Wanl (1) : WireShark :

1 ligne = 1 paquet

au milieu → on a la présentat° de chaque paquet.

Pour avoir WireShark dans l'interface de ligne de commandes on met :

puis code = su
puis system wireshark

Dans wireshark on prend eth1.

→ détails

→ @ mac de source & destinat°

3e partie → ce qui est vraiment capturé

interprétat° des caractères en ASCII des bytes à gauche.

Analyse manuelle :

- ETHERNET :

@ destinat° : 00 23 48 22 02 3c

@ src : b8 6b 23 97 8a 79.

EtherType : 08 00.

- IP :

Type : 41 version 4

IHL : 5 = 20 bytes

TOS : X 00

Longueur totale : 02 0a

Identificateur : fa 87

F1 & F0 : 40 00

TTL : 40 → 40 x 16 = 64

Protocole : 6b

Checksum : 2b 5c

@ src : ~~08 00 45 00~~ 00 a8 01 05

Préambule	@ destinat°	@ source	EtherType	données	CRC
8	6	6	2	46 à 1500	4

@ dest: 58 6b 23 97 50 1f a1 3d.

TCP:

port source: 8b ff

port dest: 00 50

Num SEQ: 91 52 02 36.

Num ACK: 0e 7f 84 32.

THL & Flag: 80 18

Taille fenêtre: 00 ed

Somme CTRL: 1507

Pointeur urgence: 00 00

Option: 01 01 08 0a 05 68 fb 1f 43 57 97 59

Capture de paquet via TcpDump:

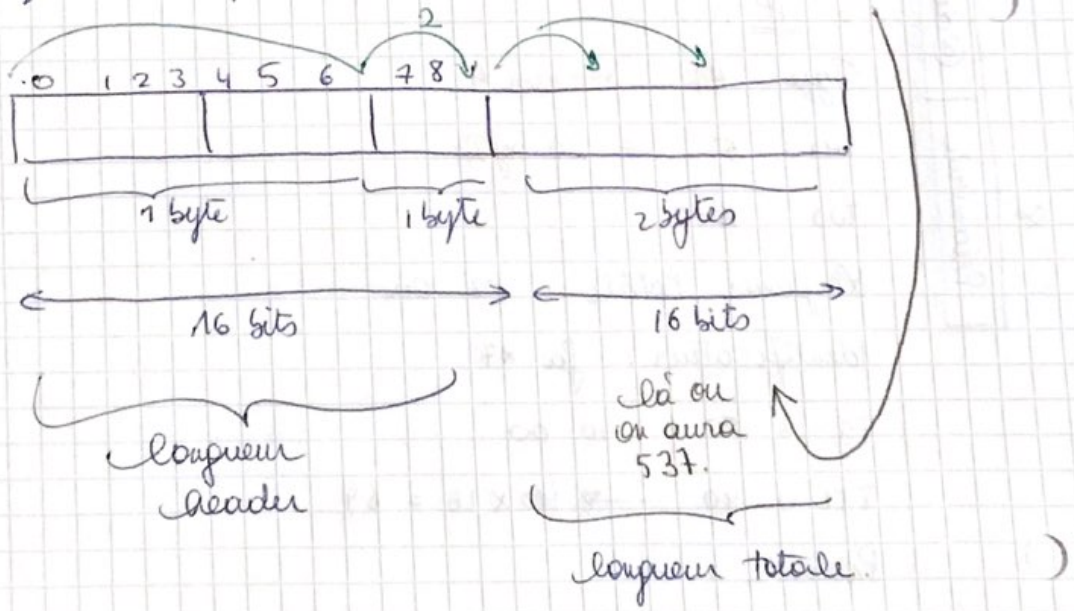
TCPDump → on peut enregistrer les captures dans 1 fichier qui pourra être ouvert

Dump a besoin de permissions donc on doit copier son contenu dans un autre fichier.

cat dump01.dmp > dump02.dmp

'ip [2:2] = 537'

↳ au champ 2 on avance de 2 à la valeur 537.



Comparer nos réponses en les refaisant d'1 autre manière!