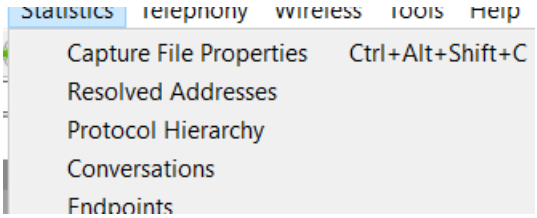
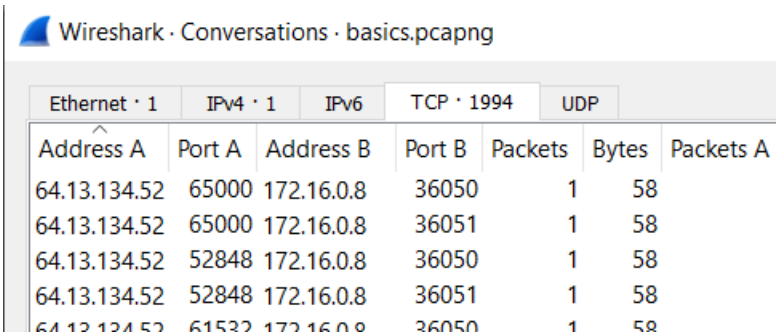
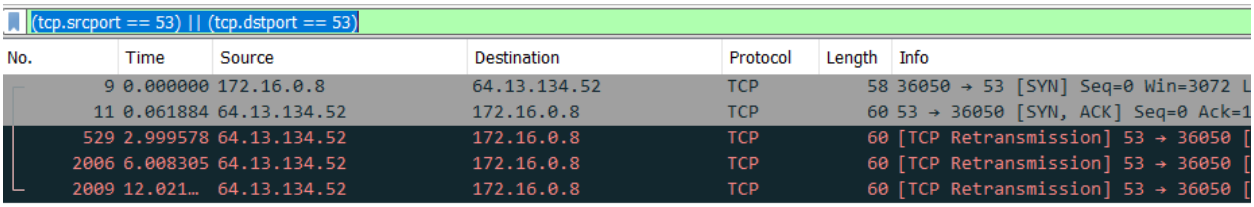




Address A	Port A	Address B	Port B	Packets	Bytes	Packets A
64.13.134.52	65000	172.16.0.8	36050	1	58	
64.13.134.52	65000	172.16.0.8	36051	1	58	
64.13.134.52	52848	172.16.0.8	36050	1	58	
64.13.134.52	52848	172.16.0.8	36051	1	58	
64.13.134.52	61532	172.16.0.8	36050	1	58	

Flag: 1994

Use this filter: (tcp.srcport == 53) || (tcp.dstport == 53) to find any source/dest ports of 53



Flag: 5

Filter: ip.dst == 64.13.134.52 we see a port scan and the only service that came back was on port 80.

ip.dst == 64.13.134.52

No.	Time	Source	Destination	Protocol	Length	Info
7	0.000052	172.16.0.8	64.13.134.52	TCP	58	36050 → 995 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
8	0.000054	172.16.0.8	64.13.134.52	TCP	58	36050 → 587 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
9	0.000052	172.16.0.8	64.13.134.52	TCP	58	36050 → 53 [SYN] Seq=0 Win=3072 Len=0 MSS=1460
10	0.000052	172.16.0.8	64.13.134.52	TCP	58	36050 → 5900 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
12	0.063306	172.16.0.8	64.13.134.52	TCP	58	36050 → 21 [SYN] Seq=0 Win=4096 Len=0 MSS=1460
13	0.000070	172.16.0.8	64.13.134.52	TCP	58	36050 → 113 [SYN] Seq=0 Win=4096 Len=0 MSS=1460
15	0.063659	172.16.0.8	64.13.134.52	TCP	58	36050 → 80 [SYN] Seq=0 Win=3072 Len=0 MSS=1460
16	0.000075	172.16.0.8	64.13.134.52	TCP	58	36050 → 139 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
18	0.062443	172.16.0.8	64.13.134.52	TCP	58	36050 → 3389 [SYN] Seq=0 Win=3072 Len=0 MSS=1460

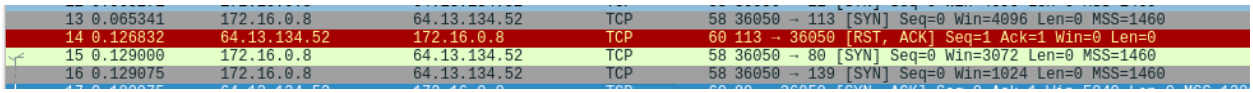
Flag: No

Back to Basics 4

20

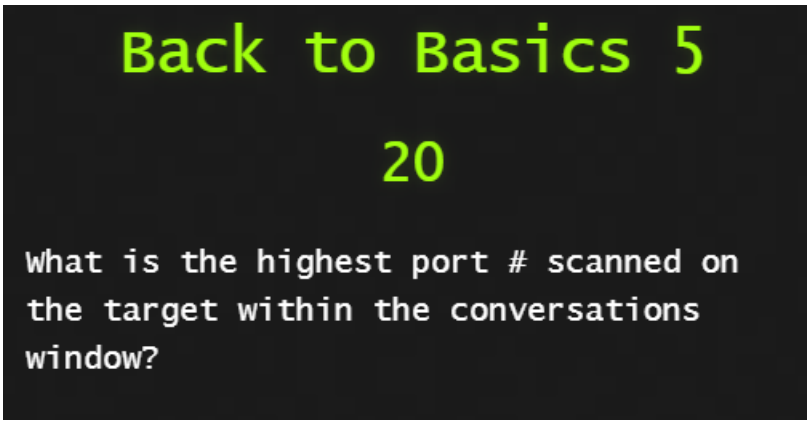
What additional bit(s) are set within the TCP header flags for the target host?

The target responded with a RST.

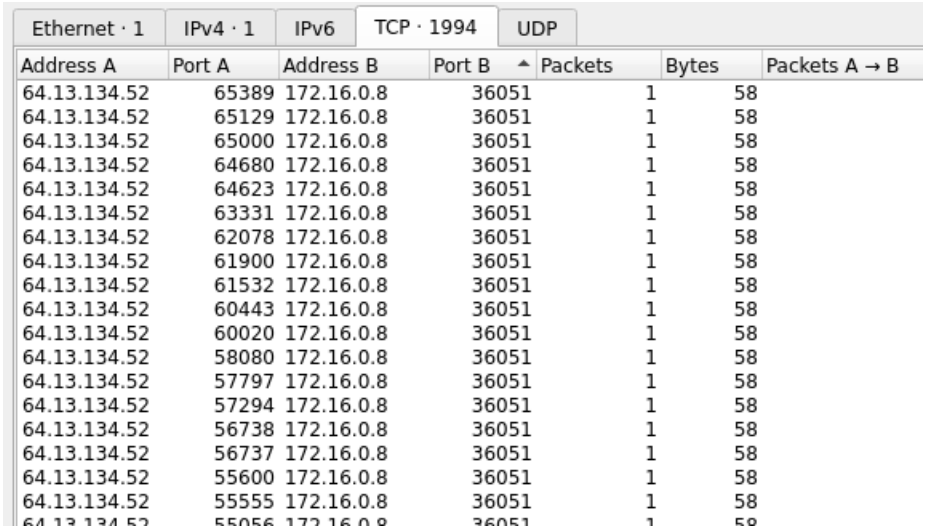


13	0.065341	172.16.0.8	64.13.134.52	TCP	58 36050 → 113 [SYN] Seq=0 Win=4096 Len=0 MSS=1460
14	0.126832	64.13.134.52	172.16.0.8	TCP	60 113 → 36050 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
15	0.129000	172.16.0.8	64.13.134.52	TCP	58 36050 → 80 [SYN] Seq=0 Win=3072 Len=0 MSS=1460
16	0.129075	172.16.0.8	64.13.134.52	TCP	58 36050 → 139 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

Flag: RST



Go to the conversations tab under statistics. Move over to the TCP tab and sort on PORT B



Ethernet · 1 | IPv4 · 1 | IPv6 | TCP · 1994 | UDP

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B
64.13.134.52	65389	172.16.0.8	36051	1	58	
64.13.134.52	65129	172.16.0.8	36051	1	58	
64.13.134.52	65000	172.16.0.8	36051	1	58	
64.13.134.52	64680	172.16.0.8	36051	1	58	
64.13.134.52	64623	172.16.0.8	36051	1	58	
64.13.134.52	63331	172.16.0.8	36051	1	58	
64.13.134.52	62078	172.16.0.8	36051	1	58	
64.13.134.52	61900	172.16.0.8	36051	1	58	
64.13.134.52	61532	172.16.0.8	36051	1	58	
64.13.134.52	60443	172.16.0.8	36051	1	58	
64.13.134.52	60020	172.16.0.8	36051	1	58	
64.13.134.52	58080	172.16.0.8	36051	1	58	
64.13.134.52	57797	172.16.0.8	36051	1	58	
64.13.134.52	57294	172.16.0.8	36051	1	58	
64.13.134.52	56738	172.16.0.8	36051	1	58	
64.13.134.52	56737	172.16.0.8	36051	1	58	
64.13.134.52	55600	172.16.0.8	36051	1	58	
64.13.134.52	55555	172.16.0.8	36051	1	58	
64.13.134.52	55056	172.16.0.8	36051	1	58	

Flag: 36051