

Packet ID	Date	Mac Address	Protocol	Source Address	Dest. Address	Source Port	Dest. Port	Packet Length	LOG prefix	Time To Live
24093	2023-03-21 2:24	00:0d:3a:f3:8e:0e:d4:af:f7:48:3e:e8:08:00	TCP	10.56.177.4	192.168.89.36	49768	22	40	SSH INPUT LS-89	128
24143	2023-03-21 1:52		TCP	192.168.89.36	10.56.177.4	22	49768	116	SSH OUTPUT WC-10.56.177.4:	64
57451	2023-03-15 0:05	00:0d:3a:0c:3b:59:c0:d6:82:33:2d:a1:08:00	TCP	10.56.177.4	172.17.89.37	51318	21	52	DNS UDP FORWARD:	127
2040	2023-03-21 1:56	00:0d:3a:f3:8e:0e:d4:af:f7:48:3e:e8:08:00	TCP	10.56.177.4	172.17.89.37	50400	80	52	HTTP FORWARD WS-89	127
7968	2023-03-21 19:29	00:22:48:b0:61:aa:d4:af:f7:3b:c0:04:08:00	UDP	10.56.177.4	172.17.89.36	50787	53	41	DNS TCP FORWARD	127
9918	2023-03-21 1:56	00:0d:3a:f3:8e:0e:d4:af:f7:48:3e:e8:08:00	TCP	10.56.177.4	172.17.89.36	50403	80	52	HTTP FORWARD LS-89	127
2044	2023-03-21 1:56	00:0d:3a:f3:8e:0e:d4:af:f7:48:3e:e8:08:00	TCP	10.56.177.4	172.17.89.37	50105	3306	40	MySQL FORWARD LS-89	127
9848	2023-03-21 1:55	00:0d:3a:f3:8e:0e:d4:af:f7:48:3e:e8:08:00	TCP	10.56.177.4	172.17.89.36	50391	21	52	FTP CONTROL PLANE FORWARD WS-	127

1. What is Packet ID? Does it follow a sequence or is it random? How can you prove / demonstrate your answer?

Packet ID distinguishes a packet from other packets and ensures that they are sent to the proper location. They appear to be in sequence which I witnessed in tcpdump.

```

.49724: Flags [P
3, length 276
4, id 19188, offs

.49724: Flags [P
3, length 276
4, id 19189, offs

.49724: Flags [P
3, length 276
4, id 19190, offs

.49724: Flags [P
3, length 276
4, id 19191, offs

.49724: Flags [P
3, length 276
4, id 19192, offs

```

1. Why Windows Client Source Port is not related to the kind of service requested? Why for example SSH request is coming from a random Source Port instead of port 22? Is there any way you can fix request port number? If yes give example, if no elaborate?

Windows Client Source Port is dynamic opposed to being static, which means it uses a random port instead of a fixed one. This can be changed by setting a specific port number in the registry.

1. Answer previous question for DNS service? Can you explain the random Source Port issue?

DNS service is also dynamic and would also explain why the Source Port is different.

1. What is MAC address? Can you find the MAC addresses of your Network Interface Cards in Azure Portal? How?

MAC address is a physical unique identifier that a network uses to identify devices. You can find the MAC address under properties in network interfaces.



