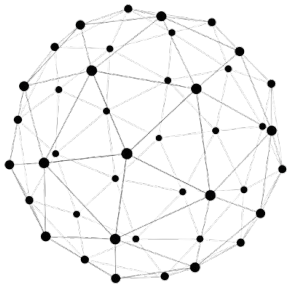
Sorbonne Université
LU2IN023 - DM Réseaux

SOUAIBY Christina 21102782

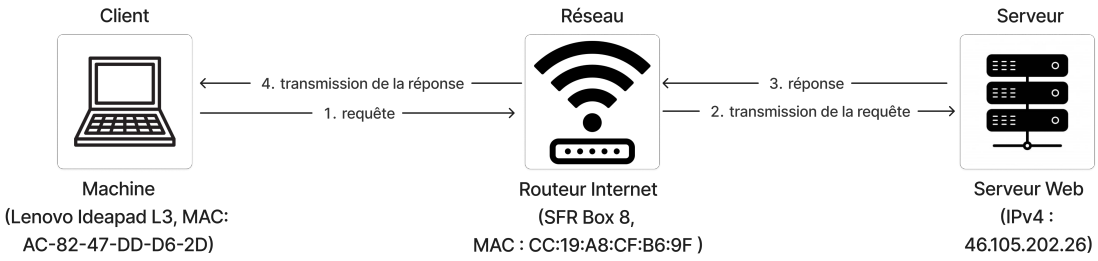
Avril 2024



Sommaire

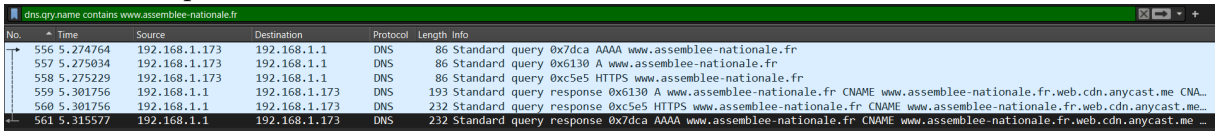
1 Configuration de la Capture

- Type de la machine client : Ordinateur portable Lenovo ideapad L3
- Fabricant de la machine client : Lenovo
- Fabricant de la carte réseaux : Intel
- Type de connexion à Internet : Wi-Fi
- Adresse MAC de la machine : AC-82-47-DD-D6-2D
- Adresse IPv4 machine : 192.168.1.173
- Adresse IPv6 machine : 2a02:8428:4aa:e301:e94b:c588:f194:eb6a
- Fournisseur Internet : SFR
- Adresse MAC de la box (routeur) : CC:19:A8:CF:B6:9F
- Adresses IPv4 des serveurs Web : (*) 46.105.202.26 [explication dans la partie2 sur Wireshark]

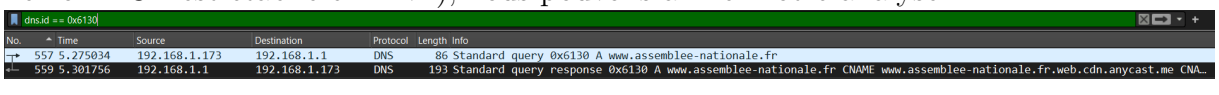


2 Capture et Analyse du Trafic

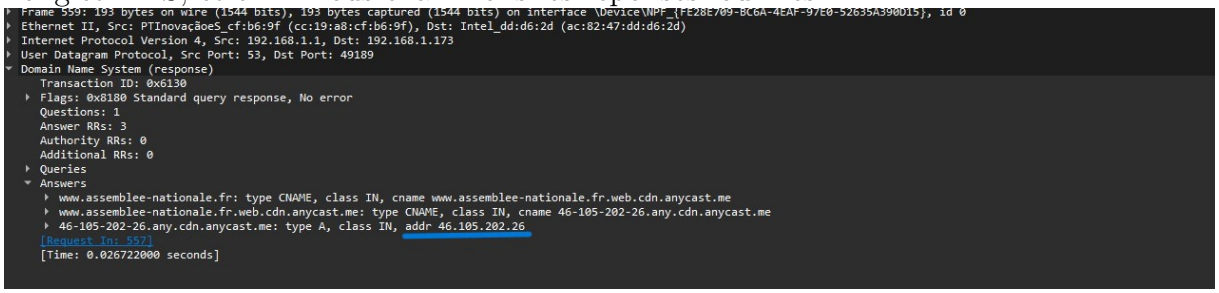
- URL Demandée : www.assemblee-nationale.fr
- La correspondance entre la requête DNS et le nom de la machine dans l'URL est confirmée. Cette vérification est réalisée en recherchant les requêtes DNS à l'aide des filtres disponibles dans Wireshark.



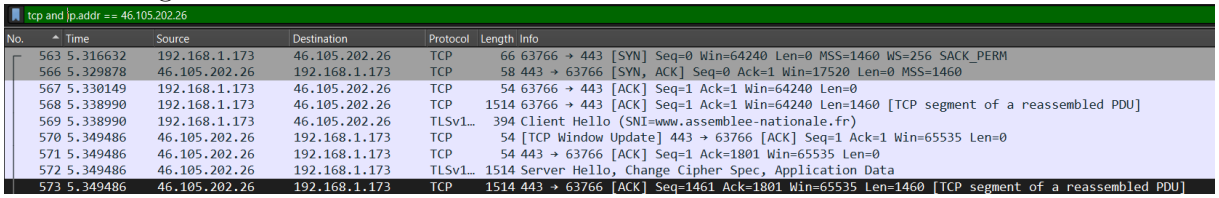
- Ensuite, en appliquant un nouveau filtre pour isoler les trames de requête-réponse DNS identifiées par le code 0x6130, correspondant à une adresse IPv4 (car la connexion TCP est établie en IPv4), nous pouvons affiner notre analyse.



- (*) nous vérifions l'adresse IPv4 du serveur web demandé en procédant comme suit: tout d'abord, nous sélectionnons la trame DNS n°559, marquée comme "Standard query response", puis nous accédons à la deuxième fenêtre, où nous sélectionnons l'onglet DNS, et enfin nous examinons les réponses fournies.

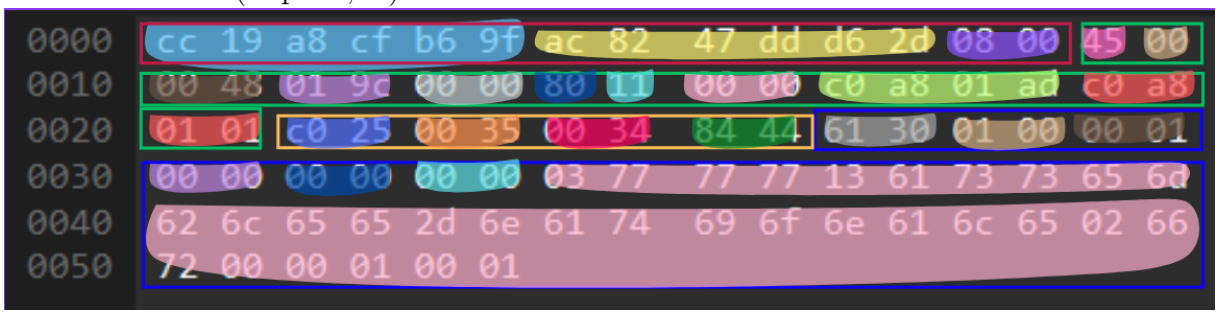


- La connexion TCP est établie avec succès avec le serveur web demandé. Après avoir identifié l'adresse IP de ce serveur, nous appliquons un filtre en utilisant la syntaxe "tcp and ip.addr == 46.105.202.26" pour obtenir toutes les trames du protocole TCP échangées entre notre machine et le serveur Web.

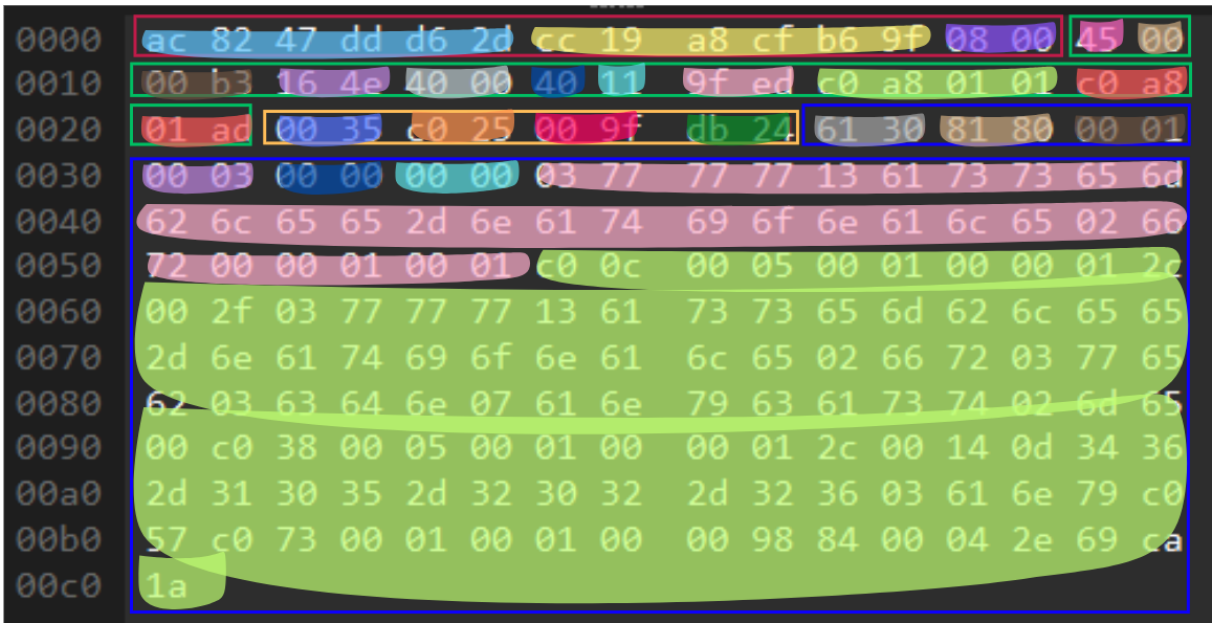


3 Représentation Hexadécimale des Messages Échangés

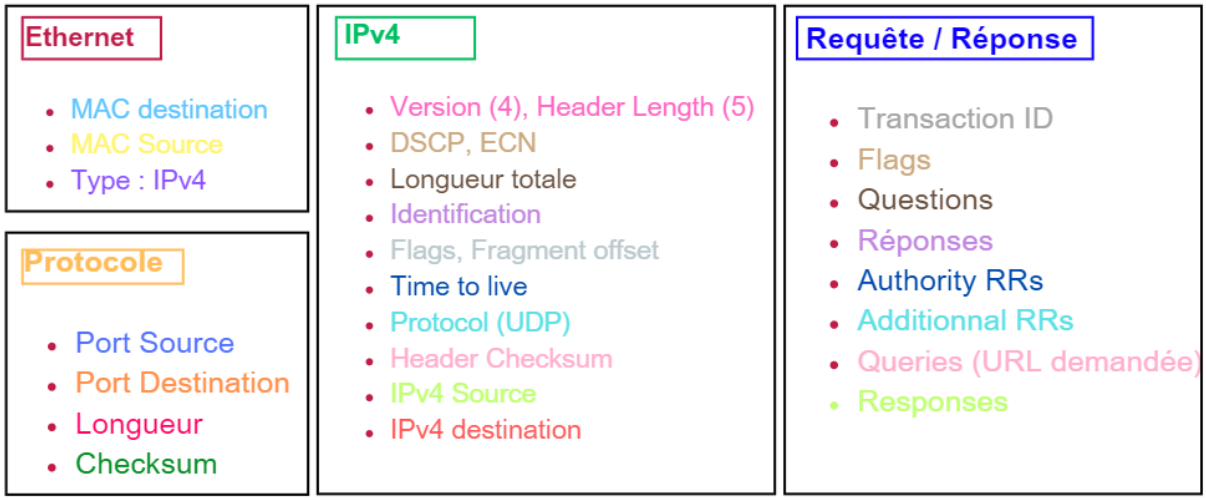
- Trame DNS 557 (requête, A)



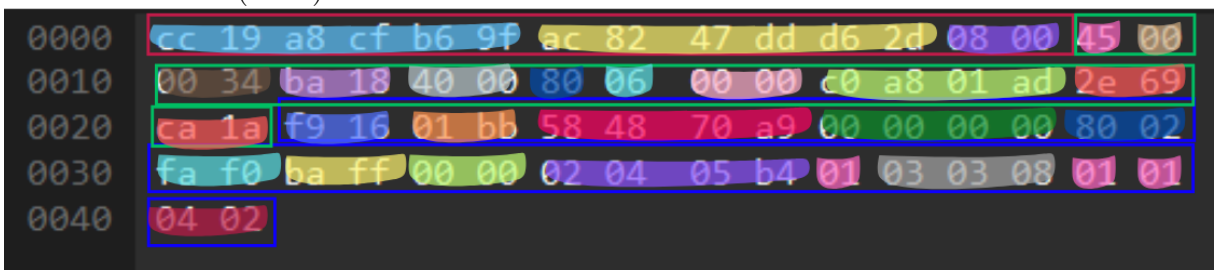
- Trame DNS 559 (réponse, A)



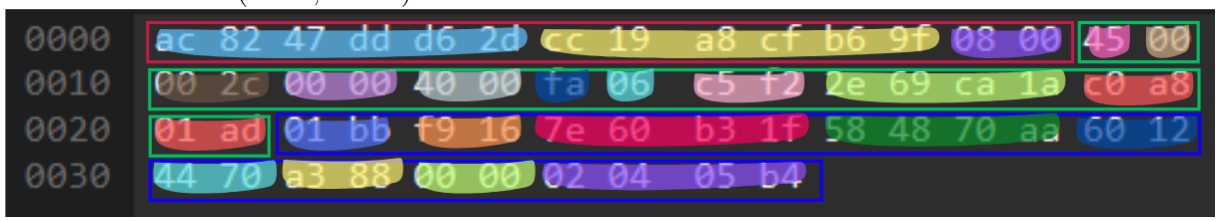
- Légende DNS (pour décoder une partie de la trame, vérifier dans quel rectangle elle se situe puis sa coloration, dans cet ordre)



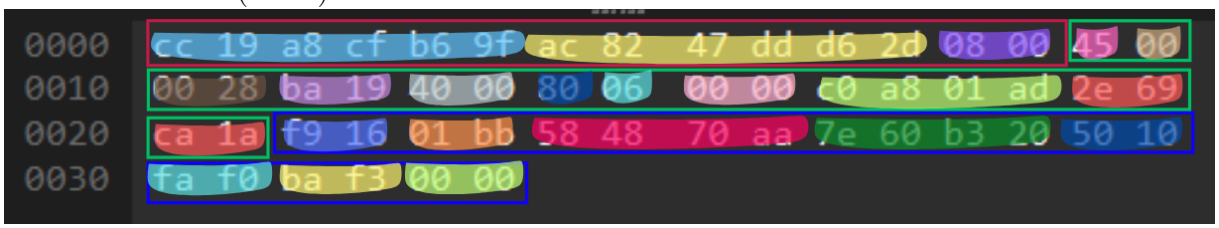
- Trame TCP 563 (SYN)



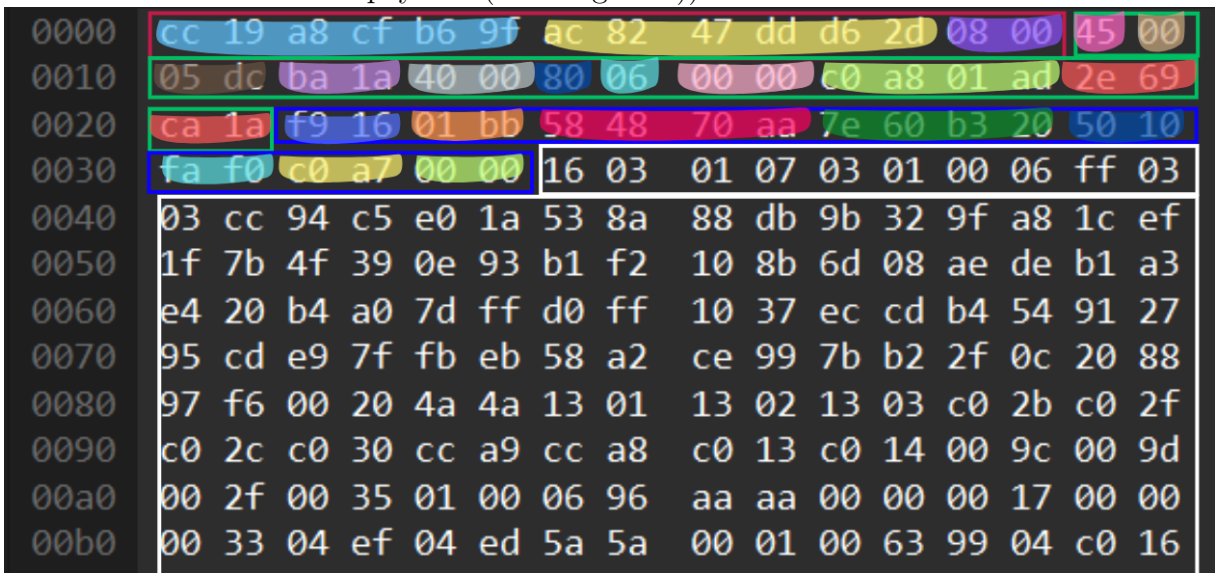
- Trame TCP 566 (SYN, ACK)



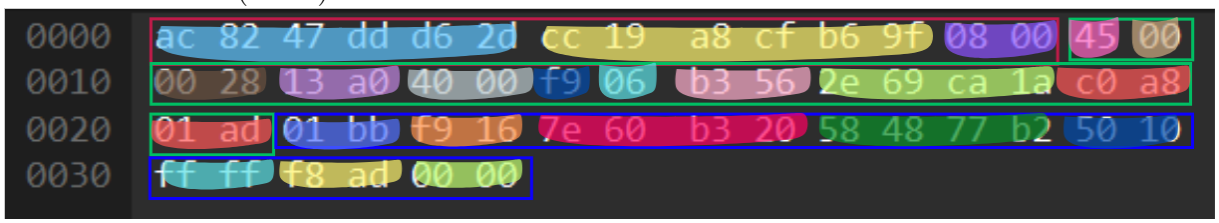
- Trame TCP 567 (ACK)



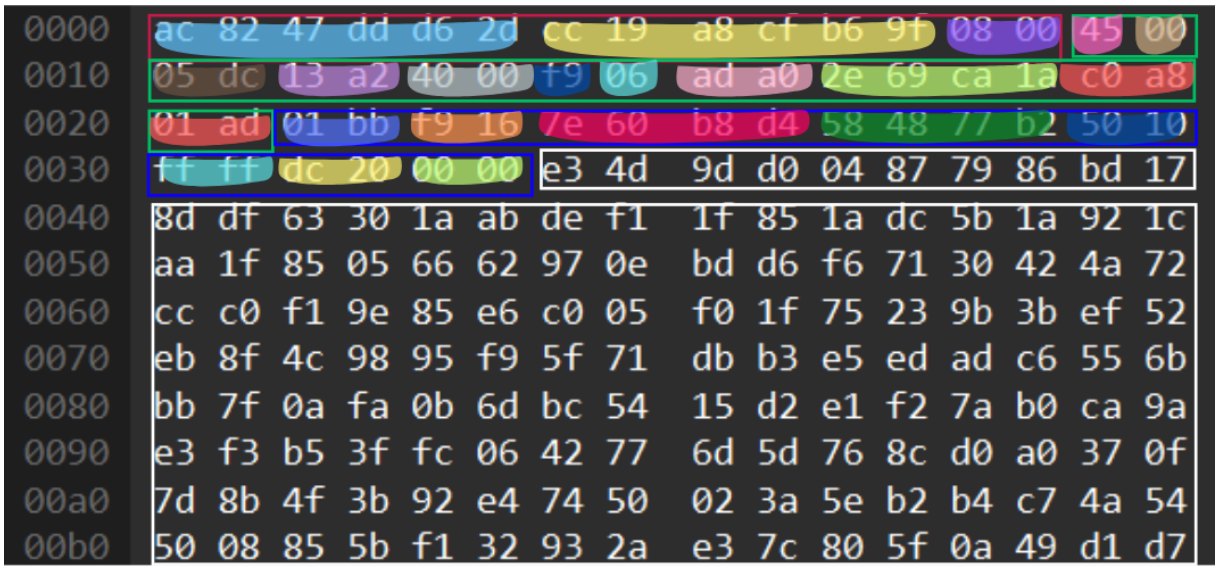
- Trame TCP 568 (ACK)
  La capture d'écran suivante représente le début de la trame. (La partie restante de la trame est constituée de payload (data segment))



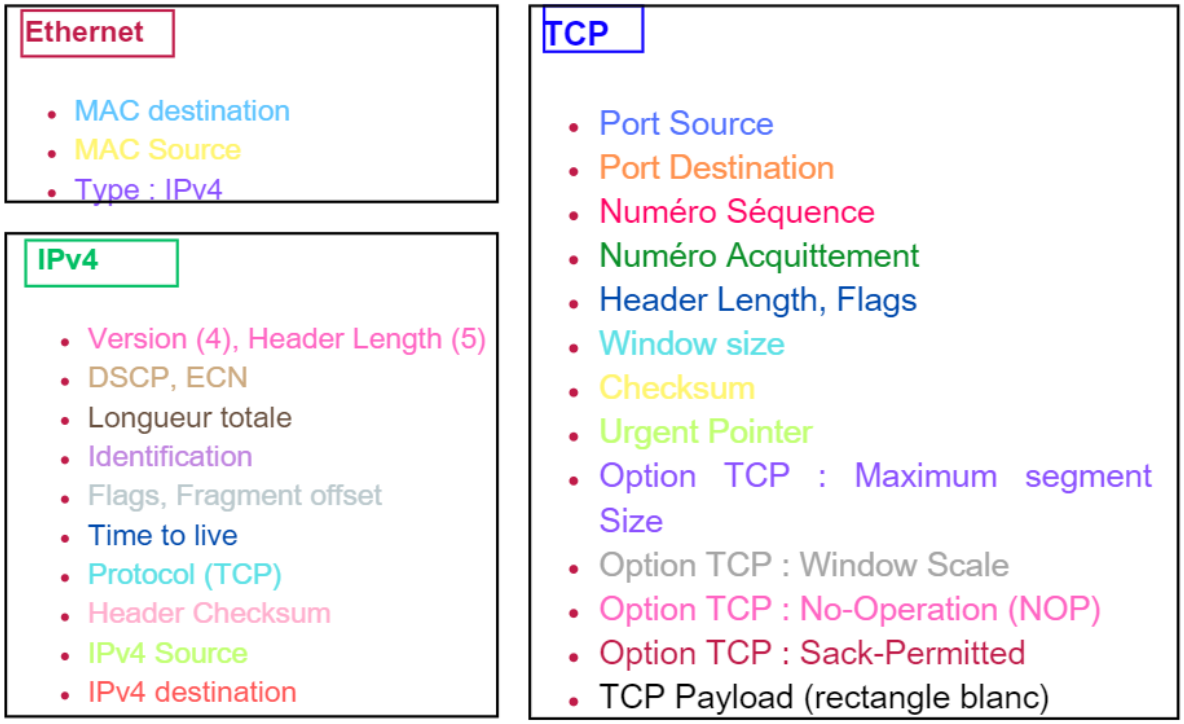
- Trame TCP 571 (ACK)



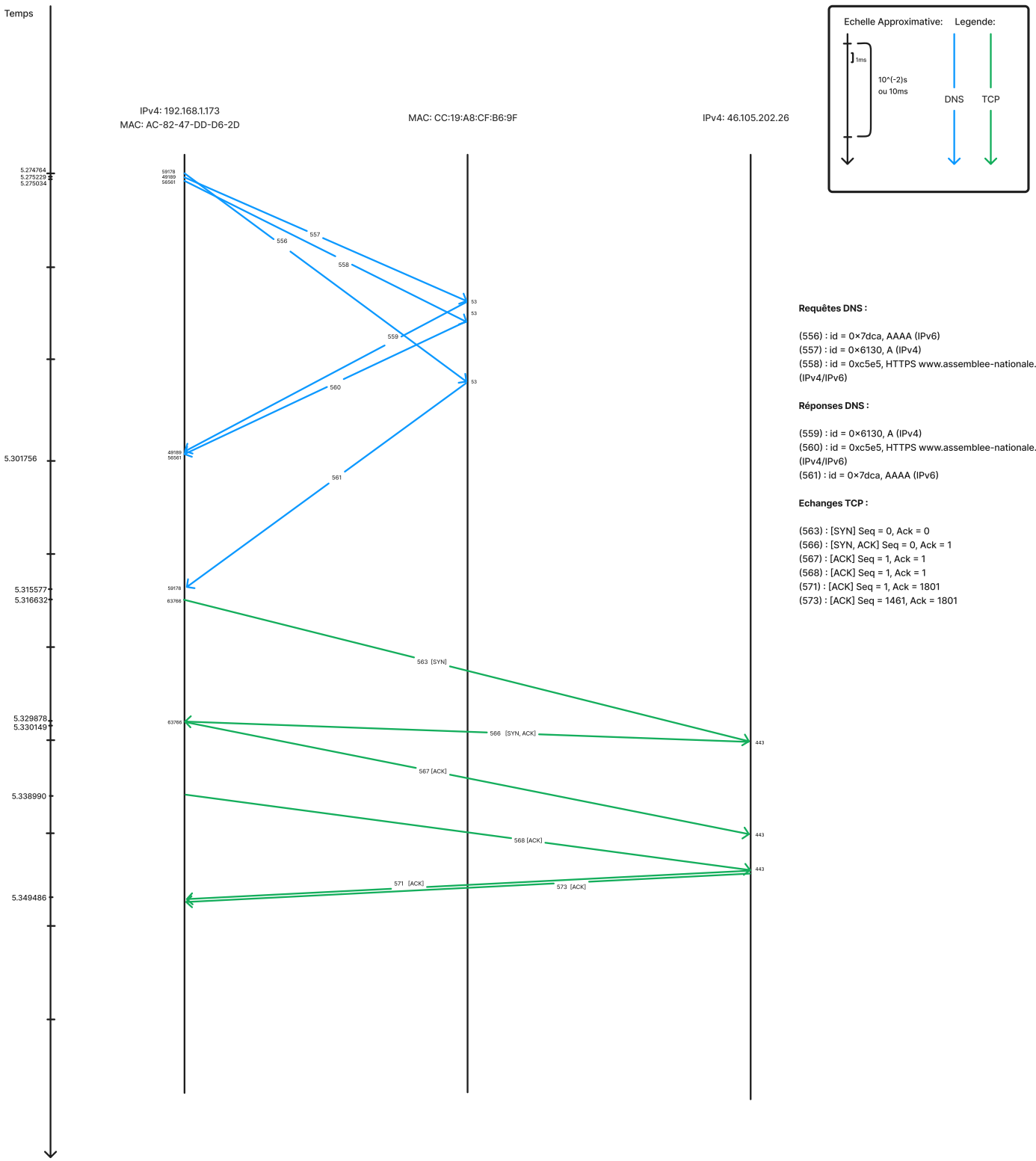
- Trame TCP 573 (ACK)
  La capture d'écran suivante représente le début de la trame. (La partie restante de la trame est constituée de payload (data segment))



- Légende TCP (pour décoder une partie de la trame, vérifier dans quel rectangle elle se situe puis sa coloration, dans cet ordre)



4 Chronogramme de l'Echange dans le temps



Requêtes DNS :

(556) : id = 0×7dca, AAAA (IPv6)
(557) : id = 0×6130, A (IPv4)
(558) : id = 0xc5e5, HTTPS www.assemblee-nationale.fr (IPv4/IPv6)

Réponses DNS :

(559) : id = 0×6130, A (IPv4)
(560) : id = 0xc5e5, HTTPS www.assemblee-nationale.fr (IPv4/IPv6)
(561) : id = 0×7dca, AAAA (IPv6)

Echanges TCP :

(563) : [SYN] Seq = 0, Ack = 0
(566) : [SYN, ACK] Seq = 0, Ack = 1
(567) : [ACK] Seq = 1, Ack = 1
(568) : [ACK] Seq = 1, Ack = 1
(571) : [ACK] Seq = 1, Ack = 1801
(573) : [ACK] Seq = 1461, Ack = 1801