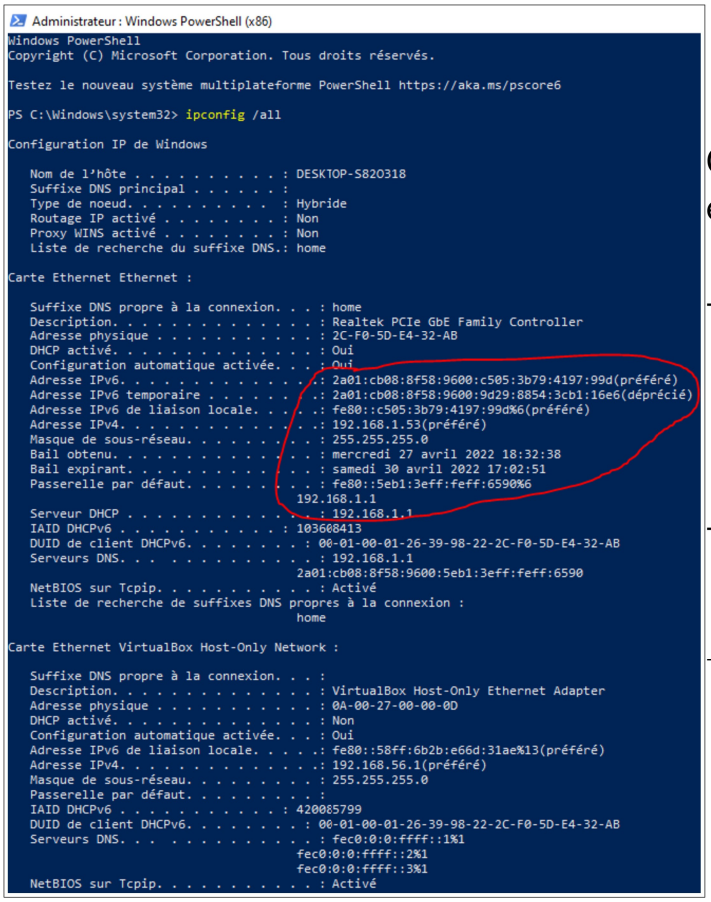
TP – Réseaux (Adresses IP et WireShark)

Je réalise la commande « ipconfig /all » dans un terminal PowerShell sur mon système d'exploitation principal (Windows) :



On peut donc remarquer plusieurs éléments :

- L'adresse Ipv6 de mon PC :
  - « 2a01:cb08:8f58:9600:c505:3b79:4197:99d »

- L'adresse Ipv4 de mon PC :
  - « 192.168.1.53 »

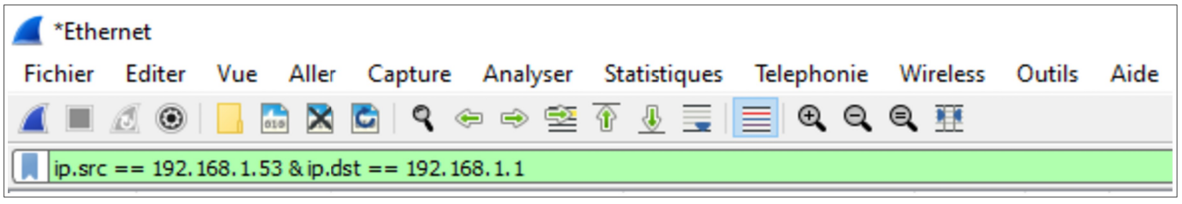
- Le masque de sous-réseau :
  - « 255.255.255.0 »
    - soit « 11111111 11111111 11111111 00000000 »
    - 24 bits à 1
    - soit « 192.168.1.53/24 »

- La date à laquelle j'ai obtenu le bail pour mon adresse ip :
  - « mercredi 27 avril 2022 18:32:38 »

- La date à laquelle le bail actuel pour mon adresse ip va s'arrêter :
  - « samedi 30 avril 2022 17:02:51 »

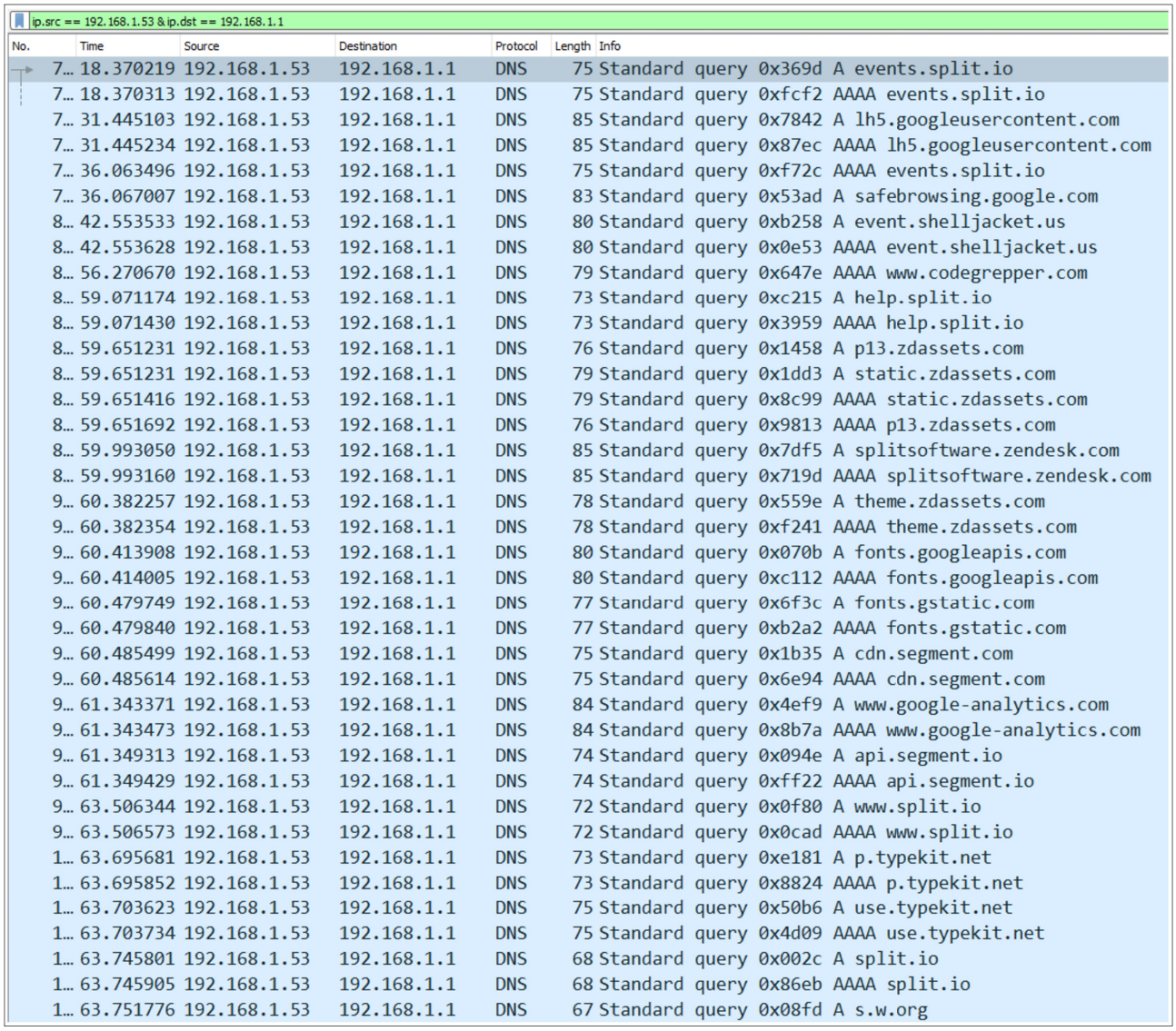
- L'adresse Ipv4 de ma passerelle, serveur DNS, serveur DHCP (ma box internet):
  - « 192.168.1.1 »

Grâce à ces informations j'ai pu réaliser un filtrage de requêtes dans le logiciel WireShark :



La commande « ip.src == 192.168.1.53 & ip.dst == 192.168.1.1 » me permet de ne récupérer que les paquets partant de mon ordinateur (ip.src) pour aller vers ma box internet (ip.dst).

Et donc en lançant l'analyse, je vois apparaître toutes les requêtes avec protocol DNS entre mon pc et ma box qui va ensuite sur Internet :



ip.src == 192.168.1.53 & ip.dst == 192.168.1.1

No.	Time	Source	Destination	Protocol	Length	Info
7…	18.370219	192.168.1.53	192.168.1.1	DNS	75	Standard query 0x369d A events.split.io
7…	18.370313	192.168.1.53	192.168.1.1	DNS	75	Standard query 0xfcf2 AAAA events.split.io
7…	31.445103	192.168.1.53	192.168.1.1	DNS	85	Standard query 0x7842 A lh5.googleusercontent.com
7…	31.445234	192.168.1.53	192.168.1.1	DNS	85	Standard query 0x87ec AAAA lh5.googleusercontent.com
7…	36.063496	192.168.1.53	192.168.1.1	DNS	75	Standard query 0xf72c AAAA events.split.io
7…	36.067007	192.168.1.53	192.168.1.1	DNS	83	Standard query 0x53ad A safebrowsing.google.com
8…	42.553533	192.168.1.53	192.168.1.1	DNS	80	Standard query 0xb258 A event.shelljacket.us
8…	42.553628	192.168.1.53	192.168.1.1	DNS	80	Standard query 0x0e53 AAAA event.shelljacket.us
8…	56.270670	192.168.1.53	192.168.1.1	DNS	79	Standard query 0x647e AAAA www.codegrepper.com
8…	59.071174	192.168.1.53	192.168.1.1	DNS	73	Standard query 0xc215 A help.split.io
8…	59.071430	192.168.1.53	192.168.1.1	DNS	73	Standard query 0x3959 AAAA help.split.io
8…	59.651231	192.168.1.53	192.168.1.1	DNS	76	Standard query 0x1458 A p13.zdassets.com
8…	59.651231	192.168.1.53	192.168.1.1	DNS	79	Standard query 0x1dd3 A static.zdassets.com
8…	59.651416	192.168.1.53	192.168.1.1	DNS	79	Standard query 0x8c99 AAAA static.zdassets.com
8…	59.651692	192.168.1.53	192.168.1.1	DNS	76	Standard query 0x9813 AAAA p13.zdassets.com
8…	59.993050	192.168.1.53	192.168.1.1	DNS	85	Standard query 0x7df5 A splitsoftware.zendesk.com
8…	59.993160	192.168.1.53	192.168.1.1	DNS	85	Standard query 0x719d AAAA splitsoftware.zendesk.com
9…	60.382257	192.168.1.53	192.168.1.1	DNS	78	Standard query 0x559e A theme.zdassets.com
9…	60.382354	192.168.1.53	192.168.1.1	DNS	78	Standard query 0xf241 AAAA theme.zdassets.com
9…	60.413908	192.168.1.53	192.168.1.1	DNS	80	Standard query 0x070b A fonts.googleapis.com
9…	60.414005	192.168.1.53	192.168.1.1	DNS	80	Standard query 0xc112 AAAA fonts.googleapis.com
9…	60.479749	192.168.1.53	192.168.1.1	DNS	77	Standard query 0x6f3c A fonts.gstatic.com
9…	60.479840	192.168.1.53	192.168.1.1	DNS	77	Standard query 0xb2a2 AAAA fonts.gstatic.com
9…	60.485499	192.168.1.53	192.168.1.1	DNS	75	Standard query 0x1b35 A cdn.segment.com
9…	60.485614	192.168.1.53	192.168.1.1	DNS	75	Standard query 0x6e94 AAAA cdn.segment.com
9…	61.343371	192.168.1.53	192.168.1.1	DNS	84	Standard query 0x4ef9 A www.google-analytics.com
9…	61.343473	192.168.1.53	192.168.1.1	DNS	84	Standard query 0x8b7a AAAA www.google-analytics.com
9…	61.349313	192.168.1.53	192.168.1.1	DNS	74	Standard query 0x094e A api.segment.io
9…	61.349429	192.168.1.53	192.168.1.1	DNS	74	Standard query 0xff22 AAAA api.segment.io
9…	63.506344	192.168.1.53	192.168.1.1	DNS	72	Standard query 0x0f80 A www.split.io
9…	63.506573	192.168.1.53	192.168.1.1	DNS	72	Standard query 0x0cad AAAA www.split.io
1…	63.695681	192.168.1.53	192.168.1.1	DNS	73	Standard query 0xe181 A p.typekit.net
1…	63.695852	192.168.1.53	192.168.1.1	DNS	73	Standard query 0x8824 AAAA p.typekit.net
1…	63.703623	192.168.1.53	192.168.1.1	DNS	75	Standard query 0x50b6 A use.typekit.net
1…	63.703734	192.168.1.53	192.168.1.1	DNS	75	Standard query 0x4d09 AAAA use.typekit.net
1…	63.745801	192.168.1.53	192.168.1.1	DNS	68	Standard query 0x002c A split.io
1…	63.745905	192.168.1.53	192.168.1.1	DNS	68	Standard query 0x86eb AAAA split.io
1…	63.751776	192.168.1.53	192.168.1.1	DNS	67	Standard query 0x08fd A s.w.org

J'utilise mon navigateur web en même temps et je me balade sur Google.
On voit donc apparaître des adresses comme typekit.net ou fonts.googleapis.com qui sont les serveurs hébergeant les polices d'écritures d'Adobe et de Google.

Il y a aussi 4 plateformes d'analyse commerciale :

- Google Analytics / Google User Content
- Split.io
- Segment.io
- Zendesk.com