

Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-F>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	199.0.0.46	199.0.0.154	TCP	60	59329 → 3389 [ACK] Seq=1 Ack=
2	0.002132	199.0.0.39	239.255.255.250	UDP	698	59142 → 3201 Len=656
3	0.080117	199.0.0.154	199.0.0.46	UDP	53	3389 → 56890 Len=11
4	0.097893	199.0.0.154	199.0.0.46	UDP	994	3389 → 56890 Len=952
5	0.135263	199.0.0.154	199.0.0.46	UDP	1279	3389 → 56890 Len=1237
6	0.135294	199.0.0.154	199.0.0.46	UDP	237	3389 → 56890 Len=195
7	0.250374	199.0.0.46	199.0.0.154	UDP	60	56890 → 3389 Len=12
8	0.374418	199.0.0.46	199.0.0.154	TLSv1.2	97	Application Data
9	0.375782	199.0.0.154	199.0.0.46	TLSv1.2	91	Application Data
10	0.382505	199.0.0.46	199.0.0.154	TLSv1.2	97	Application Data
11	0.399924	199.0.0.46	199.0.0.154	TLSv1.2	104	Application Data
12	0.400001	199.0.0.154	199.0.0.46	TCP	54	3389 → 59329 [ACK] Seq=38 Ack=
13	0.413764	199.0.0.46	199.0.0.154	TLSv1.2	104	Application Data
14	0.416623	199.0.0.41	199.0.0.255	NBNS	92	Name query NB DESKTOP-22JFBM6-
15	0.416941	199.0.0.41	224.0.0.251	MDNS	81	Standard query 0x0000 A deskto
16	0.417202	199.0.0.41	224.0.0.251	MDNS	81	Standard query 0x0000 AAAA des
17	0.417646	199.0.0.41	224.0.0.252	LLMNR	75	Standard query 0x8f29 A deskto
18	0.417909	199.0.0.41	224.0.0.252	LLMNR	75	Standard query 0xa69d AAAA des
19	0.418568	Dell_d3:12:22	Broadcast	ARP	60	Who has 199.0.0.56? Tell 199.0
20	0.429431	199.0.0.46	199.0.0.154	TLSv1.2	104	Application Data
21	0.429507	199.0.0.154	199.0.0.46	TCP	54	3389 → 59329 [ACK] Seq=38 Ack=
22	0.441982	199.0.0.154	199.0.0.46	UDP	391	3389 → 56890 Len=349
23	0.446664	199.0.0.46	199.0.0.154	TLSv1.2	104	Application Data
24	0.462240	199.0.0.46	199.0.0.154	TLSv1.2	104	Application Data
25	0.462313	199.0.0.154	199.0.0.46	TCP	54	3389 → 59329 [ACK] Seq=38 Ack=

<

> Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{28219D41-4ED8-408D-8000-000000000000}

Ethernet II, Src: Dell 89:6a:2f (8c:ec:4b:89:6a:2f), Dst: Dell 9c:e5:c3 (f8:b1:56:9c:e5:c3)

0000	f8 b1 56 9c e5 c3 8c ec 4b 89 6a 2f 00 00 45 00	..V.....K-j/-E.
0010	00 28 27 4d 40 00 80 06 44 ba c7 00 00 2e c7 00	..('M@...D.....
0020	00 9a e7 c1 0d 3d 52 0e 6e 30 54 83 9e d0 50 10	R..nBT...P.
0030	20 11 58 69 00 00 00 00 00 00 00 00	..Xi.....

نشاط مشبوه

نشاط غير مشبوه