



THE ECHOES

Description:

Null

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

```
icmp.type==0
```

No.	Time	Source	Destination	Protocol	Length	Info
2	2024-12-10 06:32:24.905407	127.0.0.1	127.0.0.1	ICMP	60	Echo (ping) reply id=0x0000, seq=0/0, ttl=64 (request in 1)
4	2024-12-10 06:32:24.907945	127.0.0.1	127.0.0.1	ICMP	28	Echo (ping) reply id=0x0000, seq=0/0, ttl=64 (request in 3)
6	2024-12-10 06:32:24.908946	127.0.0.1	127.0.0.1	ICMP	60	Echo (ping) reply id=0x0000, seq=0/0, ttl=64 (request in 5)
8	2024-12-10 06:32:24.908946	127.0.0.1	127.0.0.1	ICMP	28	Echo (ping) reply id=0x0000, seq=0/0, ttl=64 (request in 7)
10	2024-12-10 06:32:24.910451	127.0.0.1	127.0.0.1	ICMP	60	Echo (ping) reply id=0x0000, seq=0/0, ttl=64 (request in 9)
12	2024-12-10 06:32:24.911455	127.0.0.1	127.0.0.1	ICMP	60	Echo (ping) reply id=0x0000, seq=0/0, ttl=64 (request in 11)
14	2024-12-10 06:32:24.912488	127.0.0.1	127.0.0.1	ICMP	60	Echo (ping) reply id=0x0000, seq=0/0, ttl=64 (request in 13)
16	2024-12-10 06:32:24.913396	127.0.0.1	127.0.0.1	ICMP	60	Echo (ping) reply id=0x0000, seq=0/0, ttl=64 (request in 15)

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.

```
ep1QH5tCtE1tpQPpt1xxngRcXtOKBPFDBH6tAcWj7q8yna9RZSNQ
xgcKqR3Qe1fw6Ukyx6vRo9vpMwEKVXjkgW9VasHCQRvts7Qe3hQTzG
vHmEKWQgg4K5zgDiozrv01jgRTE8NppLeKgOACHmUTq3VQAATYvb2
D0iR0fKf0i1eKt41W9tQi8ttLcFwuc08NUNbnpEoToD70AKRESTo1
jwT0h3eLAypZQk2IUNThn4TtWbE4VYgTZHhXJBVL4qMccGUpmCLCM
PqcwV2ZSTOUTCTF{fZtPEj720e10KFrQPqouICBdgVAtD14N}zrIg
ZEpu7Sa0wfmCMRvq1atIKYc5zCFg4puLM4gcqd0IPD6uR2sGd7Cqa
77LIgPnXVgxCoCSzgoYhAzKkpP9Wah5nKou5JBcAjA6TXeSzzkCF2
XSNPKW2pGUUrBkpw0kJO5JGuwIbx09WRQQkv6wsAXvW4KzvTB322dJ
A4F619V7u3DXL BqvATA01WJ5HTMUqCz25WDB3zmNYb47bXfPMbi7v
$
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{[^}]*}'
```

```
(osiris@ALICE) ~/Downloads/CTF/STOUTCTF/Forensic/Echoes
$ 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{[^}]*}'
STOUTCTF{fZtPEj720e10KFrQPqouICBdgVAtD14N}
```

Flag STOUTCTF{fZtPEj720e10KFrQPqouICBdgVAtD14N}