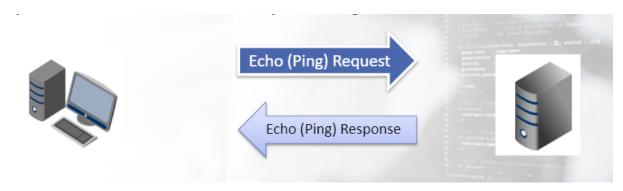
## **ICMP Traffic:**

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:

4 5.013334	192.168.43.9	8.8.8.8	ICMP	98 Echo (ping) request	id=0xd73b, seg=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	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 replay to the ping request.

## Normal ICMP:

## The Request:

```
Frame 4: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0

Ethernet II, Src: Apple_13:c5:58 (60:33:4b:13:c5:58), Dst: MS:NLB-PhysServer-26_11:f0:c8:3b (92:1a:11:f0:c8:3b)

Internet Protocol Version 4, Src: 192.168.43.9, Dst: 8.8.8.8

| Internet Protocol Version 4, Src: 192.168.43.9, Dst: 8.8.8.8

| Internet Protocol Version 4, Src: 192.168.43.9, Dst: 8.8.8.8

| Internet Protocol Version 4, Src: 192.168.43.9, Dst: 8.8.8.8

| Internet Protocol Version 4, Src: 192.168.43.9, Dst: 8.8.8.8

| Internet Protocol Version 4, Src: 192.168.43.9, Dst: 8.8.8.8

| Internet Protocol Version 4, Src: 192.168.43.9, Dst: 8.8.8.8

| Internet Protocol Version 4, Src: 192.168.43.9, Dst: 8.8.8.8

| Internet Protocol Version 4, Src: 192.168.43.9, Dst: 8.8.8.8

| Internet Protocol Version 4, Src: 192.168.43.9, Dst: 8.8.8.8

| Internet Protocol Version 4, Src: 192.168.43.9, Dst: 8.8.8.8

| Internet Protocol Version 4, Src: 192.168.43.9, Dst: 8.8.8.8

| Internet Protocol Version 4, Src: 192.168.43.9, Dst: 8.8.8.8

| Internet Protocol Version 4, Src: 192.168.43.9, Dst: 8.8.8.8

| Internet Protocol Version 4, Src: 192.168.43.9, Dst: 8.8.8.8

| Internet Protocol Version 4, Src: 192.168.43.9, Dst: 8.8.8.8

| Internet Protocol Version 4, Src: 192.168.43.9, Dst: 8.8.8.8

| Internet Protocol Version 4, Src: 192.168.43.9, Dst: 8.8.8.8

| Internet Protocol Version 4, Src: 192.168.43.9, Dst: 8.8.8.8

| Internet Protocol Version 4, Src: 192.168.43.9, Dst: 8.8.8.8

| Internet Protocol Version 4, Src: 192.168.43.9, Dst: 8.8.8.8

| Internet Protocol Version 4, Src: 192.168.43.9, Dst: 8.8.8.8

| Internet Protocol Version 4, Src: 192.168.43.9, Dst: 8.8.8.8

| Internet Protocol Version 4, Src: 192.168.43.9, Dst: 8.8.8.8

| Internet Protocol Version 4, Src: 192.168.43.9, Dst: 8.8.8.8

| Internet Protocol Version 4, Src: 192.168.43.9, Dst: 8.8.8.8

| Internet Protocol Version 4, Src: 192.168.43.9, Dst: 8.8.8.8

| Internet Protocol Version 4, Src: 192.168.43.9, Dst: 8.8.8.8

| Internet Protocol Version 4, Src: 192.168.43.9, Dst: 8.8.8
```

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:

```
▶ Frame 5: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
▶ Ethernet II, Src: MS-NLB-PhysServer-26_11:f0:c8:3b (02:1a:11:f0:c8:3b), Dst: Apple_13:c5:58 (60:33:4b:13:c5:58)
▶ Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.43.9
▼ Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.43.9
▼ Internet Solve I Status (00:10)
■ Code: 0
■ Checksum: Oxcobs [correct]
■ Checksum: Oxcobs [correct]
■ Checksum: Status: Good]
■ Identifier (BE): 55099 (0xd73b)
■ Identifier (BE): 55099 (0xd73b)
■ Identifier (BE): 0 (0x9800)
■ Sequence number (BE): 0 (0x9800)
■ Sequence number (BE): 0 (0x9800)
■ Request frame: 4]
■ [Response time: 492.204 ms]
■ Timestamp from icmp data: May 30, 2013 18:45:17.283108900 EDT
■ [Imestamp from icmp data (relative): 0.492283000 seconds]
■ Data: (48 bytes)
```

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