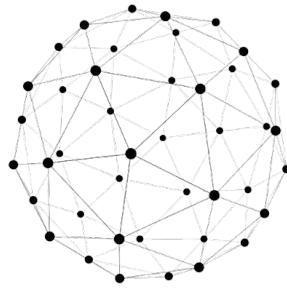


Sorbonne Université  
LU2IN023 - DM Réseaux

SOUAIBY Christina 21102782

Avril 2024

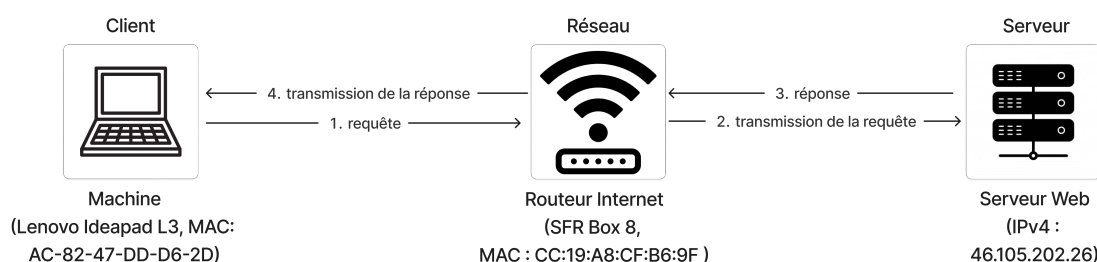


## Sommaire

1	Configuration de la Capture	2
2	Capture et Analyse du Trafic	2
3	Représentation Hexadécimale des Messages Échangés	3
4	Chronogramme de l'Échange dans le temps	6

# 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](http://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.

No.	Time	Source	Destination	Protocol	Length	Info
556	5.274764	192.168.1.173	192.168.1.1	DNS	86	Standard query 0x7dca AAAA www.assemblee-nationale.fr
557	5.275034	192.168.1.173	192.168.1.1	DNS	86	Standard query 0x6130 A www.assemblee-nationale.fr
558	5.275229	192.168.1.173	192.168.1.1	DNS	86	Standard query 0xc5e5 HTTPS www.assemblee-nationale.fr
559	5.301756	192.168.1.1	192.168.1.173	DNS	193	Standard query response 0xc5e5 www.assemblee-nationale.fr CNAME www.assemblee-nationale.fr.web.cdn.anycast.me CNA...
560	5.301756	192.168.1.1	192.168.1.173	DNS	232	Standard query response 0xc5e5 HTTPS www.assemblee-nationale.fr CNAME www.assemblee-nationale.fr.web.cdn.anycast.me...
561	5.315577	192.168.1.1	192.168.1.173	DNS	232	Standard query response 0x7dca AAAA www.assemblee-nationale.fr CNAME www.assemblee-nationale.fr.web.cdn.anycast.me...

- 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.

No.	Time	Source	Destination	Protocol	Length	Info
557	5.275034	192.168.1.173	192.168.1.1	DNS	86	Standard query 0x6130 A www.assemblee-nationale.fr
559	5.301756	192.168.1.1	192.168.1.173	DNS	193	Standard query response 0x6130 A www.assemblee-nationale.fr CNAME www.assemblee-nationale.fr.web.cdn.anycast.me CNA...

- (\*) 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.

```

Frame 559: 103 bytes on wire (1544 bits), 103 bytes captured (1544 bits) on interface DeviceNPF {FE28E709-B06A-4EAF-97E8-52635A390015}, id 0
  Ethernet II, Src: PTInovaçõeS_cf:b6:9f (cc:19:a8:cf:b6:9f), Dst: Intel_dd:d6:2d (ac:82:47:dd:d6:2d)
  Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.173
  User Datagram Protocol, Src Port: 53, Dst Port: 49189
  Domain Name System (response)
    Transaction ID: 0x6130
    Flags: 0x0100 Standard query response, No error
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 0
    Queries
    Answers
      www.assemblee-nationale.fr: type CNAME, class IN, cname www.assemblee-nationale.fr.web.cdn.anycast.me
      www.assemblee-nationale.fr.web.cdn.anycast.me: type CNAME, class IN, cname 46-105-202-26.any.cdn.anycast.me
      46-105-202-26.any.cdn.anycast.me: type A, class IN, addr 46.105.202.26
    [Time: 0.026722000 seconds]

```

- 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.

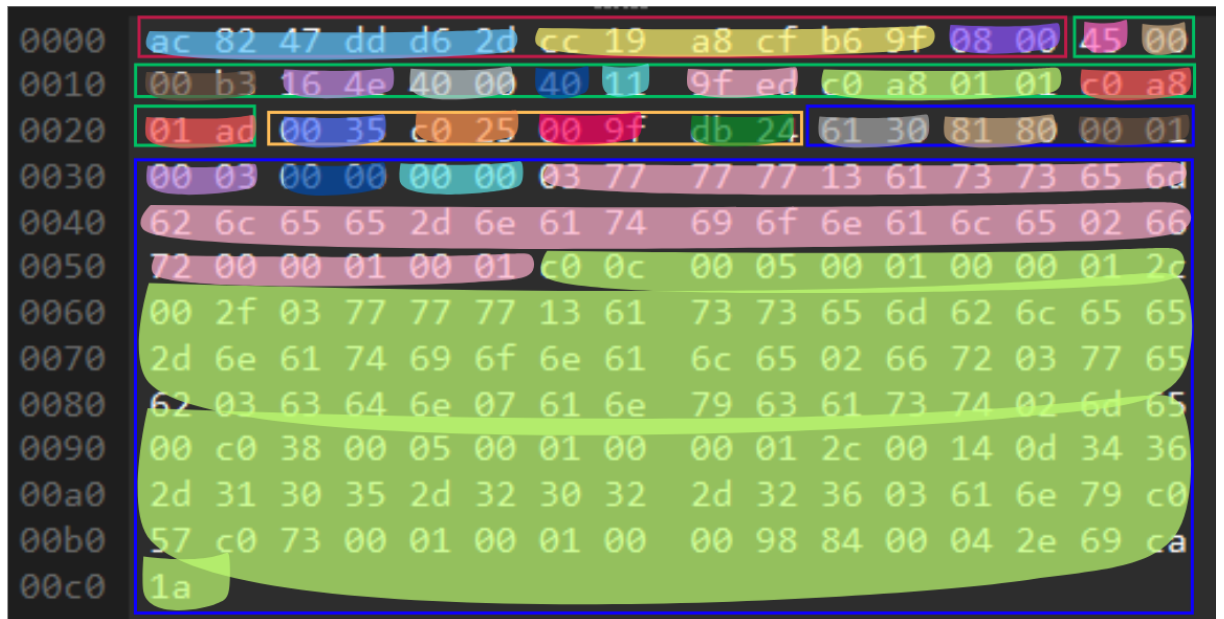
tcp and ip.addr == 46.105.202.26						
No.	Time	Source	Destination	Protocol	Length	Info
563	5.316632	192.168.1.173	46.105.202.26	TCP	66	63766 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
566	5.329878	46.105.202.26	192.168.1.173	TCP	58	443 → 63766 [SYN, ACK] Seq=0 Ack=1 Win=17520 Len=0 MSS=1460
567	5.330149	192.168.1.173	46.105.202.26	TCP	54	63766 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
568	5.338990	192.168.1.173	46.105.202.26	TCP	1514	63766 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=1460 [TCP segment of a reassembled PDU]
569	5.338990	192.168.1.173	46.105.202.26	TLSv1...	394	Client Hello (SNI=www.assemblee-nationale.fr)
570	5.349486	46.105.202.26	192.168.1.173	TCP	54	[TCP Window Update] 443 → 63766 [ACK] Seq=1 Ack=1 Win=65535 Len=0
571	5.349486	46.105.202.26	192.168.1.173	TCP	54	443 → 63766 [ACK] Seq=1 Ack=1801 Win=65535 Len=0
572	5.349486	46.105.202.26	192.168.1.173	TLSv1...	1514	Server Hello, Change Cipher Spec, Application Data
573	5.349486	46.105.202.26	192.168.1.173	TCP	1514	443 → 63766 [ACK] Seq=1461 Ack=1801 Win=65535 Len=1460 [TCP segment of a reassembled PDU]

### 3 Représentation Hexadécimale des Messages Échangés

- Trame DNS 557 (requête, A)

0000	cc 19 a8 cf b6 9f ac 82 47 dd d6 2d 08 00 45 00
0010	00 48 01 9c 00 00 80 11 00 00 c0 a8 01 ad c0 a8
0020	01 01 c0 25 00 35 00 34 84 44 61 30 01 00 00 01
0030	00 00 00 00 00 00 03 77 77 77 13 61 73 73 65 6d
0040	62 6c 65 65 2d 6e 61 74 69 6f 6e 61 6c 65 02 66
0050	72 00 00 01 00 01

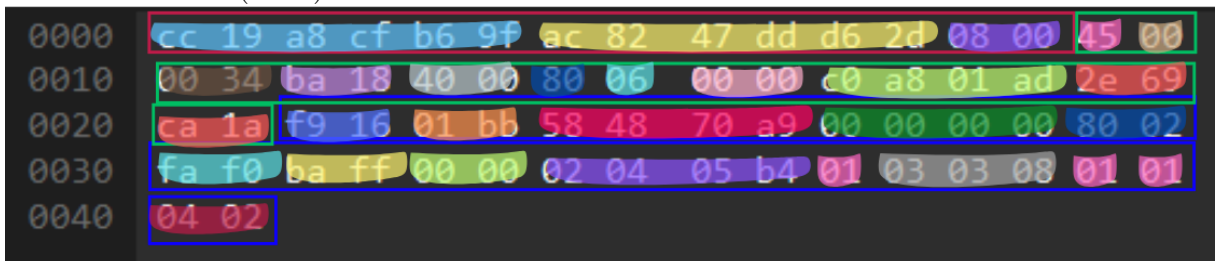
- Trame DNS 559 (réponse, A)



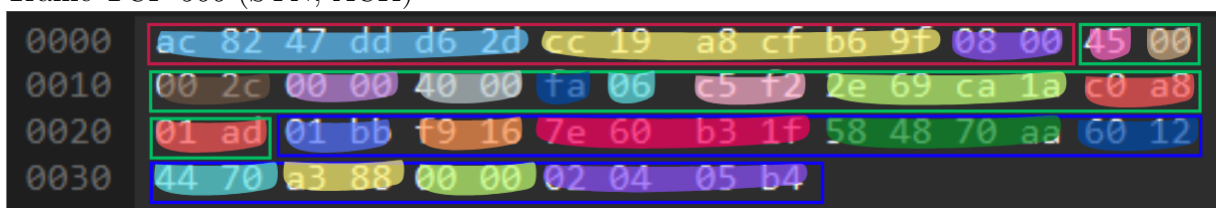
- Légende DNS (pour décoder une partie de la frame, vérifier dans quel rectangle elle se situe puis sa coloration, dans cet ordre)

<b>Ethernet</b> <ul style="list-style-type: none"> <li>• MAC destination</li> <li>• MAC Source</li> <li>• Type : IPv4</li> </ul>	<b>IPv4</b> <ul style="list-style-type: none"> <li>• Version (4), Header Length (5)</li> <li>• DSCP, ECN</li> <li>• Longueur totale</li> <li>• Identification</li> <li>• Flags, Fragment offset</li> <li>• Time to live</li> <li>• Protocol (UDP)</li> <li>• Header Checksum</li> <li>• IPv4 Source</li> <li>• IPv4 destination</li> </ul>	<b>Requête / Réponse</b> <ul style="list-style-type: none"> <li>• Transaction ID</li> <li>• Flags</li> <li>• Questions</li> <li>• Réponses</li> <li>• Authority RRs</li> <li>• Additional RRs</li> <li>• Queries (URL demandée)</li> <li>• Responses</li> </ul>
<b>Protocole</b> <ul style="list-style-type: none"> <li>• Port Source</li> <li>• Port Destination</li> <li>• Longueur</li> <li>• Checksum</li> </ul>		

- Trame TCP 563 (SYN)



- Trame TCP 566 (SYN, ACK)



- Trame TCP 567 (ACK)

0000	cc 19 a8 cf b6 9f ac 82 47 dd d6 2d 08 00 45 00
0010	00 28 ba 19 40 00 80 06 00 00 c0 a8 01 ad 2e 69
0020	ca 1a f9 16 01 bb 58 48 70 aa 7e 60 b3 20 50 10
0030	fa f0 ba f3 00 00

- 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))

0000	cc 19 a8 cf b6 9f ac 82 47 dd d6 2d 08 00 45 00
0010	05 dc ba 1a 40 00 80 06 00 00 c0 a8 01 ad 2e 69
0020	ca 1a f9 16 01 bb 58 48 70 aa 7e 60 b3 20 50 10
0030	fa f0 c0 a7 00 00 16 03 01 07 03 01 00 06 ff 03
0040	03 cc 94 c5 e0 1a 53 8a 88 db 9b 32 9f a8 1c ef
0050	1f 7b 4f 39 0e 93 b1 f2 10 8b 6d 08 ae de b1 a3
0060	e4 20 b4 a0 7d ff d0 ff 10 37 ec cd b4 54 91 27
0070	95 cd e9 7f fb eb 58 a2 ce 99 7b b2 2f 0c 20 88
0080	97 f6 00 20 4a 4a 13 01 13 02 13 03 c0 2b c0 2f
0090	c0 2c c0 30 cc a9 cc a8 c0 13 c0 14 00 9c 00 9d
00a0	00 2f 00 35 01 00 06 96 aa aa 00 00 00 17 00 00
00b0	00 33 04 ef 04 ed 5a 5a 00 01 00 63 99 04 c0 16

- Trame TCP 571 (ACK)

0000	ac 82 47 dd d6 2d cc 19 a8 cf b6 9f 08 00 45 00
0010	00 28 13 a0 40 00 f9 06 b3 56 2e 69 ca 1a c0 a8
0020	01 ad 01 bb f9 16 7e 60 b3 20 58 48 77 b2 50 10
0030	ff ff f8 ad 00 00

- 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))

0000	ac	82	47	dd	d6	2d	cc	19	a8	cf	b6	9f	08	00	45	00
0010	05	dc	13	a2	40	00	f9	06	ad	a0	2e	69	ca	1a	c0	a8
0020	01	ad	01	bb	f9	16	7e	60	b8	d4	58	48	77	b2	50	10
0030	ff	ff	dc	20	00	00	e3	4d	9d	d0	04	87	79	86	bd	17
0040	8d	df	63	30	1a	ab	de	f1	1f	85	1a	dc	5b	1a	92	1c
0050	aa	1f	85	05	66	62	97	0e	bd	d6	f6	71	30	42	4a	72
0060	cc	c0	f1	9e	85	e6	c0	05	f0	1f	75	23	9b	3b	ef	52
0070	eb	8f	4c	98	95	f9	5f	71	db	b3	e5	ed	ad	c6	55	6b
0080	bb	7f	0a	fa	0b	6d	bc	54	15	d2	e1	f2	7a	b0	ca	9a
0090	e3	f3	b5	3f	fc	06	42	77	6d	5d	76	8c	d0	a0	37	0f
00a0	7d	8b	4f	3b	92	e4	74	50	02	3a	5e	b2	b4	c7	4a	54
00b0	50	08	85	5b	f1	32	93	2a	e3	7c	80	5f	0a	49	d1	d7

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

<div>Ethernet</div> <ul style="list-style-type: none"> <li>• MAC destination</li> <li>• MAC Source</li> <li>• Type : IPv4</li> </ul>	<div>TCP</div> <ul style="list-style-type: none"> <li>• Port Source</li> <li>• Port Destination</li> <li>• Numéro Séquence</li> <li>• Numéro Acquiescement</li> <li>• Header Length, Flags</li> <li>• Window size</li> <li>• Checksum</li> <li>• Urgent Pointer</li> <li>• Option TCP : Maximum segment Size</li> <li>• Option TCP : Window Scale</li> <li>• Option TCP : No-Operation (NOP)</li> <li>• Option TCP : Sack-Permitted</li> <li>• TCP Payload (rectangle blanc)</li> </ul>
<div>IPv4</div> <ul style="list-style-type: none"> <li>• Version (4), Header Length (5)</li> <li>• DSCP, ECN</li> <li>• Longueur totale</li> <li>• Identification</li> <li>• Flags, Fragment offset</li> <li>• Time to live</li> <li>• Protocol (TCP)</li> <li>• Header Checksum</li> <li>• IPv4 Source</li> <li>• IPv4 destination</li> </ul>	

## 4 Chronogramme de l'Echange dans le temps

