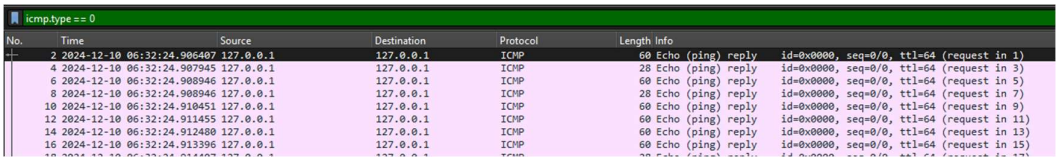
THE ECHOES

Description:

Null

1. **Filter icmp with the Echo (ping) reply only with the query of :**

icmp.type==0



2. **We can save the data Export as csv or simply use command.**

3. **Use commandline to extract**

Using command extracts the data information from a network capture file. It filters for specific ICMP packets (type 0), picks out certain data fields, and processes them step by step. First, uses tshark to read the file and extract the relevant data. Then, awk selects and formats parts of the data. The processed data is converted back to binary using xxd.

```
$
tshark -r TheEchos.pcap -Y "icmp.type == 0" -T fields -e data | awk 'NF
{print substr($0, 1, 2)}' ORS='' | xxd -r -p
```

4. **Grep the flag**

Reading through file there is actually ***'STOUTCTF'***. We can grep it for the specific text that we want.


```
$
tshark -r TheEchos.pcap -Y "icmp.type == 0" -T fields -e data | awk 'NF
{print substr($0, 1, 2)}' ORS='' | xxd -r -p | grep -o 'STOUTCTF{[^}]*}'
```

Flag	STOUTCTF{fZtPEj720e1OKFrQPqouICBdgVAtD14N}