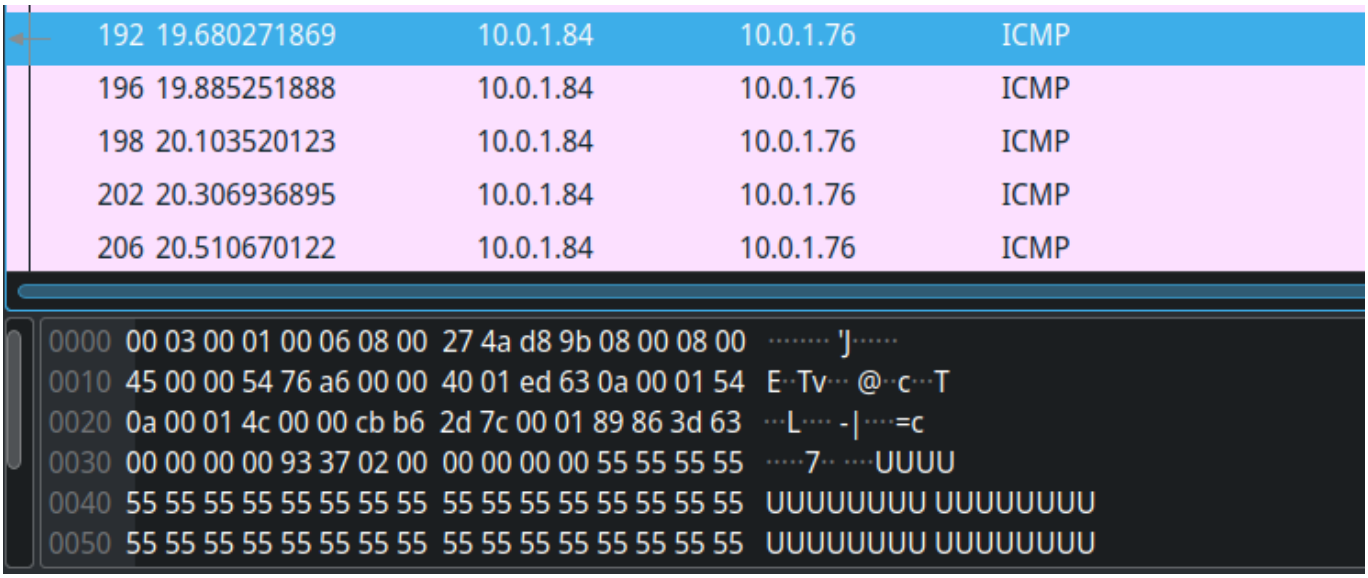
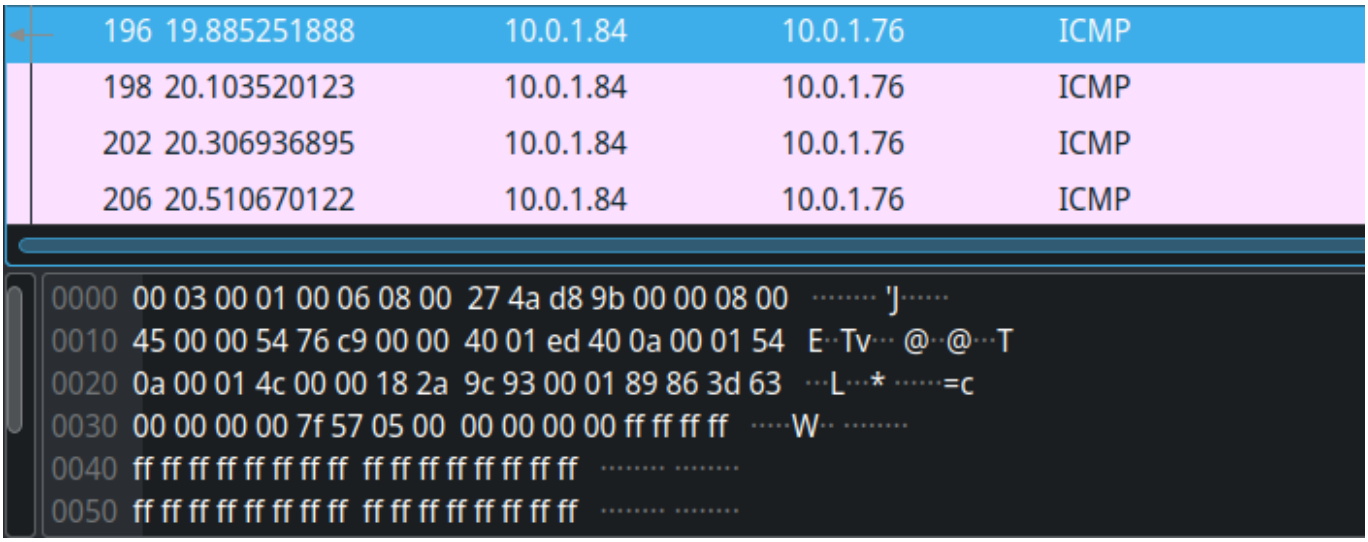
SusPaquet

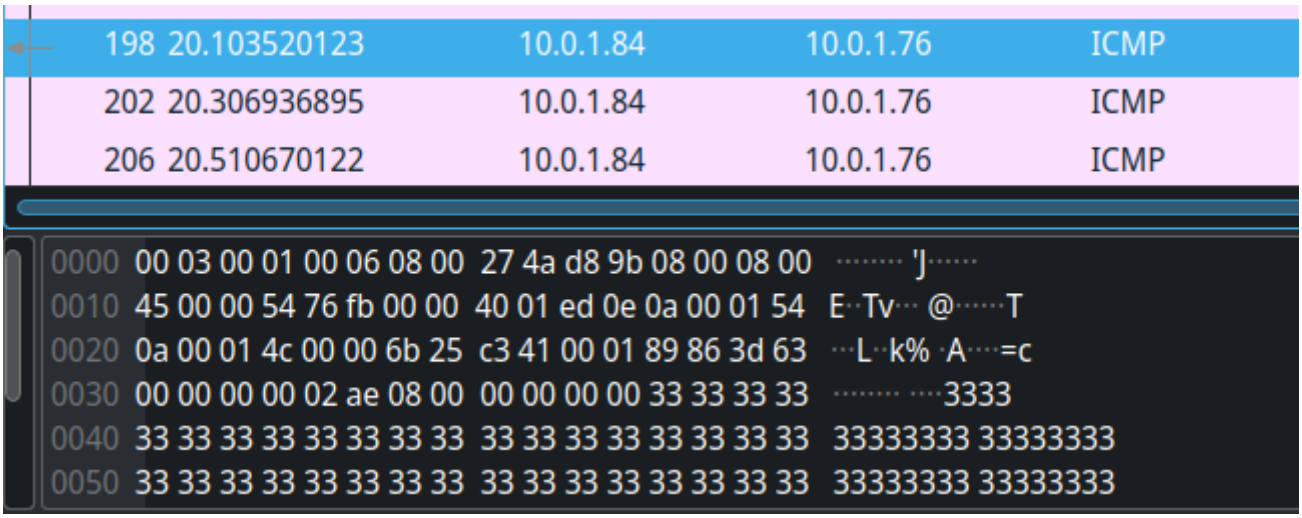
Auteur: bWlrYQ

1. Recon

La capture semble de prime abord tout à fait banale, il n'y a que des protocoles de base en revanche on peut remarquer que le buffer ICMP n'est pas celui par défaut et qu'il change à chaque echo request.







Quand on regarde encore plus le charset utilisé est celui de l'hexadécimal, on peut essayer de décoder ça en prenant la première lettre du buffer à chaque fois.

2. Décodage et flag

On peut faire ce sympathique one-liner 😃

```
tshark -r susPaquet.pcapng -Y '(ip.src==10.0.1.76 && icmp)' -x | grep "^0050" |
cut -d ' ' -f 3 | cut -c1 | tr -d '\n' | xxd -r -p
```

Et voilà:

Flag: FMCTF{IcMp_1sNt_CompLicAtEd_!!!}

Note: mes compliments à ceux qui le feront à la main, vous avez du courage 😃))