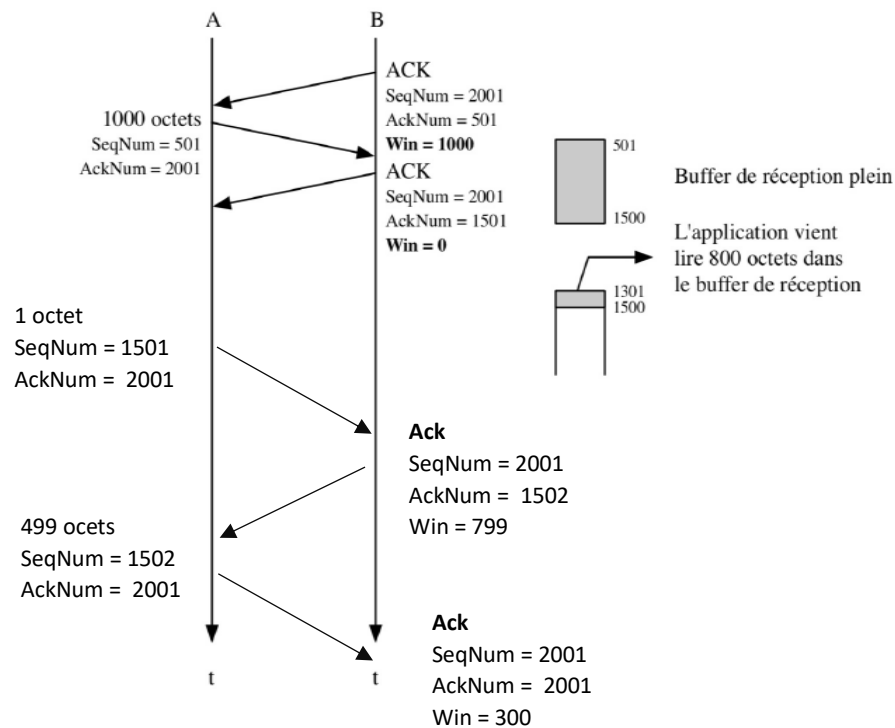


TP2

1. Contrôle de flux dans TCP

1. La fenêtre Window nous indique qu'il reste 3007 octets disponibles, donc la fenetre de reception totale sera de Acknum + Win. Donc la plage de reception sera comprise entre 2513 et 2513 + 3007. Donc [2513 ;5520].

2.



2. Continuation sur WireShark

2) Les données sont présentées en hexadécimale

3)

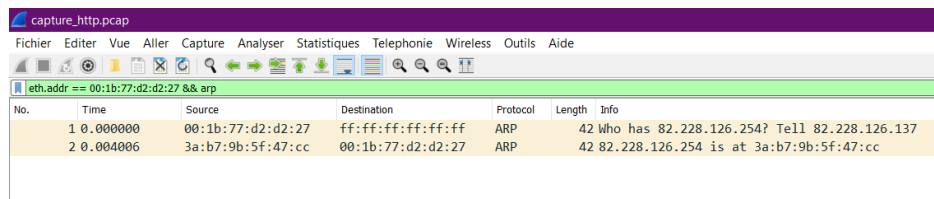
	Destination	Protocol	Length	Info
d2:d2:27	ff:ff:ff:ff:ff:ff	ARP	42	Who has 8
5f:47:cc	00:1b:77:d2:d2:27	ARP	42	82.228.12
6.137	212.27.53.252	DNS	67	Standard
.252	82.228.126.137	DNS	99	Standard
6.137	212.27.53.252	DNS	67	Standard
.252	82.228.126.137	DNS	118	Standard
6.137	81.255.174.189	TCP	66	54267 → 8
4.189	82.228.126.137	TCP	60	80 → 5426
6.137	81.255.174.189	TCP	54	54267 → 8
6.137	81.255.174.189	HTTP	389	GET / HTTP
4.189	82.228.126.137	TCP	60	80 → 5426
4.189	82.228.126.137	HTTP	256	HTTP/1.1

On remarque l'utilisation des protocoles suivants ; ARP, DNS, TCP et http.

4) 3000

3. Filtre d'affichage WireShark

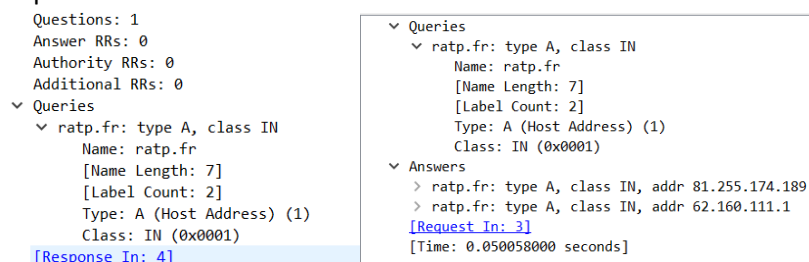
1)



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	00:1b:77:d2:d2:27	ff:ff:ff:ff:ff:ff	ARP	42	Who has 82.228.126.254? Tell 82.228.126.137
2	0.004006	3a:b7:9b:5f:47:cc	00:1b:77:d2:d2:27	ARP	42	82.228.126.254 is at 3a:b7:9b:5f:47:cc

4. Trace http

- 1) En observant la partie Info de la première trame, on remarque que le but de cette trame est d'obtenir l'adresse IP associé à l'adresse MAC « 82.228.126.254 ». Cette requête est envoyée à toutes les machines, ceci se voit dans l'adresse de destination « ff:ff:ff:ff:ff:ff ». Ensuite, on remarque la réponse dans la deuxième trame, on en déduit que l'adresse IP source est « 3a:b7:9b:5f:47:cc », et l'adresse IP destination est « 00:1b:77:d2:d2:27 ».
- 2) Dans les trames 3 4, on remarque que le but est d'obtenir l'adresse IP associé au site ratp.fr.

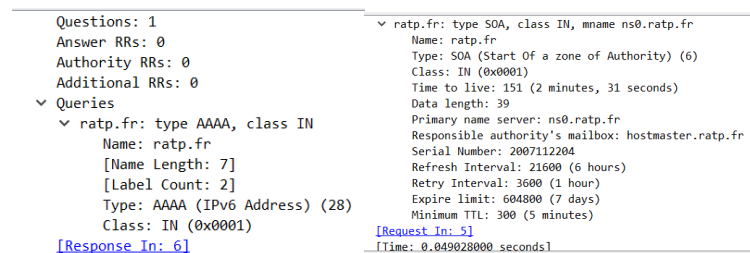


```
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
  ratp.fr: type A, class IN
    Name: ratp.fr
    [Name Length: 7]
    [Label Count: 2]
    Type: A (Host Address) (1)
    Class: IN (0x0001)
[Response In: 4]

Queries
  ratp.fr: type A, class IN
    Name: ratp.fr
    [Name Length: 7]
    [Label Count: 2]
    Type: A (Host Address) (1)
    Class: IN (0x0001)
Answers
  ratp.fr: type A, class IN, addr 81.255.174.189
  ratp.fr: type A, class IN, addr 62.160.111.1
[Request In: 3]
[Time: 0.050058000 seconds]
```

En observant la réponse dans la trame 4, on remarque 2 adresses Ip qui sont associés au site ratp.fr.

La requête 5 s'agit d'un autre type de la 3.

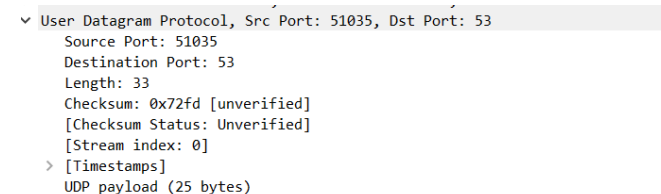


```
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
  ratp.fr: type AAAA, class IN
    Name: ratp.fr
    [Name Length: 7]
    [Label Count: 2]
    Type: AAAA (IPv6 Address) (28)
    Class: IN (0x0001)
[Response In: 6]

  ratp.fr: type SOA, class IN, mname ns0.ratp.fr
    Name: ratp.fr
    Type: SOA (Start Of a zone of Authority) (6)
    Class: IN (0x0001)
    Time to live: 151 (2 minutes, 31 seconds)
    Data length: 39
    Primary name server: ns0.ratp.fr
    Responsible authority's mailbox: hostmaster.ratp.fr
    Serial Number: 2007112204
    Refresh Interval: 21600 (6 hours)
    Retry Interval: 3600 (1 hour)
    Expire limit: 604800 (7 days)
    Minimum TTL: 300 (5 minutes)
[Request In: 5]
[Time: 0.049028000 seconds]
```

On voit que le type est AAAA, et donc demande l'adresse IPv6. Or en observant la réponse, on remarque qu'il n'a pas pu obtenir une adresse.

3)

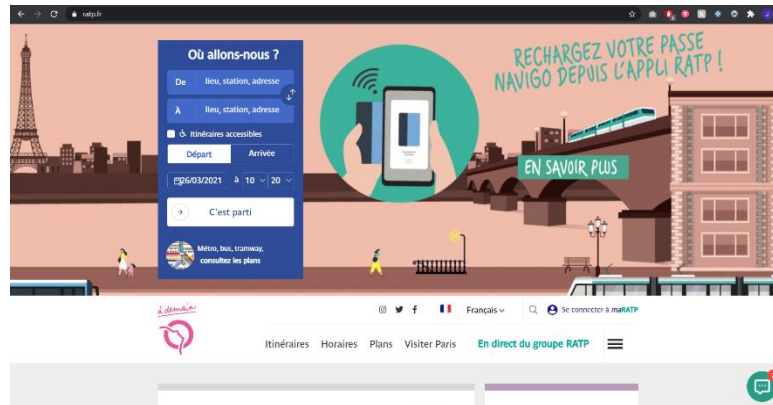


```
User Datagram Protocol, Src Port: 51035, Dst Port: 53
Source Port: 51035
Destination Port: 53
Length: 33
Checksum: 0x72fd [unverified]
[Checksum Status: Unverified]
[Stream index: 0]
  Timestamps
    UDP payload (25 bytes)
```

Il s'agit du protocole UDP. La fonctionnalité principale de ce protocole est de pouvoir transmettre des petites quantités de données entre un serveur et de nombreux clients. Comme dans ce cas, les requêtes ne sont pas volumineuses, donc ce protocole permet d'avoir un échange rapide. Ce protocole ne gère pas la connexion avec la couche de transfert.

4) Obtenir l'adresse IP du site ratp.fr, afin de pouvoir envoyer les requêtes http pour accéder à la page web.

5)



En allant sur la page de ratp.fr, on remarque qu'il y a plusieurs onglets sur la page. En appuyant sur certains boutons nous pouvons être envoyé vers une autre page, donc les différentes requêtes Get sont pour obtenir les sources de tous ces pages.

6) Le protocole utilisé dans cette requête est le TCP. En comparant avec le UDP utilisés dans les requêtes 3 à 6, on observe des différences dans les entêtes.

```
Internet Protocol Version 4, Src: 82.228.126.137, Dst: 81.255.174.189
Transmission Control Protocol, Src Port: 54267, Dst Port: 80, Seq: 0, Len: 0
  Source Port: 54267
  Destination Port: 80
  [Stream index: 0]
  [TCP Segment Len: 0]
  Sequence Number: 0 (relative sequence number)
  Sequence Number (raw): 1232320046
  [Next Sequence Number: 1 (relative sequence number)]
  Acknowledgment Number: 0
  Acknowledgment number (raw): 0
  1000 .... = Header Length: 32 bytes (8)
```

On remarque que l'entête est plus long, et ceci vient de fait que dans le protocole TCP est plus sécurisé. Ce protocole permet aussi de transmettre des paquets d'informations plus grands et en plusieurs segments. Tandis que le UDP permet de transmettre un seul segment. Ce protocole permet aussi d'établir la connexion avec la couche de transfert.

7)

No.	Time	Source	Destination	Protocol	Length	Info
10	0.157520	82.228.126.137	81.255.174.189	HTTP	389	GET / HTTP/1.1
12	0.211815	81.255.174.189	82.228.126.137	HTTP	256	HTTP/1.1 304 Not Modified
14	0.279021	82.228.126.137	81.255.174.189	HTTP	167	GET /crise/index_niv2.htm HTTP/1.1
17	0.336676	81.255.174.189	82.228.126.137	HTTP	255	HTTP/1.1 304 Not Modified
21	0.349759	82.228.126.137	81.255.174.189	HTTP	155	GET /blank.htm HTTP/1.1
23	0.362836	82.228.126.137	81.255.174.189	HTTP	175	GET /blank.htm HTTP/1.1
27	0.411531	81.255.174.189	82.228.126.137	HTTP	255	HTTP/1.1 304 Not Modified
29	0.421090	81.255.174.189	82.228.126.137	HTTP	254	HTTP/1.1 304 Not Modified
37	0.533317	82.228.126.137	81.255.174.188	HTTP	137	GET / HTTP/1.1
45	0.645791	81.255.174.188	82.228.126.137	HTTP	551	HTTP/1.1 200 OK (text/html)
46	0.763550	82.228.126.137	81.255.174.188	HTTP	529	GET /pics/v_home_ratp/niv3bis/reseaux.gif HTTP/1.1
49	0.820898	81.255.174.188	82.228.126.137	HTTP	237	HTTP/1.1 304 Not Modified
52	0.823792	82.228.126.137	81.255.174.188	HTTP	531	GET /pics/v_home_ratp/niv3bis/logo_ratp.gif HTTP/1.1
53	0.825140	82.228.126.137	81.255.174.188	HTTP	528	GET /pics/v_home_ratp/niv3bis/exclam.gif HTTP/1.1
56	0.878725	81.255.174.188	82.228.126.137	HTTP	237	HTTP/1.1 304 Not Modified
59	0.883179	81.255.174.188	82.228.126.137	HTTP	238	HTTP/1.1 304 Not Modified
63	0.944826	82.228.126.137	80.118.149.113	HTTP	519	GET /hit.xiti?z=63390&z=1&p=HOME_NIV2bis&hl=19x2x29&r=1200x800&undefined32&ref=http://ratp.fr/crise/index_niv2.htm HTTP/1.1
64	1.005677	80.118.149.113	82.228.126.137	HTTP	462	HTTP/1.1 200 OK (GIF89a)

On applique le filtre « http ».

- 8) Dans cette trame, on observe que la requête obtient le contenu texte de la page.
Ensuite, des requêtes Get sont faites pour obtenir les images et les liens dans la page.

9)

```
▼ Queries
  ▼ logc5.xiti.com: type A, class IN
    Name: logc5.xiti.com
    [Name Length: 14]
    [Label Count: 3]
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    [Response In: 54]
```

Dans cette requête on quitte le domaine ratp.fr, pour accéder à logc5.xiti.com.

Cette requête est liée, car on souhaite obtenir une image sur la page ratp.fr qui présente sur le site logc5.xiti.com.