M1 CMI ISR
IBIS Ibrahim

Rapport Analyseur réseau

Après avoir effectué la commande `make`, le programme peut être lancé comme ci-dessous :

Capture en ligne :

```
./bin/analyse -i <interface> -v <1..3>
```

Depuis un fichier :

```
./bin/analyse -o <fichier_capture> -v <1..3>
```

Application d'un filtre :

```
./bin/analyse -i <interface> -v <1..3> -f 'src port 80'
```

Plusieurs captures sont fournis dans le dossier `src/traces/` afin de pouvoir faire des tests.

Les protocoles disponibles sont : `Ethernet, IP, TCP, UDP, HTTP, TELNET, ARP, BOOTP/DHCP, FTP, IMAP, SMTP, POP.`

Trois types d'affichage sont possibles

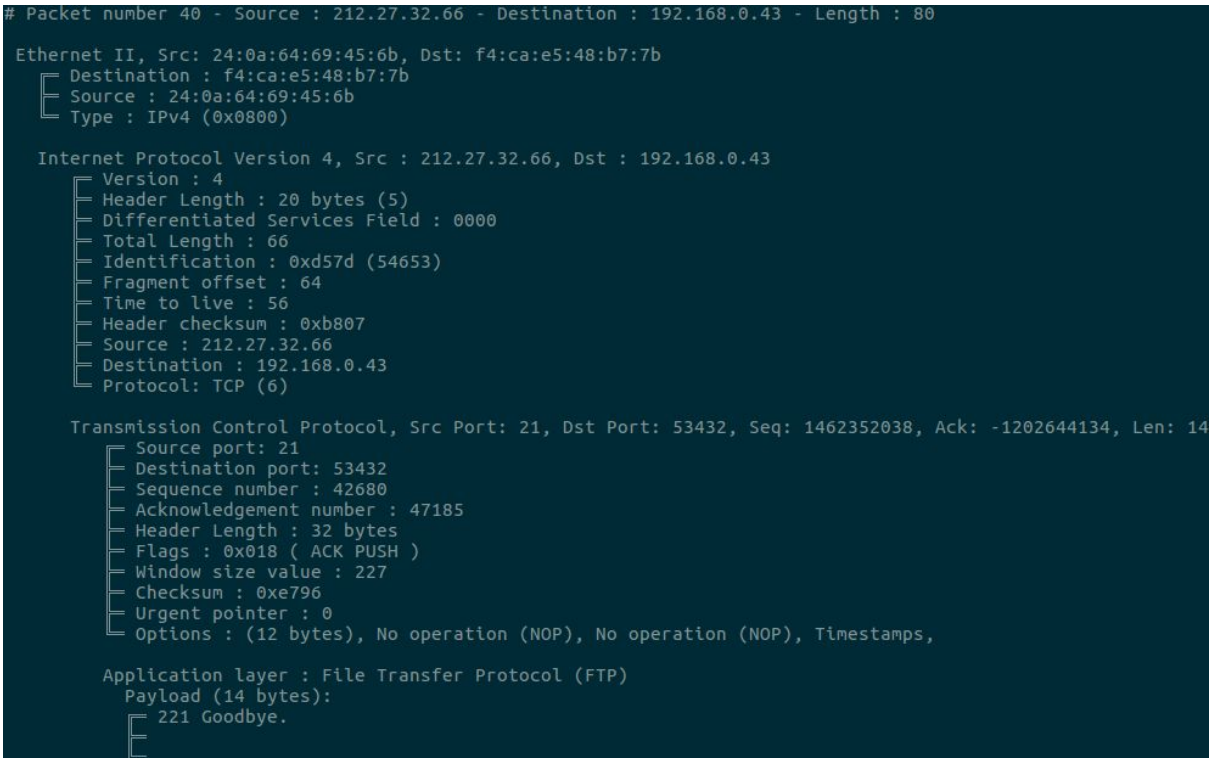
- très concis : une ligne par trame (`-v 1`)

```
# Packet number 1 - Source : 0.0.0.0 - Destination : 255.255.255.255  - Protocol : BOOTP/DHCP - Length : 324 - Info : DHCP Discover - Transaction ID 0xac2effff
```

- synthétique : une ligne par protocole, soit quelques lignes par trame (`-v 2`)

```
# Packet number 38 - Source : 217.13.4.24 - Destination : 192.168.170.56 - Length : 83
Ethernet II, Src: 00:60:08:45:e4:55, Dst: 00:12:a9:00:32:23
  Internet Protocol Version 4, Src : 217.13.4.24, Dst : 192.168.170.56
     User Datagram Protocol, Src Port: 53, Dst Port: 1711
       Application layer : DNS
```

- complet : la totalité des champs protocolaires et des contenus applicatifs (`-v 3`)


Packet number 40 - Source : 212.27.32.66 - Destination : 192.168.0.43 - Length : 80
Ethernet II, Src: 24:0a:64:69:45:6b, Dst: f4:ca:e5:48:b7:7b
Destination : f4:ca:e5:48:b7:7b
Source : 24:0a:64:69:45:6b
Type : IPv4 (0x0800)
Internet Protocol Version 4, Src : 212.27.32.66, Dst : 192.168.0.43
Version : 4
Header Length : 20 bytes (5)
Differentiated Services Field : 0000
Total Length : 66
Identification : 0xd57d (54653)
Fragment offset : 64
Time to live : 56
Header checksum : 0xb807
Source : 212.27.32.66
Destination : 192.168.0.43
Protocol: TCP (6)
Transmission Control Protocol, Src Port: 21, Dst Port: 53432, Seq: 1462352038, Ack: -1202644134, Len: 14
Source port: 21
Destination port: 53432
Sequence number : 42680
Acknowledgement number : 47185
Header Length : 32 bytes
Flags : 0x018 (ACK PUSH)
Window size value : 227
Checksum : 0xe796
Urgent pointer : 0
Options : (12 bytes), No operation (NOP), No operation (NOP), Timestamps,
Application layer : File Transfer Protocol (FTP)
Payload (14 bytes):
221 Goodbye.