

TP CyberObs



TP 17.1.7 Explorer le trafic DNS

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

```
C:\> Invite de commandes - nslookup

Microsoft Windows [version 10.0.19045.4529]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\enzod>ipconfig /flushdns

Configuration IP de Windows

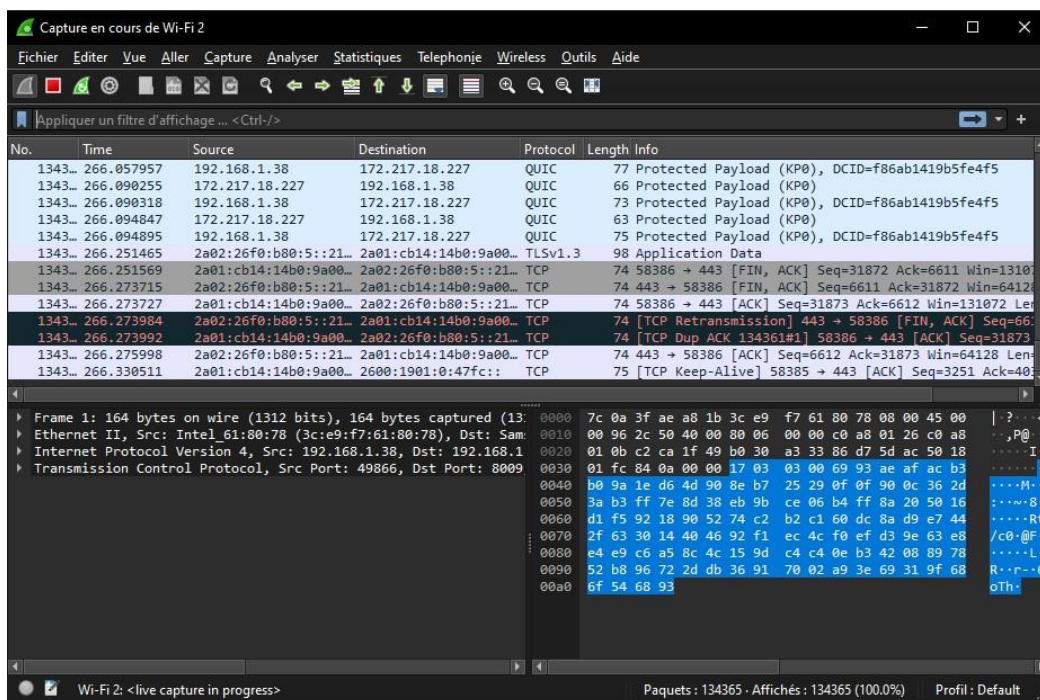
Cache de résolution DNS vidé.

C:\Users\enzod>nslookup
Serveur par défaut : dns.google
Address: 8.8.8.8

> cisco.com
Serveur : dns.google
Address: 8.8.8.8

Réponse ne faisant pas autorité :
Nom : cisco.com
Addresses: 2001:420:1101:1::185
          72.163.4.185
```

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 :

The screenshot shows a Wireshark capture of network traffic. The filter bar at the top is set to 'udp.port == 53'. The packet list on the left shows several DNS packets. Packet 1444 is selected, showing a DNS query from source 192.168.1.38 to destination 8.8.8.8. The packet details pane on the right shows the Ethernet II header with source MAC 3c:e9:f7:61:80:78 and destination MAC 08:87:c6:ec:d7:20. The Internet Protocol Version 4 header shows source 192.168.1.38 and destination 8.8.8.8. The UDP header shows source port 53 and destination port 53. The DNS header shows a query for 'cisco.com'.

No.	Time	Source	Destination	Protocol	Length	Info
1443..	386.867781	8.8.8.8	192.168.1.38	DNS	184	Standard query response 0x8b21 A apps.Overwolf.com
1443..	387.690523	192.168.1.38	8.8.8.8	DNS	78	Standard query 0x3a5c A api.curseforge.com
1443..	387.690721	192.168.1.38	8.8.8.8	DNS	78	Standard query 0xbd22 AAAA api.curseforge.com
1443..	387.707820	8.8.8.8	192.168.1.38	DNS	205	Standard query response 0xbd22 AAAA api.curseforge.com
1443..	387.721825	8.8.8.8	192.168.1.38	DNS	185	Standard query response 0x3a5c A api.curseforge.com
1444..	395.448635	192.168.1.38	8.8.8.8	DNS	69	Standard query 0x0002 A cisco.com
1444..	395.456509	8.8.8.8	192.168.1.38	DNS	85	Standard query response 0x0002 A cisco.com A 72.163.4.185
1444..	395.458550	192.168.1.38	8.8.8.8	DNS	69	Standard query 0x0003 AAAA cisco.com
1444..	395.467263	8.8.8.8	192.168.1.38	DNS	97	Standard query response 0x0003 AAAA cisco.com
1448..	403.861005	192.168.1.38	8.8.8.8	DNS	83	Standard query 0x9bc5 A ctldl.windowsupdate.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

The screenshot shows a Wireshark capture of network traffic. The filter bar at the top is set to 'udp.port == 53'. The packet list on the left shows several DNS packets. Packet 1444 is selected, showing a DNS query from source 192.168.1.38 to destination 8.8.8.8. The packet details pane on the right shows the Ethernet II header with source MAC 3c:e9:f7:61:80:78 and destination MAC 08:87:c6:ec:d7:20. The Internet Protocol Version 4 header shows source 192.168.1.38 and destination 8.8.8.8. The UDP header shows source port 53 and destination port 53. The DNS header shows a query for 'cisco.com'.

No.	Time	Source	Destination	Protocol	Length	Info
1443..	386.867781	8.8.8.8	192.168.1.38	DNS	184	Standard query response 0x8b21 A apps.Overwolf.com CNAME d16bv4fprkw6sn.cloudfront.net...
1443..	387.690523	192.168.1.38	8.8.8.8	DNS	78	Standard query 0x3a5c A api.curseforge.com
1443..	387.690721	192.168.1.38	8.8.8.8	DNS	78	Standard query 0xbd22 AAAA api.curseforge.com
1443..	387.707820	8.8.8.8	192.168.1.38	DNS	205	Standard query response 0xbd22 AAAA api.curseforge.com CNAME d2tbmgre3xsgj3.cloudfront...
1443..	387.721825	8.8.8.8	192.168.1.38	DNS	185	Standard query response 0x3a5c A api.curseforge.com CNAME d2tbmgre3xsgj3.cloudfront.net...
1444..	395.448635	192.168.1.38	8.8.8.8	DNS	69	Standard query 0x0002 A cisco.com
1444..	395.456509	8.8.8.8	192.168.1.38	DNS	85	Standard query response 0x0002 A cisco.com A 72.163.4.185
1444..	395.458550	192.168.1.38	8.8.8.8	DNS	69	Standard query 0x0003 AAAA cisco.com
1444..	395.467263	8.8.8.8	192.168.1.38	DNS	97	Standard query response 0x0003 AAAA cisco.com AAAA 2001:420:1101:1::185
1448..	403.861005	192.168.1.38	8.8.8.8	DNS	83	Standard query 0x9bc5 A ctldl.windowsupdate.com
1448..	403.861196	192.168.1.38	8.8.8.8	DNS	83	Standard query 0x4de8 AAAA ctldl.windowsupdate.com
1448..	403.881023	8.8.8.8	192.168.1.38	DNS	251	Standard query response 0x9bc5 A ctldl.windowsupdate.com CNAME ctldl.windowsupdate.com...
1448..	403.888614	8.8.8.8	192.168.1.38	DNS	405	Standard query response 0x4de8 AAAA ctldl.windowsupdate.com CNAME ctldl.windowsupdate.com...
1449..	405.729115	192.168.1.38	8.8.8.8	DNS	84	Standard query 0xb3a5 A www.google-analytics.com
1449..	405.743255	8.8.8.8	192.168.1.38	DNS	100	Standard query response 0xb3a5 A www.google-analytics.com A 142.251.37.46
1467..	407.489944	192.168.1.38	8.8.8.8	DNS	89	Standard query 0x6a08 AAAA pagead2.googlesyndication.com
1467..	407.490142	192.168.1.38	8.8.8.8	DNS	89	Standard query 0x908c A pagead2.googlesyndication.com
1467..	407.490295	192.168.1.38	8.8.8.8	DNS	89	Standard query 0x6f1b HTTPS pagead2.googlesyndication.com
1469..	407.504361	8.8.8.8	192.168.1.38	DNS	114	Standard query response 0x6f1b HTTPS pagead2.googlesyndication.com HTTPS
1469..	407.515927	8.8.8.8	192.168.1.38	DNS	105	Standard query response 0x908c A pagead2.googlesyndication.com A 142.250.200.226

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

```
▶ Internet Protocol Version 4, Src: 192.168.1.38, Dst: 8.8.8.8
▼ User Datagram Protocol, Src Port: 64167, Dst Port: 53
  Source Port: 64167
  Destination Port: 53
  Length: 35
  Checksum: 0xd212 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 805]
  ▼ [Timestamps]
    [Time since first frame: 0.000000000 seconds]
    [Time since previous frame: 0.000000000 seconds]
  UDP payload (27 bytes)
```

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.

```
Carte réseau sans fil Wi-Fi 2 :

Suffixe DNS propre à la connexion. . . : home
Description. . . . . : Intel(R) Wi-Fi 6E AX210 160MHz
Adresse physique . . . . . : 3C-E9-F7-61-80-78
DHCP activé. . . . . : Oui
Configuration automatique activée. . . : Oui
Adresse IPv6. . . . . : 2a01:cb14:14b0:9a00:f4:9193:b83c:c2a1(préféré)
Adresse IPv6 temporaire . . . . . : 2a01:cb14:14b0:9a00:4c01:5799:6494:947e(préféré)
Adresse IPv6 de liaison locale. . . . : fe80::236e:177c:f753:952e%6(préféré)
Adresse IPv4. . . . . : 192.168.1.38(préféré)
Masque de sous-réseau. . . . . : 255.255.255.0
Bail obtenu. . . . . : vendredi 28 juin 2024 20:35:58
Bail expirant. . . . . : samedi 29 juin 2024 20:35:56
Passerelle par défaut. . . . . : fe80::a87:c6ff:feec:d720%6
                                192.168.1.1
Serveur DHCP . . . . . : 192.168.1.1
IAID DHCPv6 . . . . . : 87878135
DUID de client DHCPv6. . . . . : 00-01-00-01-29-D2-19-27-D8-5E-D3-5E-97-13
Serveurs DNS. . . . . : 8.8.8.8
                                8.8.4.4
```

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_{0E3D8863-5E8B-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 01 .....
0060 85 .....
```

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

```
▼ Answers
  ▼ cisco.com: type AAAA, class IN, addr 2001:420:1101:1::185
    Name: cisco.com
    Type: AAAA (28) (IP6 Address)
    Class: IN (0x0001)
    Time to live: 919 (15 minutes, 19 seconds)
    Data length: 16
    AAAA Address: 2001:420:1101:1::185
```

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