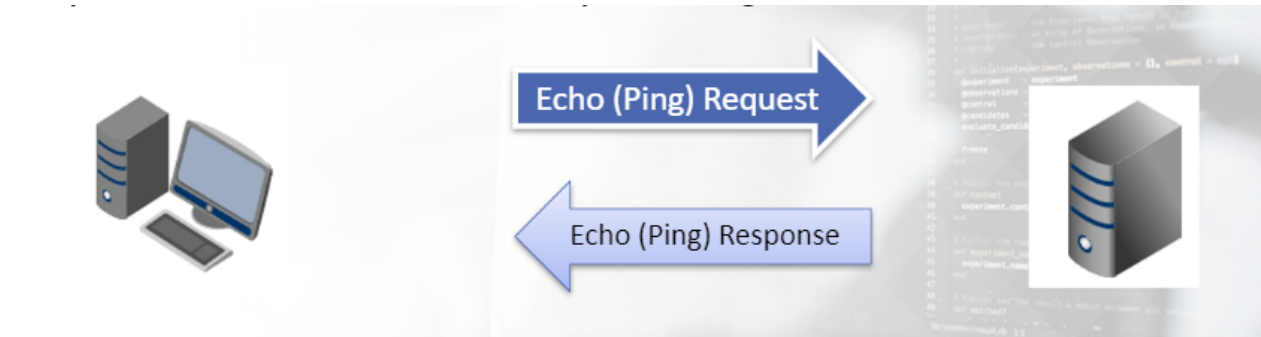


ICMP Traffic:

ICMP stands for Internet Control Message Protocol, this protocol is mainly used to see if a node or device within the network receive connection, to if its active. Its used with tools like ping, and tracer.

Here is a visualize way of how the ping works:



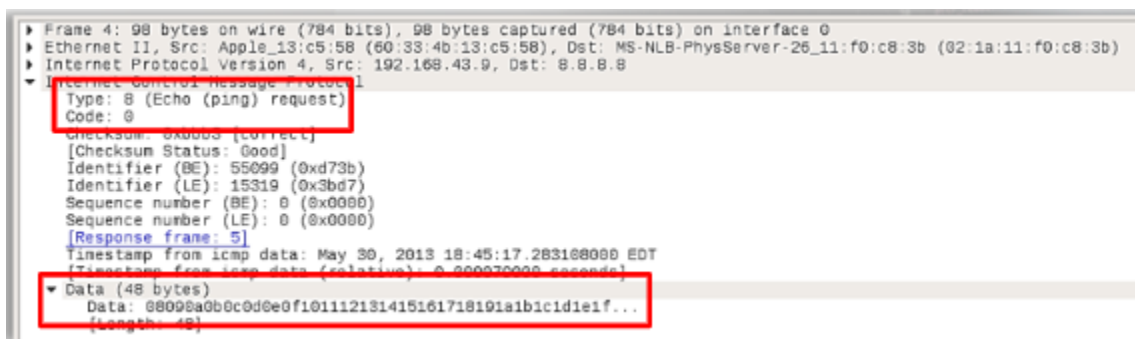
Here is some ICMP Request Echo (Ping) and Reply Echo (ping) Replay:

4	5.013334	192.168.43.9	8.8.8.8	ICMP	98 Echo (ping) request	id=0xd73b, seq=0/0, ttl=64 (reply in 5)
5	5.505538	8.8.8.8	192.168.43.9	ICMP	98 Echo (ping) reply	id=0xd73b, seq=0/0, ttl=40 (request in 4)
6	6.019290	192.168.43.9	8.8.8.8	ICMP	98 Echo (ping) request	id=0xd73b, seq=1/256, ttl=64 (reply in 7)
7	6.153653	8.8.8.8	192.168.43.9	ICMP	98 Echo (ping) reply	id=0xd73b, seq=1/256, ttl=40 (request in 6)
8	7.015108	192.168.43.9	8.8.8.8	ICMP	98 Echo (ping) request	id=0xd73b, seq=2/512, ttl=64 (reply in 9)
9	7.781987	8.8.8.8	192.168.43.9	ICMP	98 Echo (ping) reply	id=0xd73b, seq=2/512, ttl=40 (request in 8)

We see "Echo (ping) request" which is the ICMP request or we can ping, and we see "Echo (ping) reply" which is reply to the ping request.

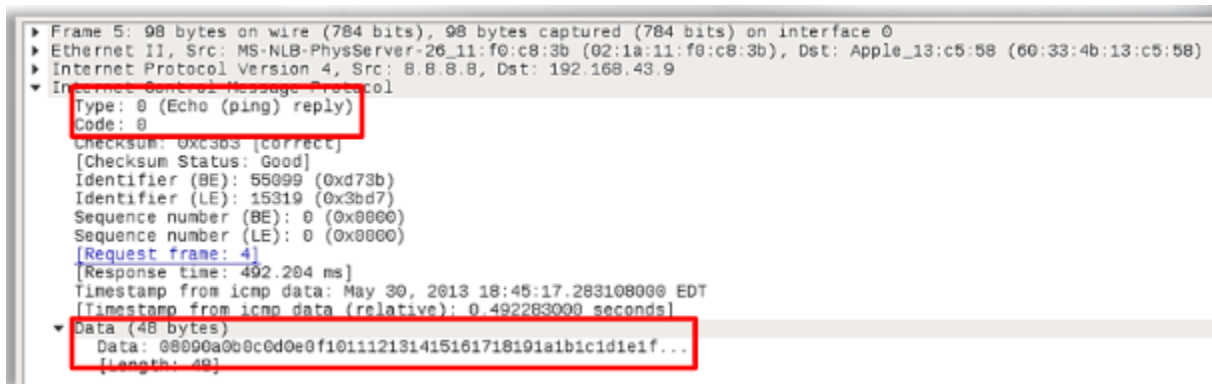
Normal ICMP:

The Request:



Here we see the "Type: 8" which indicates its ICMP Request. And the data section has random text in it and its usually **48 bytes**:

The Response or the Reply:



Here we see the “Type: 0” and this mean it’s a replay. And we see some random data in the Data section:

As we can guess or imagine, the Data filed of an ICMP packet be used as covert channel to send commands or even exfiltrate data, so Large ICMP packets should be a RED flag.

And we should also look for unusual types/codes in the ICMP packet such as timestamp.

And the ICMP can also be used for Host discovery, like an attacker compromise a host within the network and to discover the hosts, it might use ICMP Ping to see what IPs are active within the network