo (ping) reply    id=0x0001
   42 2.890582    192.168.0.71   192.168.0.1   ICMP         74 Echo (ping) request  id=0x0001
   43 2.891465    192.168.0.1    192.168.0.71  ICMP         74 Echo (ping) reply    id=0x0001
```

10. Solo tráfico de origen desde una IP:

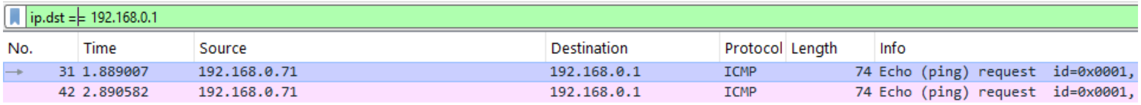
ip.src == 192.168.1.10



```
ip.src == 192.168.0.1
No.   Time        Source         Destination   Protocol Length  Info
   32 1.889220    192.168.0.1    192.168.0.71  ICMP         74 Echo (ping) reply
   43 2.891465    192.168.0.1    192.168.0.71  ICMP         74 Echo (ping) reply
```

11. Solo tráfico con destino a una IP:

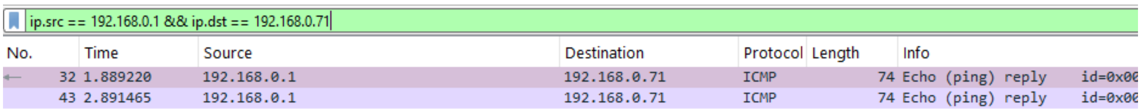
ip.dst == 192.168.1.10



```
ip.dst == 192.168.0.1
No.   Time        Source         Destination   Protocol Length  Info
   31 1.889007    192.168.0.71   192.168.0.1   ICMP         74 Echo (ping) request  id=0x0001,
   42 2.890582    192.168.0.71   192.168.0.1   ICMP         74 Echo (ping) request  id=0x0001,
```

12. Tráfico entre dos IP específicas:

ip.src == 192.168.1.10 && ip.dst == 192.168.1.20

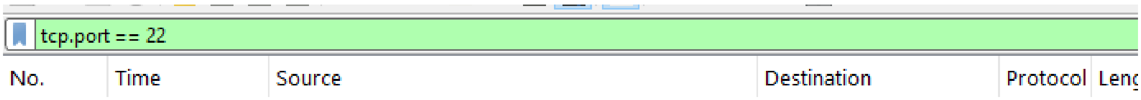


```
ip.src == 192.168.0.1 && ip.dst == 192.168.0.71
No.   Time        Source         Destination   Protocol Length  Info
   32 1.889220    192.168.0.1    192.168.0.71  ICMP         74 Echo (ping) reply    id=0x00
   43 2.891465    192.168.0.1    192.168.0.71  ICMP         74 Echo (ping) reply    id=0x00
```

Puertos

13. Tráfico en un puerto concreto (ej. 22 – SSH):

tcp.port == 22

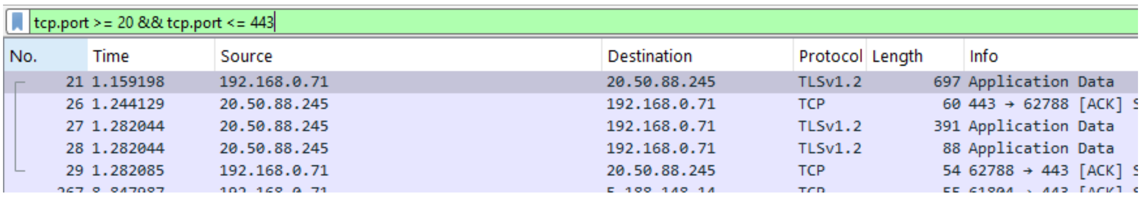


tcp.port == 22

No.	Time	Source	Destination	Protocol	Leng

14. **Tráfico en un rango de puertos (ej. 20 a 25):**

tcp.port >= 20 && tcp.port <= 25

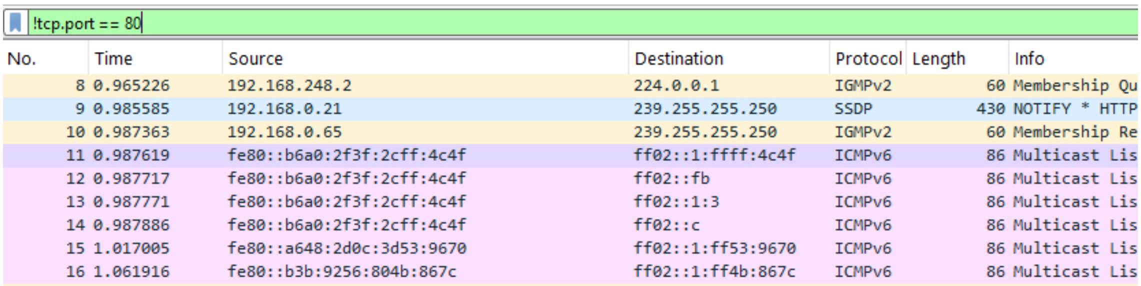


tcp.port >= 20 && tcp.port <= 443

No.	Time	Source	Destination	Protocol	Length	Info
21	1.159198	192.168.0.71	20.50.88.245	TLSv1.2	697	Application Data
26	1.244129	20.50.88.245	192.168.0.71	TCP	60	443 → 62788 [ACK]
27	1.282044	20.50.88.245	192.168.0.71	TLSv1.2	391	Application Data
28	1.282044	20.50.88.245	192.168.0.71	TLSv1.2	88	Application Data
29	1.282085	192.168.0.71	20.50.88.245	TCP	54	62788 → 443 [ACK]
267	8.847087	192.168.0.71	5.188.148.14	TCP	55	61804 → 443 [ACK]

15. **Tráfico NO en un puerto concreto (ej. todo excepto 80):**

!tcp.port == 80



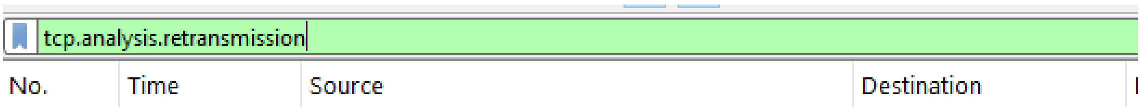
!tcp.port == 80

No.	Time	Source	Destination	Protocol	Length	Info
8	0.965226	192.168.248.2	224.0.0.1	IGMPv2	60	Membership Qu
9	0.985585	192.168.0.21	239.255.255.250	SSDP	430	NOTIFY * HTTP
10	0.987363	192.168.0.65	239.255.255.250	IGMPv2	60	Membership Re
11	0.987619	fe80::b6a0:2f3f:2cff:4c4f	ff02::1:ffff:4c4f	ICMPv6	86	Multicast Lis
12	0.987717	fe80::b6a0:2f3f:2cff:4c4f	ff02::fb	ICMPv6	86	Multicast Lis
13	0.987771	fe80::b6a0:2f3f:2cff:4c4f	ff02::1:3	ICMPv6	86	Multicast Lis
14	0.987886	fe80::b6a0:2f3f:2cff:4c4f	ff02::c	ICMPv6	86	Multicast Lis
15	1.017005	fe80::a648:2d0c:3d53:9670	ff02::1:ff53:9670	ICMPv6	86	Multicast Lis
16	1.061916	fe80::b3b:9256:804b:867c	ff02::1:ff4b:867c	ICMPv6	86	Multicast Lis

🔷 TCP avanzado

16. **Retransmisiones TCP:**

tcp.analysis.retransmission

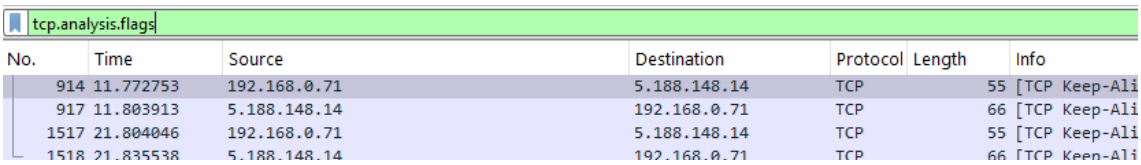


tcp.analysis.retransmission

No.	Time	Source	Destination

17. **Paquetes TCP con errores:**

tcp.analysis.flags

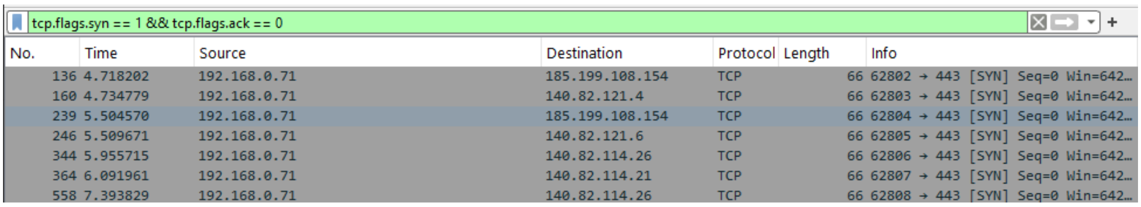


tcp.analysis.flags

No.	Time	Source	Destination	Protocol	Length	Info
914	11.772753	192.168.0.71	5.188.148.14	TCP	55	[TCP Keep-Ali
917	11.803913	5.188.148.14	192.168.0.71	TCP	66	[TCP Keep-Ali
1517	21.804046	192.168.0.71	5.188.148.14	TCP	55	[TCP Keep-Ali
1518	21.835538	5.188.148.14	192.168.0.71	TCP	66	[TCP Keep-Ali

18. **Solo handshakes TCP (SYN):**

tcp.flags.syn == 1 && tcp.flags.ack == 0

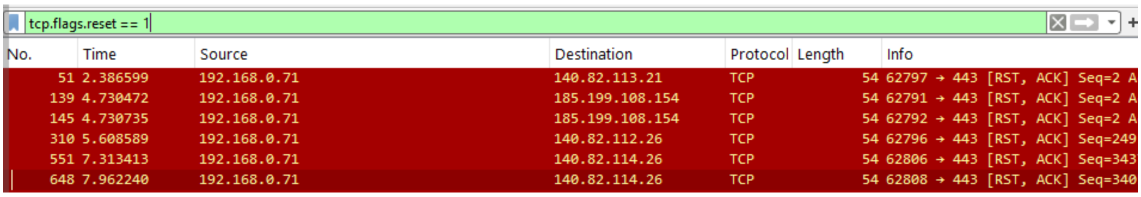


tcp.flags.syn == 1 && tcp.flags.ack == 0

No.	Time	Source	Destination	Protocol	Length	Info
136	4.718202	192.168.0.71	185.199.108.154	TCP	66	62802 → 443 [SYN] Seq=0 Win=642…
160	4.734779	192.168.0.71	140.82.121.4	TCP	66	62803 → 443 [SYN] Seq=0 Win=642…
239	5.504570	192.168.0.71	185.199.108.154	TCP	66	62804 → 443 [SYN] Seq=0 Win=642…
246	5.509671	192.168.0.71	140.82.121.6	TCP	66	62805 → 443 [SYN] Seq=0 Win=642…
344	5.955715	192.168.0.71	140.82.114.26	TCP	66	62806 → 443 [SYN] Seq=0 Win=642…
364	6.091961	192.168.0.71	140.82.114.21	TCP	66	62807 → 443 [SYN] Seq=0 Win=642…
558	7.393829	192.168.0.71	140.82.114.26	TCP	66	62808 → 443 [SYN] Seq=0 Win=642…

19. **Conexiones TCP reseteadas (RST):**

tcp.flags.reset == 1



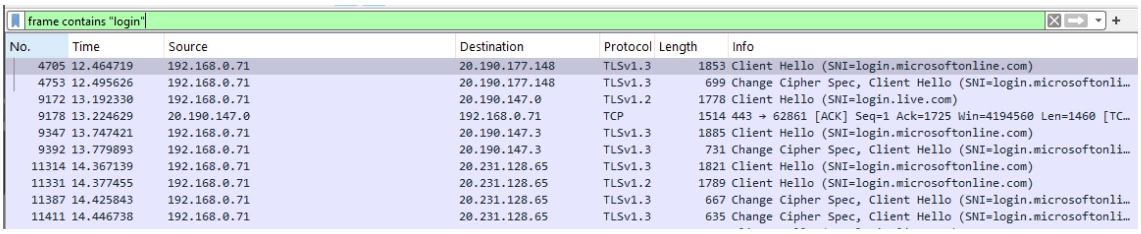
tcp.flags.reset == 1

No.	Time	Source	Destination	Protocol	Length	Info
51	2.386599	192.168.0.71	140.82.113.21	TCP	54	62797 → 443 [RST, ACK] Seq=2 A
139	4.730472	192.168.0.71	185.199.108.154	TCP	54	62791 → 443 [RST, ACK] Seq=2 A
145	4.730735	192.168.0.71	185.199.108.154	TCP	54	62792 → 443 [RST, ACK] Seq=2 A
310	5.608589	192.168.0.71	140.82.112.26	TCP	54	62796 → 443 [RST, ACK] Seq=249
551	7.313413	192.168.0.71	140.82.114.26	TCP	54	62806 → 443 [RST, ACK] Seq=343
648	7.962240	192.168.0.71	140.82.114.26	TCP	54	62808 → 443 [RST, ACK] Seq=340

🔷 Otros filtros útiles

20. **Mostrar solo paquetes que contienen un texto (ej. "login"):**

frame contains "login"



frame contains "login"

No.	Time	Source	Destination	Protocol	Length	Info
4705	12.464719	192.168.0.71	20.190.177.148	TLSv1.3	1853	Client Hello (SNI=login.microsoftonline.com)
4753	12.495626	192.168.0.71	20.190.177.148	TLSv1.3	699	Change Cipher Spec, Client Hello (SNI=login.microsoftonli…
9172	13.192330	192.168.0.71	20.190.147.0	TLSv1.2	1778	Client Hello (SNI=login.live.com)
9178	13.224629	20.190.147.0	192.168.0.71	TCP	1514	443 → 62861 [ACK] Seq=1 Ack=1725 Win=4194560 Len=1460 [TC…
9347	13.747421	192.168.0.71	20.190.147.3	TLSv1.3	1885	Client Hello (SNI=login.microsoftonline.com)
9392	13.779893	192.168.0.71	20.190.147.3	TLSv1.3	731	Change Cipher Spec, Client Hello (SNI=login.microsoftonli…
11314	14.367139	192.168.0.71	20.231.128.65	TLSv1.3	1821	Client Hello (SNI=login.microsoftonline.com)
11331	14.377455	192.168.0.71	20.231.128.65	TLSv1.2	1789	Client Hello (SNI=login.microsoftonline.com)
11387	14.425843	192.168.0.71	20.231.128.65	TLSv1.3	667	Change Cipher Spec, Client Hello (SNI=login.microsoftonli…
11411	14.446738	192.168.0.71	20.231.128.65	TLSv1.3	635	Change Cipher Spec, Client Hello (SNI=login.microsoftonli…