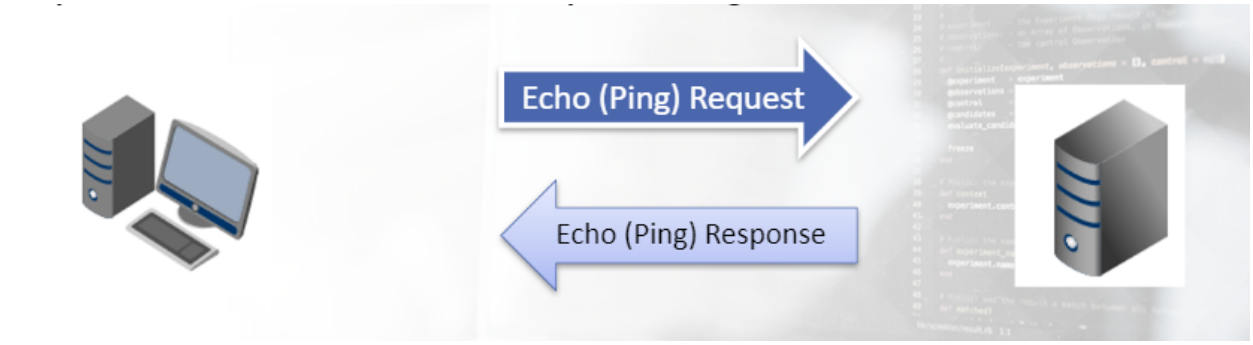
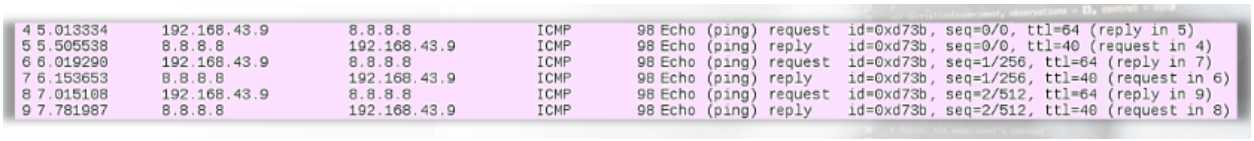
ICMP Traffic:

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 tracert.

Here is a visualize way of how the ping works:



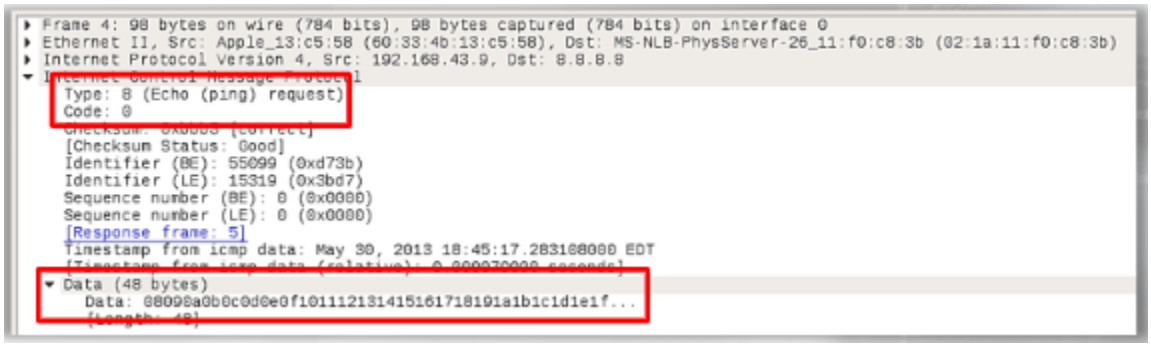
Here is some ICPM Request Echo (Ping) and Reply Echo (ping) Replay:



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

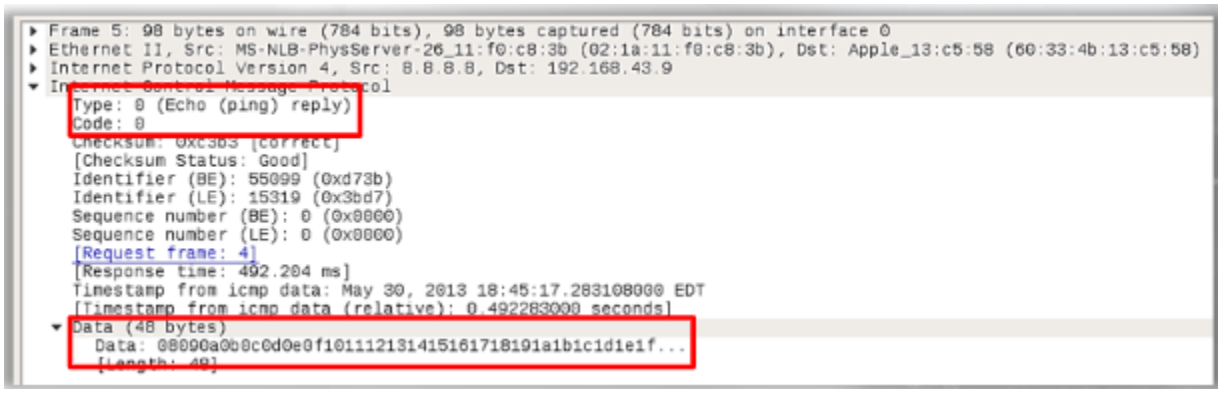
Normal ICMP:

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