université de BORDEAUX

TD3 - Analyse de Trames

1 Analyse d'un Paquet IP

Voici un paquet IP contenant un datagramme TCP contenant un extrait de connexion FTP. Le contenu du paquet est donné en format hexadécimal et chaque ligne représente 16 octets.

```
0x00:  45 00 00 48|5d cb 40 00|3a 06 16 2f|0b 0c 0d 0e
0x10:  0b 0c 0d 0f|00 15 04 01|f7 90 50 b5|18 fa 80 3f
0x20:  80 18 00 2e|47 f2 00 00|01 01 08 0a|1c 92 0d 8a
0x30:  00 3a b7 ac|53 53 48 2d|32 2e 30 2d|4f 70 65 6e
0x40:  53 53 48 5f|34 2e 33 0a
```

Chaque caractère `'|'` de la trame correspond à la fin d'une ligne dans la description de format correspondante [1], donc tous les 4 octets. Vous trouverez en annexe (ci-dessous) les formats des en-têtes IP et TCP. Vous pouvez la dégraffer pour plus de facilités. L'en-tête IP commence donc par 45 00 et se termine par 0d 0f (20 octets en tout), et l'entête TCP commence par 00 15 et se termine par 00 00 (20 octets en tout) [2]

1. Quelles sont les adresses IP de la source et du destinataire ?
2. Quel est le numéro de port de la source ? À votre avis, la source correspond-t-elle à un client ou à un serveur ? Justifier votre réponse.
3. Même question pour le port destination.

2 Analyse de Trames Ethernet

On rappelle qu'une trame Ethernet est composé d'un en-tête de 14 octets, d'au moins 46 octets de données et de 4 octets pour le code CRC. Vous trouverez en annexe (ci-dessous) des détails sur le contenu d'un en-tête Ethernet. On considère une capture tcpdump de trames visualisée grâce à l'outil Wireshark (voir Figure 1). La partie supérieure de la fenêtre représente toutes les trames de la capture et la partie inférieure représente le détail de la trame 6 en surbrillance.

1. On précise que ces caractères ont été rajoutés à des fins pédagogiques. Ils ne seront jamais présent sur une trame classique.
2. plus 12 octets d'options

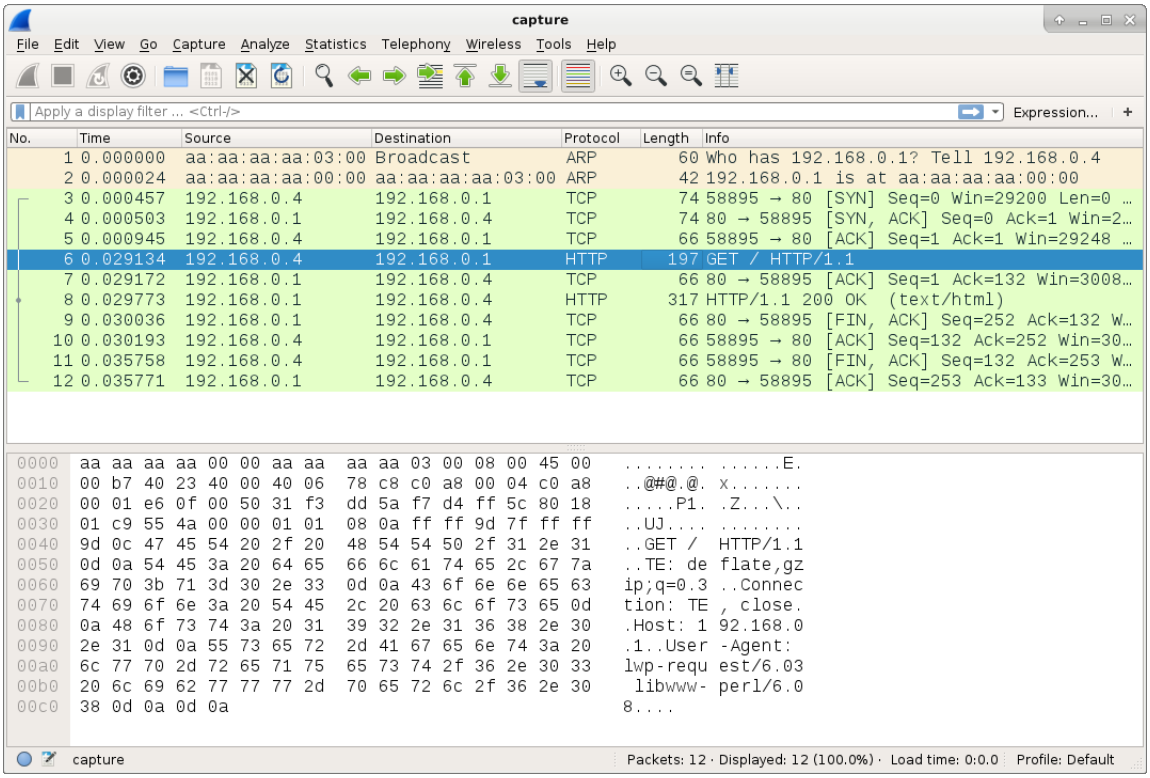


FIGURE 1 – Capture tcpdump visualisé avec Wireshark

1. Décrire précisément le rôle des trames n° 1 et 2 ?
2. Quel est le rôles des trames n° 3 à 5 ? De même, quel est le rôle des trames n° 9 à 12 ?
3. A quoi correspond selon vous l'échange des trames n° 6 et 8 ?

On se concentre maintenant sur le détail de la trame n° 6.

1. Quelle est l'adresse MAC source et destination ? Quelle est la valeur correspondant au protocole réseau (en hexa) ? Il s'agit du protocole IPv4.
2. Dans le paquet IP, quelle est la valeur du champs hdrl (HeaDeR Length) ? Ce nombre représente la longueur de l'en-tête du paquet IP, comptée en mots de 32 bits. En déduire la taille en octets de cet en-tête ?
3. Donner l'écriture en hexadécimal des adresses IP de la source et du destinataire sans faire de calculs.
4. Que trouve-t-on immédiatement après l'en-tête IP ? Que représente les 4 premiers octets ? Décodez ces valeurs.

3 Routage

Voici un extrait de l'état d'une machine :

```
$ /sbin/ifconfig
```

```
eth0      Link encap:Ethernet  HWaddr 00:e0:81:59:41:61
          inet adr:10.0.231.3  Bcast:10.0.231.255  Masque:255.255.255.0
          adr inet6: fe80::2e0:81ff:fe59:4161/64 Scope:Lien
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:128132681 errors:0 dropped:30245 overruns:0 frame:0
          TX packets:102746056 errors:0 dropped:0 overruns:0 carrier:0
          Octets reçus:71419922701 (71.4 GB) Octets transmis:53179042712 (53.1 GB)

$ /sbin/route
Destination     Passerelle      Genmask         Indic Metric Ref    Use Iface
10.0.231.0      *               255.255.255.0   U     0      0        0 eth0
default         10.0.231.253    0.0.0.0         UG    100    0        0 eth0

$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
10.0.231.253             ether   00:18:18:e8:0f:e0   C                     eth0
```

1. Quelle est l'adresse MAC de la machine sur laquelle les commandes précédentes ont été lancés ? Par quelle machine doit-on passer pour toute communication hors du réseau local ? Donner son adresse MAC.
2. Lorsque l'on se connecte à `10.0.231.4` , quel est le chemin des paquets ? Est-ce qu'il a été nécessaire d'utiliser le protocole ARP ? Précisez les adresses MAC des trames émises pour les paquets de notre connexion.
3. Même question pour se connecter à `10.0.230.4` . Expliquez pourquoi le comportement est différent.
4. Lorsque l'on essaie de se connecter à `10.0.232.4` , on n'obtient pas de réponse. Pourtant lorsque l'on se connecte depuis la machine dont l'adresse IP est `10.0.232.3` , on obtient bien une réponse. Expliquer pourquoi cela est possible.
5. Voici la version moderne de ces outils :

```
$ ip addr ls
1: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP gr
    link/ether 00:e0:81:59:41:61  brd ff:ff:ff:ff:ff:ff
    inet 10.0.231.3/24 brd 10.0.231.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::2e0:81ff:fe59:4161/64 scope link
       valid_lft forever preferred_lft forever

$ ip route ls
default via 10.0.231.253 dev eth0 onlink
10.0.231.0/24 dev eth0 proto kernel scope link src 10.0.231.3

$ ip neigh ls
10.0.231.253 dev eth0 lladdr 00:18:18:e8:0f:e0 REACHABLE
```

Repérer les mêmes informations utiles. Sous Windows, c'est encore un autre format avec la commande `ipconfig` :

```
Adresse IP. . . . . . . . . . . . : 10.0.231.3
Masque de sous-réseau . . . . . . : 255.255.255.0
Adresse IP. . . . . . . . . . . . : fe80::2e0:81ff:fe59:4161%4
Passerelle par défaut . . . . . . : 10.0.231.253
```

Et sur un OpenBSD c'est un format, sur un routeur Cisco encore un autre, etc. Heureusement que les adresse ne s'écrivent pas de la même façon !

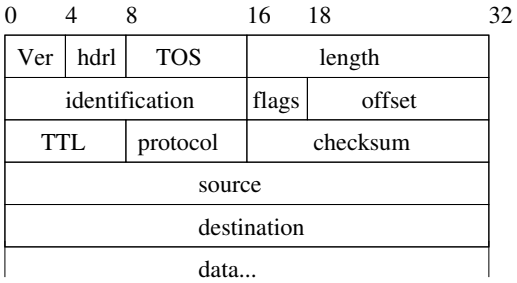
4 Annexe

Format d'en-tête Ethernet

@MAC dest.	@MAC source	prot.	data	CRC

- Adresse destination : 6 octets
- Adresse source : 6 octets
- protocole : 2 octets
- données : au moins 46 octets
- CRC : 4 octets

Format d'en-tête IPv4



Format d'en-tête TCP