Protocoles réseaux
TD n° 8 : Traces de paquets (suite)

Exercice 1 :

```
23:21:13.490893 IP6 2a01:e0a:283:47b0:8731:4158:5978:9b1e.57782 > 2001:dc3::35.53:
    5690 [1au] A? _.fr. (45)
23:21:13.529321 IP6 2001:dc3::35.53 > 2a01:e0a:283:47b0:8731:4158:5978:9b1e.57782:
     5690- 0/6/5 (504)
23:21:13.530910 IP 192.168.0.18.57474 > 194.0.9.1.53:
     23577 [1au] A? _.irif.fr. (50)
23:21:13.565620 IP 194.0.9.1.53 > 192.168.0.18.57474:
     23577-| 0/0/1 (66)
23:21:13.819248 IP6 2a01:e0a:283:47b0:8731:4158:5978:9b1e.52850 > 2001:660:3301:8000::1:2.53:
     661 [1au] A? www.irif.fr. (52)
23:21:13.831212 IP6 2001:660:3301:8000::1:2.53 > 2a01:e0a:283:47b0:8731:4158:5978:9b1e.52850:
     661*- 1/0/1 A 81.194.27.171 (56)
```

1. Quelle est la structure du protocole de couche application ? Qui est client ? Qui est serveur ?
2. Que représente le premier entier affiché pour chaque requête et réponse ?
3. Quel est le protocole de couche application ?
4. Pourquoi ce protocole utilise-t-il UDP plutôt que TCP ?
5. Ce protocole n'est pas sécurisé, ce qui pose des problèmes d'authenticité et de confidentialité, avant le fournisseur de service jouant le rôle de l'attaquant. Donnez deux raisons pour lesquelles le fournisseur de service pourrait vouloir attaquer ce protocole.
6. Pour pallier à ce problème, l'IETF propose d'encapsuler ce protocole dans HTTPS. Commentaire ?

Exercice 2 :

```
12:57:16.581515 IP 192.168.0.18.23222 > 95.161.221.194.30833: UDP, length 285
12:57:20.490839 IP 192.168.0.18.23222 > 157.7.194.141.6881: UDP, length 58
12:57:20.768031 IP 157.7.194.141.6881 > 192.168.0.18.23222: UDP, length 58
12:57:20.768246 IP 192.168.0.18.23222 > 185.183.32.185.33831: UDP, length 110
12:57:20.788525 IP 185.183.32.185.33831 > 192.168.0.18.23222: UDP, length 299
12:57:21.518066 IP 72.132.156.52.50321 > 192.168.0.18.23222: UDP, length 101
12:57:21.518275 IP 192.168.0.18.23222 > 72.132.156.52.50321: UDP, length 266
12:57:21.567798 IP 1.171.146.42.6881 > 192.168.0.18.23222: UDP, length 97
12:57:21.568011 IP 192.168.0.18.23222 > 1.171.146.42.6881: UDP, length 285
12:57:23.465573 IP 192.168.0.18.23222 > 88.23.92.69.51413: UDP, length 58
12:57:23.521455 IP 88.23.92.69.51413 > 192.168.0.18.23222: UDP, length 49
```

1. Quelle est la structure du protocole de couche application ? Qui sont les pairs en jeu ?
2. Pourquoi ce protocole utilise-t-il UDP plutôt que TCP ?
3. Sachant qu'il s'agit d'un sous-protocole de la suite BitTorrent, devinez à quoi sert ce protocole.

Exercice 3 :

```
13:05:05.312847 IP6 2a01:e0a:283:47b0:8731:4158:5978:9b1e.45682 > 2001:41d0:404:200::62ef.8
443: Flags [P.], seq 4279:4549, ack 1463, win 501,
     options [nop,nop,TS val 1437966609 ecr 2
533919660], length 270
13:05:05.312898 IP6 2a01:e0a:283:47b0:8731:4158:5978:9b1e.45682 > 2001:41d0:404:200::62ef.8443:
    Flags [P.], seq 4549:5065, ack 1463, win 501, options [...], length 516
13:05:05.312931 IP6 2a01:e0a:283:47b0:8731:4158:5978:9b1e.45682 > 2001:41d0:404:200::62ef.8443:
     Flags [P.], seq 5065:5311, ack 1463, win 501, options [...], length 246
...
13:05:06.243735 IP6 2a01:e0a:283:47b0:8731:4158:5978:9b1e.40750 > 2001:41d0:404:200::62ef.41969:
    UDP, length 73
13:05:06.264213 IP6 2a01:e0a:283:47b0:8731:4158:5978:9b1e.40750 > 2001:41d0:404:200::62ef.41969:
    UDP, length 76
13:05:06.264253 IP6 2a01:e0a:283:47b0:8731:4158:5978:9b1e.40750 > 2001:41d0:404:200::62ef.41969:
    UDP, length 1113
13:05:06.284810 IP6 2a01:e0a:283:47b0:8731:4158:5978:9b1e.40750 > 2001:41d0:404:200::62ef.41969:
    UDP, length 71
13:05:06.300288 IP6 2a01:e0a:283:47b0:8731:4158:5978:9b1e.40750 > 2001:41d0:404:200::62ef.41969:
    UDP, length 1159
13:05:06.305382 IP6 2a01:e0a:283:47b0:8731:4158:5978:9b1e.40750 > 2001:41d0:404:200::62ef.41969:
    UDP, length 70
...
13:05:07.606059 IP6 2a01:e0a:283:47b0:8731:4158:5978:9b1e.40750 > 2001:41d0:404:200::62ef.41969:
    UDP, length 88
13:05:07.606117 IP6 2a01:e0a:283:47b0:8731:4158:5978:9b1e.40750 > 2001:41d0:404:200::62ef.41969:
    UDP, length 824
13:05:07.622699 IP6 2001:41d0:404:200::62ef.41969 > 2a01:e0a:283:47b0:8731:4158:5978:9b1e.40750:
    UDP, length 76
```

Cette trace capture un morceau de vidéoconférence.

1. Pourquoi y a-t-il des échanges TCP et des échanges UDP ?

2. Pourquoi la taille des paquets UDP varie-t-elle ?

3. S'agit-il d'un protocole fiable ?