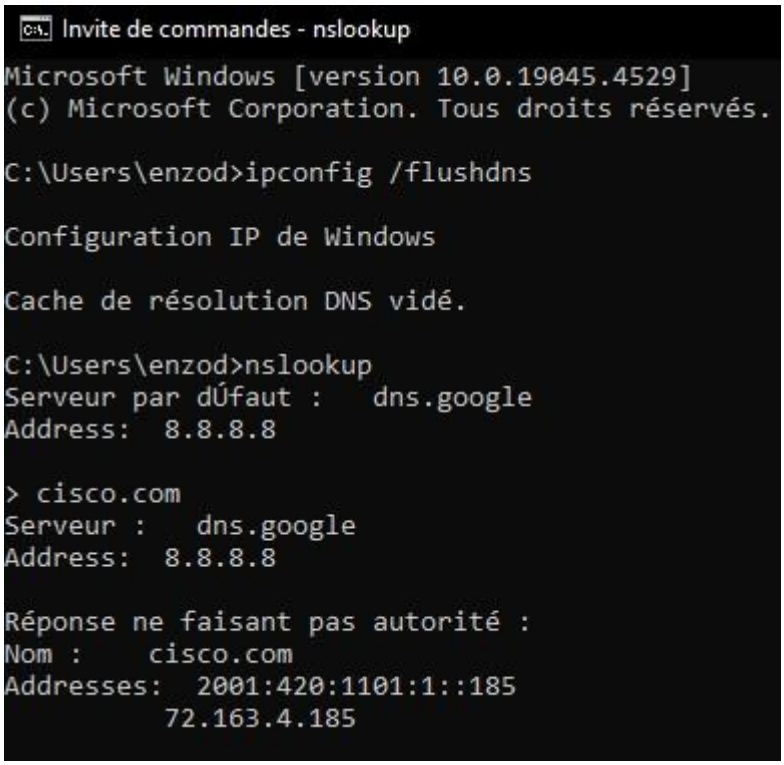
Enzo Dugelay

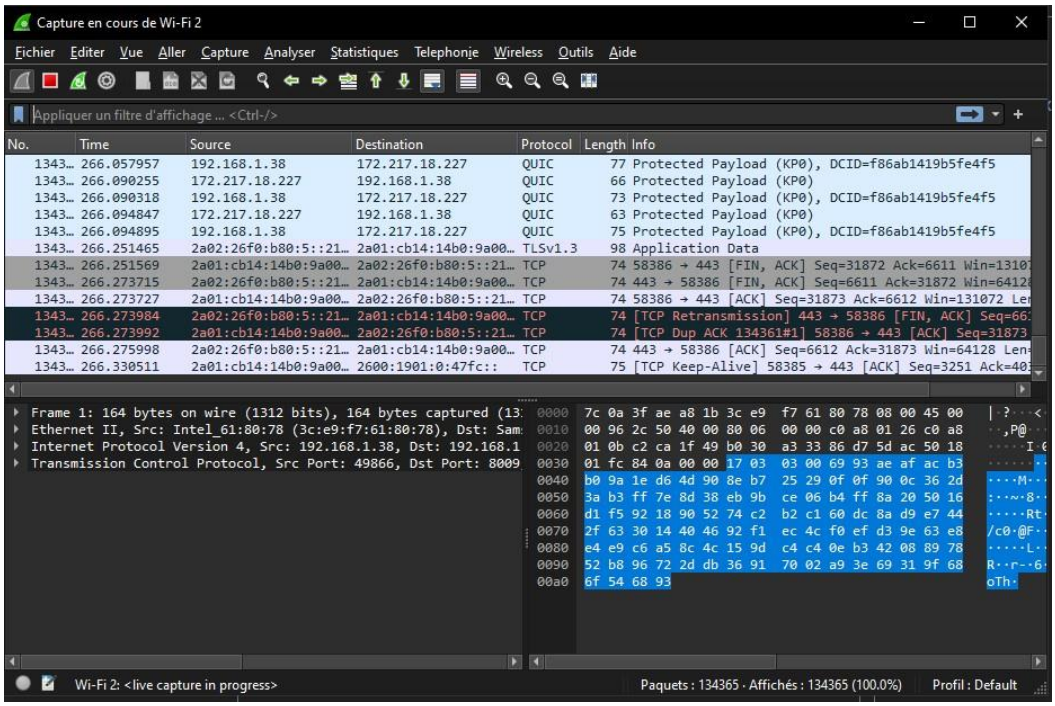
TP CyberObs

TP 17.1.7 Explorer le trafic DNS

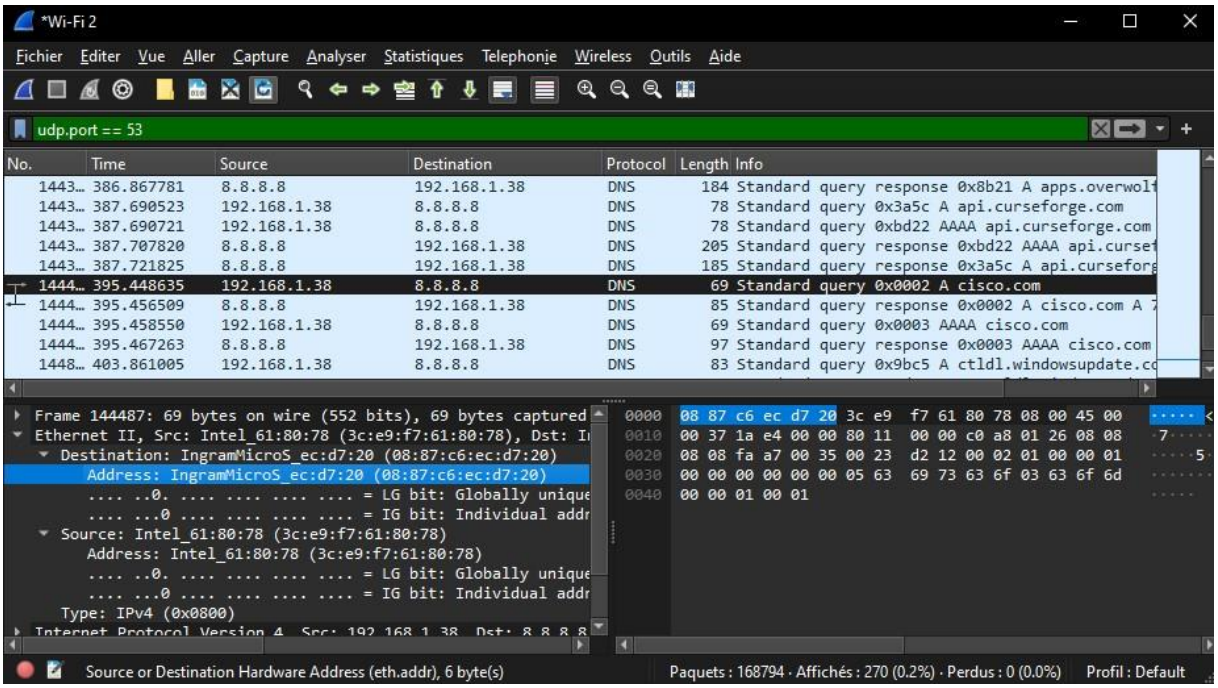
Dans l'invité de commande je vide le cache DNS :



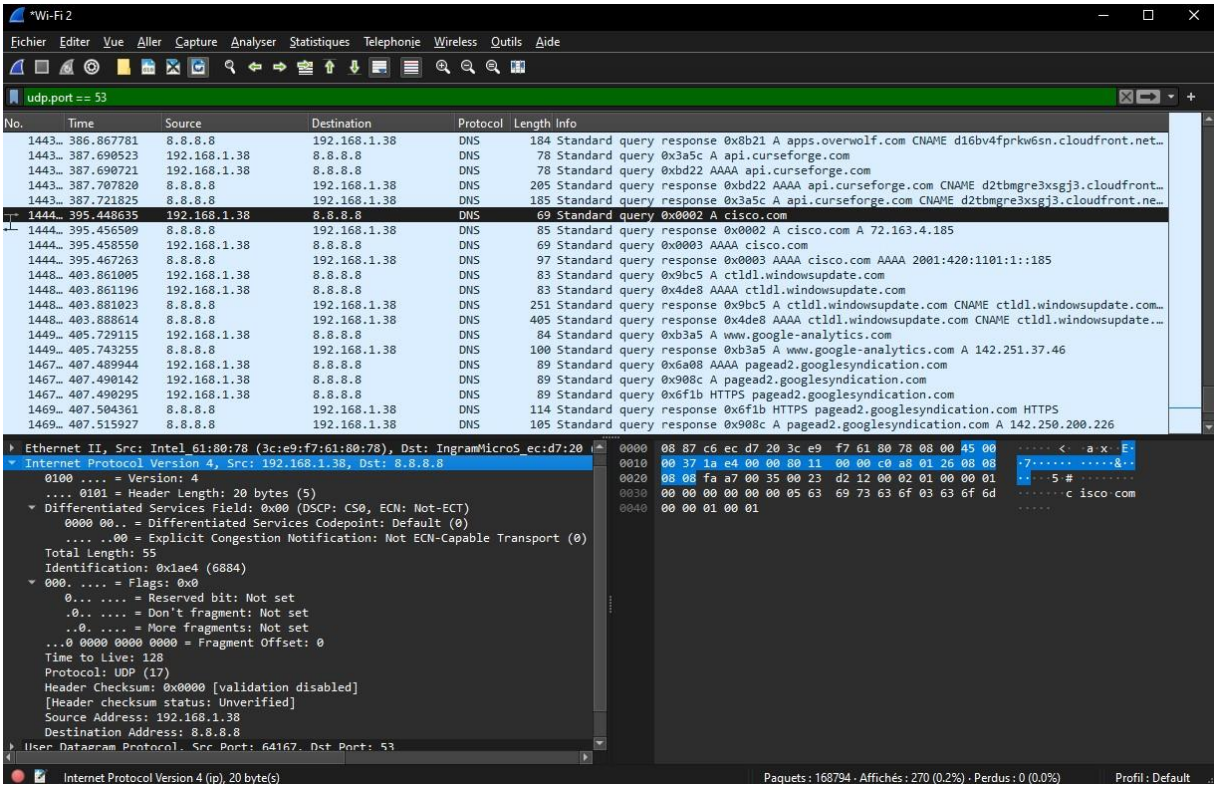
Je télécharge Wireshark et je peux analyser les trames de la wifi par exemple :



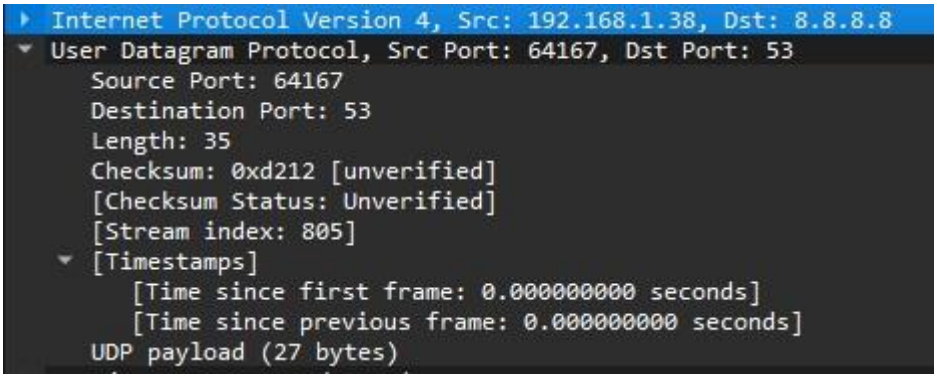
Je retrouve bien le packet DNS correspondant à la requête envers cisco.com :



L'adresse mac de destination est donc 08:87:c6:ec:d7:20 et l'adresse mac source est 3c:e9:f7:61:80:78

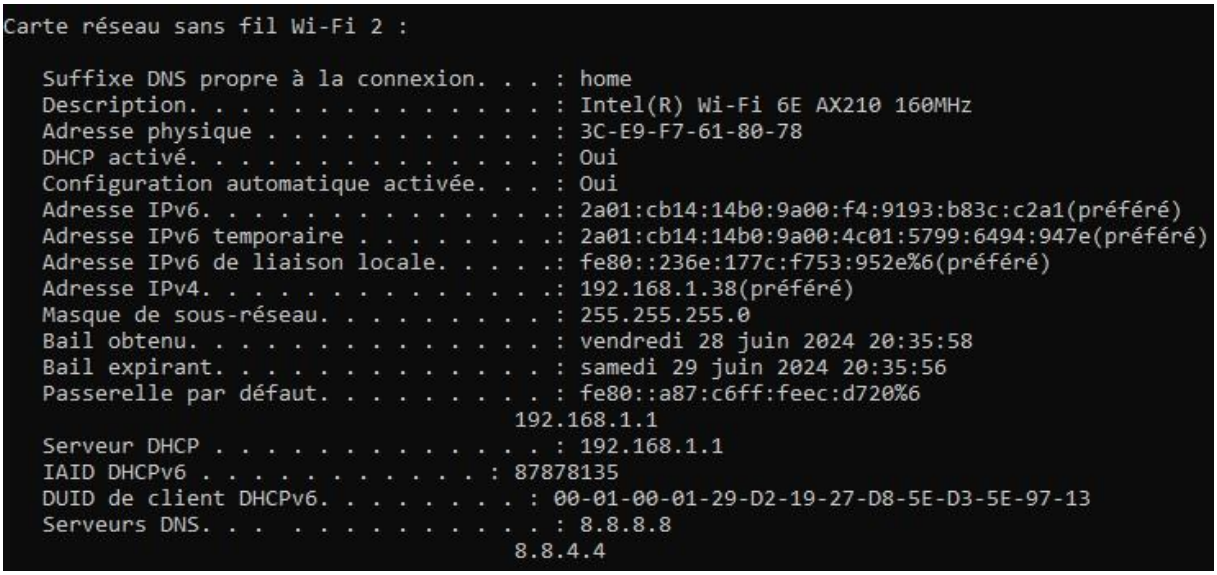


L’adresse IP source est 192.168.1.38 et l’adresse IP de destination est 8.8.8.8



Le port source est 64167 et le port destination 53.

Je fais ensuite les commandes **arp –a** et **ipconfig /all** pour enregistrer les adresses MAC et IP de l'ordinateur.



J’ai repris les mêmes IP qu’observées sur Wireshark.

```
▾ Domain Name System (query)
    Transaction ID: 0x0002
  ▾ Flags: 0x0100 Standard query
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Standard query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... .0.. .... = Z: reserved (0)
      .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
    ▸ cisco.com: type A, class IN
    [Response In: 144488]
```

Pour la réponse contenant Standard query response :

Les IP et mac source et destination ne changent pas

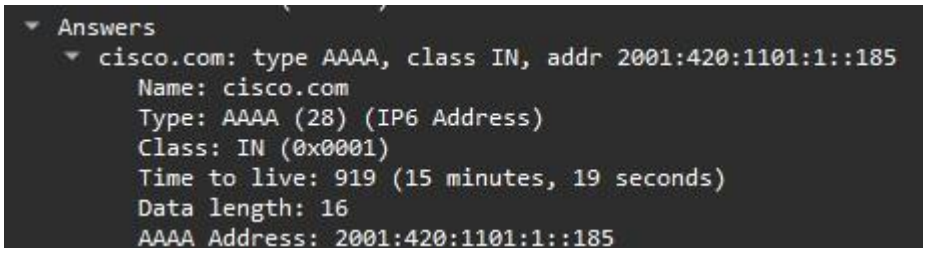
```
▸ Ethernet II, Src: IngramMicroS_ec:d7:20 (08:87:c6:ec:d7:20), Dst: Intel_61:80:78 (3c:e9:f7:61:80:78)
▸ Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.1.38
```

Wireshark · Paquet 144490 · Wi-Fi 2

```
▸ Frame 144490: 97 bytes on wire (776 bits), 97 bytes captured (776 bits) on interface \Device\NPF_{0E3D8863-5EBB-4044-BB0A-EC8490C3C1C0}, id 0
▸ Ethernet II, Src: IngramMicroS_ec:d7:20 (08:87:c6:ec:d7:20), Dst: Intel_61:80:78 (3c:e9:f7:61:80:78)
▸ Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.1.38
▸ User Datagram Protocol, Src Port: 53, Dst Port: 64168
▾ Domain Name System (response)
    Transaction ID: 0x0003
  ▾ Flags: 0x8180 Standard query response, No error
      1... .... .... .... = Response: Message is a response
      .000 0... .... .... = Opcode: Standard query (0)
      .... .0.. .... .... = Authoritative: Server is not an authority for domain
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... 1... .... = Recursion available: Server can do recursive queries
      .... .... .0.. .... = Z: reserved (0)
      .... .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
      .... .... ...0 .... = Non-authenticated data: Unacceptable
      .... .... .... 0000 = Reply code: No error (0)
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
    ▸ cisco.com: type AAAA, class IN
  ▸ Answers
    [Request In: 144489]
    [Time: 0.008713000 seconds]

0000  3c e9 f7 61 80 78 08 87  c6 ec d7 20 08 00 45 00   <··a·x·· ··· ··E·
0010  00 53 1f d4 00 00 78 11  50 e8 08 08 08 08 c0 a8   ·S····x· P·······
0020  01 26 00 35 fa a8 00 3f  d6 1d 00 03 81 80 00 01   ·&·5···? ········
0030  00 01 00 00 00 00 05 63  69 73 63 6f 03 63 6f 6d   ·······c isco·com
0040  00 00 1c 00 01 c0 0c 00  1c 00 01 00 00 03 97 00   ········ ········
0050  10 20 01 04 20 11 01 00  01 00 00 00 00 00 00 01   ·· ·· ··· ········
0060  85                                                ·
```

Le serveur DNS ne peut donc pas envoyer des requêtes récursives.



Dans les réponses je peux retrouver les mêmes résultats qu'avec nslookup.