

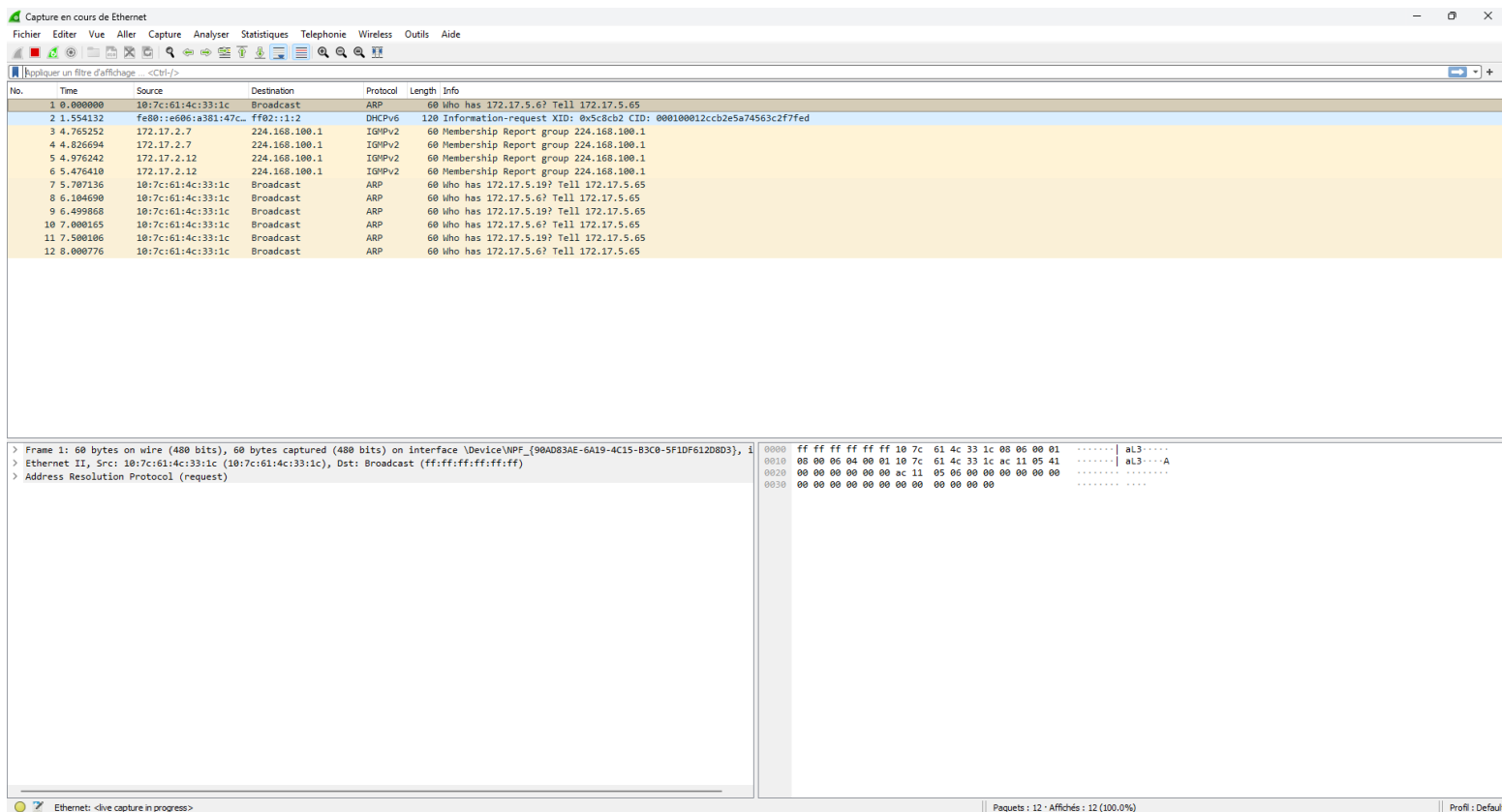
TP 5 – Trames ARP, ICMP et DNS

Sommaire

Captures de Trames ARP et ICMP :.....	1
Captures de Trames ARP, DNS et ICMP :.....	6
Commande Tracert et capture de trames ICMP.....	12

Captures de Trames ARP et ICMP :

Ouverture de wireshark et lancement d'une capture de Trames :



Ping du serveur du serveur Aviateur (172.17.254.5) :

```
Microsoft Windows [version 10.0.26100.6584]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\mballester>ping 172.17.254.5

Envoi d'une requête 'Ping' 172.17.254.5 avec 32 octets de données :
Réponse de 172.17.254.5 : octets=32 temps<1ms TTL=64
Réponse de 172.17.254.5 : octets=32 temps<1ms TTL=64
Réponse de 172.17.254.5 : octets=32 temps<1ms TTL=64
Réponse de 172.17.254.5 : octets=32 temps<1ms TTL=64

Statistiques Ping pour 172.17.254.5:
  Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
  Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms

C:\Users\mballester>
```

Echange ARP et ICMP suite au ping de aviateur :

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Stormshi_2a:a8:34	Broadcast	ARP	60	Who has 172.17.2.15? Tell 172.17.250.3
2	0.677235	Giga-Byt_2f:9c:c6	Broadcast	ARP	60	Who has 172.17.2.19? Tell 172.17.2.12
17	3.046547	Giga-Byt_2f:9c:c6	Broadcast	ARP	60	Who has 172.17.2.19? Tell 172.17.2.12
21	3.672886	Giga-Byt_2f:9c:c6	Broadcast	ARP	60	Who has 172.17.2.19? Tell 172.17.2.12
28	4.666963	Giga-Byt_2f:9c:c6	Broadcast	ARP	60	Who has 172.17.2.19? Tell 172.17.2.12
30	5.784341	Giga-Byt_2f:80:d8	Synology_32:37:b5	ARP	42	Who has 172.17.254.5? Tell 172.17.2.14
31	5.785200	Synology_32:37:b5	Giga-Byt_2f:80:d8	ARP	60	172.17.254.5 is at 00:11:32:32:37:b5
4	1.068323	172.17.2.14	172.17.254.5	ICMP	74	Echo (ping) request id=0x0001, seq=69/17664, ttl=128 (reply in 5)
5	1.068885	172.17.254.5	172.17.2.14	ICMP	74	Echo (ping) reply id=0x0001, seq=69/17664, ttl=64 (request in 4)
9	2.082754	172.17.2.14	172.17.254.5	ICMP	74	Echo (ping) request id=0x0001, seq=70/17920, ttl=128 (reply in 10)
10	2.083301	172.17.254.5	172.17.2.14	ICMP	74	Echo (ping) reply id=0x0001, seq=70/17920, ttl=64 (request in 9)
18	3.087199	172.17.2.14	172.17.254.5	ICMP	74	Echo (ping) request id=0x0001, seq=71/18176, ttl=128 (reply in 19)
19	3.087767	172.17.254.5	172.17.2.14	ICMP	74	Echo (ping) reply id=0x0001, seq=71/18176, ttl=64 (request in 18)
23	4.092261	172.17.2.14	172.17.254.5	ICMP	74	Echo (ping) request id=0x0001, seq=72/18432, ttl=128 (reply in 24)
24	4.093041	172.17.254.5	172.17.2.14	ICMP	74	Echo (ping) reply id=0x0001, seq=72/18432, ttl=64 (request in 23)

Contenu de cache ARP pour vérifiez la présence de l'association @IP-@MAC correspondant à Aviateur :

```
Interface : 172.17.2.14 --- 0xa
Adresse Internet      Adresse physique      Type
172.17.2.12          74-56-3c-2f-9c-c6     dynamique
172.17.2.15          74-56-3c-2f-9c-fc     dynamique
172.17.5.3           60-cf-84-c0-b1-66     dynamique
172.17.250.3         00-0d-b4-2a-a8-34     dynamique
172.17.254.1         d4-ae-52-7d-0e-2b     dynamique
172.17.254.5         00-11-32-32-37-b5     dynamique
172.17.255.255       ff-ff-ff-ff-ff-ff     statique
224.0.0.2            01-00-5e-00-00-02     statique
224.0.0.22           01-00-5e-00-00-16     statique
224.0.0.252          01-00-5e-00-00-fc     statique
224.168.100.1        01-00-5e-28-64-01     statique
239.255.255.250     01-00-5e-7f-ff-fa     statique
239.255.255.254     01-00-5e-7f-ff-fe     statique *
```

Quelle signification ont les octets de position 0x0C et 0x0D ligne 0000 ? :

- Les octets de position 0x0C et 0x0D signifie qu'il corresponde au champ ethertype qui correspond ici au protocole ARP (0806)

Quelle est la fonction de la trame ARP Request ? :

- La fonction de la trame ARP Request est de demander une adresse MAC par rapport a une adresse IP

Quelle signification ont les octets de position 0x04 et 0x05 ligne 0010 ? :

- Ces octets corresponde au champ Opcode (00 01 pour une request et 00 02 pour une reply)

Quelle est la longueur d'un message ARP contenu dans la trame ? :

- La longueur d'un message ARP est de 28 octets

Quelle est la longueur de la trame ARP Request ? :

- La longueur de la trame ARP Request est de 42 octets

Quelle est la longueur de la trame ARP Reply ? :

- La longueur de la trame ARP Reply est de 60 octets

Combien d'octets sont utilisés pour le padding ? :

- 18 octets sont utilisés pour le padding

Trame ARP Request	
@MAC Destination = 00:11:32:32:37:b5	
@MAC Source = 74:56:3c:2f:80:d8	
Ethernet Type = 0806	
Op code (valeur hexa.) = 00 01	
@MAC de la cible = 00:11:32:32:37:b5	
@IP de la cible = 172.17.254.5	

Selection d'une Trame ICMP echo request :

4	1.068323	172.17.2.14	172.17.254.5	ICMP	74 Echo (ping) request	id=0x0001, seq=69/17664, ttl=128 (reply in 5)
5	1.068885	172.17.254.5	172.17.2.14	ICMP	74 Echo (ping) reply	id=0x0001, seq=69/17664, ttl=64 (request in 4)
9	2.082754	172.17.2.14	172.17.254.5	ICMP	74 Echo (ping) request	id=0x0001, seq=70/17920, ttl=128 (reply in 10)
10	2.083301	172.17.254.5	172.17.2.14	ICMP	74 Echo (ping) reply	id=0x0001, seq=70/17920, ttl=64 (request in 9)
18	3.087199	172.17.2.14	172.17.254.5	ICMP	74 Echo (ping) request	id=0x0001, seq=71/18176, ttl=128 (reply in 19)
19	3.087767	172.17.254.5	172.17.2.14	ICMP	74 Echo (ping) reply	id=0x0001, seq=71/18176, ttl=64 (request in 18)
23	4.091261	172.17.2.14	172.17.254.5	ICMP	74 Echo (ping) request	id=0x0001, seq=72/18432, ttl=128 (reply in 24)
24	4.093041	172.17.254.5	172.17.2.14	ICMP	74 Echo (ping) reply	id=0x0001, seq=72/18432, ttl=64 (request in 23)

> Frame 4: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{90AD83AE-6A19-4C15-83C0-5F1DF612D8D3}, 1		0000	00 11 32 32 37 b5 74 56 3c 2f 80 d8 08 00 45 00	..227 tv </----E
> Ethernet II, Src: Giga-Byt_2f:80:d8 (74:56:3c:2f:80:d8), Dst: Synology_32:37:b5 (00:11:32:32:37:b5)		0010	00 3c 4b 8a 00 00 80 01 00 00 ac 11 02 0e ac 11	<K-----
> Destination: Synology_32:37:b5 (00:11:32:32:37:b5)		0020	fe 05 08 00 4d 16 00 01 00 45 61 62 63 64 65 66	...Eabcdef
> Source: Giga-Byt_2f:80:d8 (74:56:3c:2f:80:d8)		0030	67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76	ghijklmopqrstuv
Type: IPv4 (0x0800)		0040	77 61 62 63 64 65 66 67 68 69	wabcedfg hi
> Internet Protocol Version 4, Src: 172.17.2.14, Dst: 172.17.254.5				
> Internet Control Message Protocol				

Quelle signification ont les octets de position 0x0C et 0x0D ligne 0000 ? :

- Les octets de position 0x0C et 0x0D corresponde au champ Ethertype, ce qui signifie que ici ils corresponde au protocole IP (0800)

Quelle signification a l'octet de position 0x07 ligne 0010 ? :

- L'octet de position 0x07 ligne 10 est 01 ce qui correspond au protocole ICMP

Quelle est la longueur de la trame ? :

- La longueur de la trame est de 74 octets

Quelle est la longueur du paquet IP ? :

- La longueur du paquet IP est de 60 octets

Quelle est la longueur du message ICMP ? :

- La longueur du message ICMP est 40 octets

Quelle signification a l'octet de position 0x02 ligne 0020 ? :

- L'octet de position 0x02 ligne 0020 correspond au champ TYPE qui est ici 08 ce qui correspond bien a une echo request

A quoi correspondent les octets à partir de l'octet 0x0A, ligne 0020 ? :

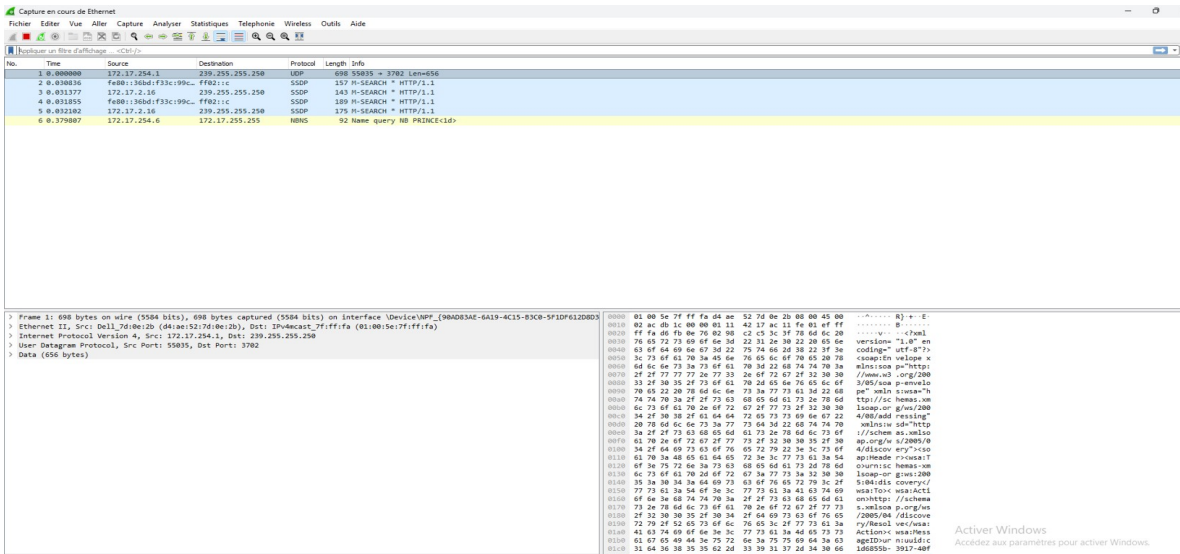
- Les octets a partir de l'octet 0x0A ligne 0020 correspondent au données du message ICMP

Sélectionnez une trame ICMP Echo Reply. Quelle est le nom et la valeur de l'octet de position 0x02 ligne 0020 ? :

- L'octet de position 0x02 ligne 0020 correspond au champ TYPE, ici il a pour valeur 00 ce qui correspond bien a une echo reply

Captures de Trames ARP, DNS et ICMP :

démarrage d'une capture de trame :



je vide la cache ARP a l'aide de la commande arp -b * :

```

Microsoft Windows [version 10.0.26100.6584]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\mballester>arp -b *

Affiche et modifie les tables de traduction d'adresses IP en adresses
physiques utilisées par le protocole de résolution d'adresses ARP.

ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr] [-v]

-a          Affiche les entrées ARP en cours en interrogeant les données
            en cours du protocole. Si inet_addr est spécifié, seules les
            adresses IP et physiques de l'ordinateur spécifié sont
            affichées. Si plus d'une interface réseau utilise ARP, les
            entrées de chaque table ARP sont affichées.
-g          Identique à -a.
-v          Affiche les entrées ARP en cours en mode verbeux. Toutes les
            entrées non valides ainsi que celles de l'interface de retour
            de bouclage sont affichées.
inet_addr  Spécifie un adresse Internet.
-N if_addr Affiche les entrées ARP de chaque interface réseau spécifiée
            par if_addr.
-d          Supprime l'hôte spécifié par inet_addr. inet_addr peut
            contenir le caractère générique * pour supprimer tous
            les hôtes.
-s          Ajoute l'hôte et associe l'adresse Internet inet_addr
            avec l'adresse physique eth_addr. L'adresse physique
            est donnée sous forme de 6 octets hexadécimaux séparés
            par des tirets. L'entrée est permanente.
eth_addr   Spécifie une adresse physique.
if_addr    Spécifie l'adresse Internet de l'interface dont la table
            de traduction d'adresses doit être modifiée.
            Si ce paramètre n'est pas indiqué, la première interface
            applicable sera utilisée.

Exemples :
> arp -s 157.55.85.212 00-aa-00-62-c6-09 ... Ajoute une entrée statique.
> arp -a ... Affiche la table ARP.

C:\Users\mballester>

```

et ensuite je ping le serveur web www.ac-nice.fr :

```
C:\Users\mballester>ping www.ac-nice.fr

Envoi d'une requête 'ping' sur www.ac-nice.fr.cdn.cloudflare.net [141.101.90.104] avec 32 octets de données :
Réponse de 141.101.90.104 : octets=32 temps=16 ms TTL=53
Réponse de 141.101.90.104 : octets=32 temps=17 ms TTL=53
Réponse de 141.101.90.104 : octets=32 temps=17 ms TTL=53
Réponse de 141.101.90.104 : octets=32 temps=17 ms TTL=53

Statistiques Ping pour 141.101.90.104:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 16ms, Maximum = 17ms, Moyenne = 16ms

C:\Users\mballester>
```

Capture ICMP ARP DNS :

No.	Time	Source	Destination	Protocol	Length	Info
102	0.661521	Vmware_22:87:16d	Broadcast	ARP	60	Who has 172.17.254.1? Tell 172.17.243.11
109	7.226959	Giga-Byt_2f:81:87	Broadcast	ARP	60	Who has 172.17.5.3? Tell 172.17.2.3
111	7.580436	Dell_7d:8e:2b	Giga-Byt_2f:9c:f7	ARP	60	Who has 172.17.2.8? Tell 172.17.254.1
114	7.629987	Vmware_22:87:16d	Broadcast	ARP	60	Who has 172.17.254.1? Tell 172.17.254.1
124	8.211895	Giga-Byt_2f:80:d8	Dell_7d:8e:2b	ARP	42	Who has 172.17.254.1? Tell 172.17.2.14
125	8.212786	Dell_7d:8e:2b	Giga-Byt_2f:80:d8	ARP	60	172.17.254.1 is at d4:aa:52:76:8e:2b
126	8.218541	Giga-Byt_2f:81:87	Broadcast	ARP	60	Who has 172.17.5.3? Tell 172.17.2.3
128	8.276888	Cisco_e9:0e:00	Broadcast	ARP	60	Who has 172.17.2.15? Tell 172.17.250.6
129	8.278187	Cisco_e9:0e:00	Broadcast	ARP	60	Who has 172.17.2.15? Tell 172.17.250.7
144	8.630222	Vmware_22:87:16d	Broadcast	ARP	60	Who has 172.17.244.15? Tell 172.17.243.11
28	3.480957	172.17.2.14	172.17.254.1	DNS	74	Standard query 0xc2f73 A www.ac-nice.fr
29	3.441185	172.17.2.14	172.17.254.1	DNS	74	Standard query response 0xc2f73 A www.ac-nice.fr
30	3.467115	172.17.254.1	172.17.2.14	DNS	185	Standard query response 0x3f73 A www.ac-nice.fr CNAME www.ac-nice.fr.cdn.cloudflare.net A 141.101.90.107 A 141.101.90.105 A 141.101.90.104 A 141.101.90.106
34	3.816664	172.17.2.14	172.17.254.1	DNS	72	Standard query 0x2968 A www.bing.com
35	3.816839	172.17.2.14	172.17.254.1	DNS	72	Standard query response 0x2968 A www.bing.com
36	3.818384	172.17.254.1	172.17.2.14	DNS	254	Standard query response 0xe558 HTTPS www.bing.com CNAME www-www.bing.com trafficmanager.net CNAME www.bing.com.edgekey.net CNAME e86303.dscx.akamaiedge.net SOA n0dscx.akamaiedge.net
37	3.819468	172.17.254.1	172.17.2.14	DNS	337	Standard query response 0x286d A www.bing.com CNAME www-www.bing.com trafficmanager.net CNAME www.bing.com.edgekey.net CNAME e86303.dscx.akamaiedge.net A 2.16.11.64 A 2.16.11.88 A 2.16.11.104
31	3.473219	172.17.2.14	141.101.90.107	ICMP	74	Echo (ping) request id=0x0001, seq=1/256, ttl=128 (reply in 32)
32	3.504369	141.101.90.107	172.17.2.14	ICMP	74	Echo (ping) reply id=0x0001, seq=1/256, ttl=53 (request in 31)
64	4.467796	172.17.2.14	141.101.90.107	ICMP	74	Echo (ping) request id=0x0001, seq=2/512, ttl=128 (reply in 60)
69	6.524191	141.101.90.107	172.17.2.14	ICMP	74	Echo (ping) reply id=0x0001, seq=2/512, ttl=53 (request in 64)
78	5.486188	172.17.2.14	141.101.90.107	ICMP	74	Echo (ping) request id=0x0001, seq=3/768, ttl=128 (reply in 88)
88	5.522453	141.101.90.107	172.17.2.14	ICMP	74	Echo (ping) reply id=0x0001, seq=3/768, ttl=53 (request in 78)
99	6.501831	172.17.2.14	141.101.90.107	ICMP	74	Echo (ping) request id=0x0001, seq=4/1024, ttl=128 (reply in 100)

La liste des trames commence par une requête et une réponse ARP. Quelle est la machine dont l'adresse MAC est recherchée ? :

- La machine dont l'adresse MAC est recherchée est la machine qui possède l'adresse IP qui est ici 172.17.254.1

Trame ARP request
@MAC destination = d4:ae:52:7d:0e:2b @MAC source = 74:56:3c:2f:80:d8 Ethernet Type = 0806
Opcode (valeurs hexa.) = 01 @MAC de la cible = d4:ae:52:7d:0e:2b @IP de la cible = 172.17.254.1

Pour quelle raison trouve-t-on ensuite une requête DNS avant l'échange de trames ICMP suite à l'exécution de la commande ping proprement dite ? :

- Avant d'envoyer les trames ICMP donc le ping, le nom du domaine doit être traduit en adresse IP. La traduction est réalisé par une requête DNS. Le client interroge le serveur DNS pour obtenir l'adresse IP avant de pouvoir lancer le ping.

Consultation du cache DNS à l'aide de la commande `ipconfig /displaydns` et vérification de la présence de l'enregistrement DNS `ac-nice.fr` et de l'adresse IP associée :

```

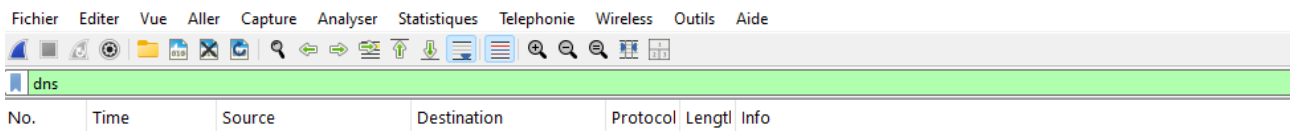
www.ac-nice.fr
-----
Nom d'enregistrement. : www.ac-nice.fr
Type d'enregistrement : 5
Durée de vie . . . . : 293
Longueur de données . : 8
Section . . . . . : Réponse
Enregistrement CNAME : www.ac-nice.fr.cdn.cloudflare.net

Nom d'enregistrement. : www.ac-nice.fr.cdn.cloudflare.net
Type d'enregistrement : 1
Durée de vie . . . . : 293
Longueur de données . : 4
Section . . . . . : Réponse
Enregistrement (hôte) : 141.101.90.104

Nom d'enregistrement. : www.ac-nice.fr.cdn.cloudflare.net
Type d'enregistrement : 1
Durée de vie . . . . : 293
Longueur de données . : 4
Section . . . . . : Réponse
Enregistrement (hôte) : 141.101.90.105

```

Démarrage d'une nouvelle capture et saisie de la commande ping www.ac-nice.fr dans l'invite de commandes :



On ne constate pas de requête DNS puisque l'enregistrement est présent dans le cache DNS.

Vidage du cache DNS :

```
C:\Users\mballester>ipconfig /flushdns
Configuration IP de Windows
Cache de résolution DNS vidé.
C:\Users\mballester>
```

Redémarrage d'une capture pour re-visualiser la requêtes DNS :

No.	Time	Source	Destination	Protocol	Length	Info
420	5.567921	HewlettPacka_2b:49:...	Broadcast	ARP	60	Who has 172.17.230.50? Tell 172.17.200.100
421	5.569877	HewlettPacka_2b:49:...	Broadcast	ARP	60	Who has 172.17.170.142? Tell 172.17.200.100
422	5.587702	GigaByteTech_2f:7f:...	Dell_7d:0e:2b	ARP	42	Who has 172.17.254.1? Tell 172.17.2.18
423	5.588223	Dell_7d:0e:2b	GigaByteTech_2f:7f:...	ARP	60	172.17.254.1 is at d4:ae:52:7d:0e:2b
424	5.600610	HewlettPacka_2b:49:...	Broadcast	ARP	60	Who has 172.17.170.151? Tell 172.17.200.100
425	5.603303	HewlettPacka_2b:49:...	Broadcast	ARP	60	Who has 172.17.230.50? Tell 172.17.200.100
426	5.634310	Dell_7d:0e:2b	GigaByteTech_2f:7f:...	ARP	60	Who has 172.17.2.18? Tell 172.17.254.1
53	1.818081	172.17.2.18	172.17.254.1	DNS	70	Standard query 0x9539 A www.ac-nice.fr
176	2.838449	172.17.2.18	172.17.254.1	DNS	74	Standard query 0xc41f A teams.live.com
179	2.888625	172.17.2.18	172.17.2.18	DNS	123	Standard query response 0x9539 A www.ac-nice.fr CNAME www.ac-nice.fr.cdn.cloudflare.net A 141.101.90.186 A 141.101.90.105 A 141.101.90.107 A 141.101.90.104
200	2.955883	172.17.2.18	172.17.254.1	DNS	77	Standard query 0x2100 A ocsip.digicert.com
207	2.982190	172.17.2.18	172.17.2.18	DNS	198	Standard query response 0x2100 A ocsip.digicert.com CNAME ocsip.edge.digicert.com CNAME cac-ocsip.digicert.com.edgekey.net CNAME e3913.cd.akamaiedge.net A 104.75.232.13
236	3.097046	172.17.2.18	172.17.254.1	DNS	79	Standard query 0x8066 A to-do.microsoft.com
241	3.149716	172.17.254.1	172.17.2.18	DNS	176	Standard query response 0x8066 A to-do.microsoft.com CNAME reroute.microsoft.com CNAME reroute443.trafficmanager.net A 20.231.239.246 A 20.112.250.133
347	4.538972	172.17.2.18	172.17.254.1	DNS	81	Standard query 0xc758 A oneocsp.microsoft.com
350	4.562816	172.17.2.18	172.17.2.18	DNS	168	Standard query response 0xc758 A oneocsp.microsoft.com CNAME oneocsp-microsoft-com-a-0003.a-msedge.net CNAME a-0003.a-msedge.net A 204.79.197.203
63	1.816088	172.17.2.18	141.101.90.106	ICMP	74	Echo (ping) request id=0x0001, seq=17/4352, ttl=128 (reply in 67)
67	1.845834	141.101.90.106	172.17.2.18	ICMP	74	Echo (ping) reply id=0x0001, seq=17/4352, ttl=53 (request in 63)
126	2.028714	172.17.2.18	141.101.90.106	ICMP	74	Echo (ping) request id=0x0001, seq=18/4608, ttl=128 (reply in 129)
129	2.046341	141.101.90.106	172.17.2.18	ICMP	74	Echo (ping) reply id=0x0001, seq=18/4608, ttl=53 (request in 126)
214	3.026889	172.17.2.18	141.101.90.106	ICMP	74	Echo (ping) request id=0x0001, seq=19/4864, ttl=128 (reply in 223)
223	3.052450	141.101.90.106	172.17.2.18	ICMP	74	Echo (ping) reply id=0x0001, seq=19/4864, ttl=53 (request in 214)


```

> Frame 61: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{409CF837-3706-4807-9099-685D620547EE},
Ethernet II, Src: GigaByteTech_2f:7f:ea (74:56:3c:2f:7f:ea), Dst: Dell_7d:0e:2b (d4:ae:52:7d:0e:2b)
  > Destination: Dell_7d:0e:2b (d4:ae:52:7d:0e:2b)
  > Source: GigaByteTech_2f:7f:ea (74:56:3c:2f:7f:ea)
  Type: IPv4 (0x0800)
  [Stream index: 5]
  > Internet Protocol Version 4, Src: 172.17.2.18, Dst: 172.17.254.1
  > User Datagram Protocol, Src Port: 59793, Dst Port: 53
    Source Port: 59793
    Destination Port: 53
    Length: 40
    Checksum: 0x5870 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
    [Stream Packet Number: 1]
    [Timestamps]
    UDP payload (32 bytes)
  > Domain Name System (query)
    Transaction ID: 0x9539
    > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  > Queries
    > www.ac-nice.fr: type A, class IN
    [Response Tm: 61]
  
```

les différents protocoles encapsulés dans une trame DNS sont :

- Le protocole IP
- Le protocole UDP
- Le protocole DNS

Quelle est la machine destinataire de la requête DNS ? Quelle est son IP (cf. en-tête IP) ? :

- La machine destinataire de la requête DNS est le serveur et il a pour IP 172.17.254.1

Quelle signification ont les octets de position 0x0C, 0x0D ligne 0000 et 0x07 ligne 0010 ? :

- les octets 0x0C et 0x0D ligne 0000 correspondre au champ ethertype, il ont pour valeur 0800 ce qui signifie que derrière on va avoir le protocole IP

- l'octet 0x07 ligne 0010 correspond au champ protocol qui a ici pour valeur 11 (17 decimal) ce qui correspond au protocol UDP

Quelle est la longueur de l'en-tête IP ? :

- La longueur de l'en tête IP est de 20 bytes (octets)

Quelle est la longueur de l'en-tête de transport dans cette trame ? :

- La longueur de l'en tête de transport de cette trame (UDP) est de 8 octets

Quelle signification ont les octets de position 0x04 et 0x05 ligne 0020 ? :

- Les octets de position 0x04 et 0x05 ligne 20 corresponde au champ port, ils ont pour valeur 0035 ici ce qui correspond au port destination (53) dont le port du serveur DNS

Quels sont les valeurs hexadécimales des octets correspondant au nom de domaine internet ac-nice.fr ? :

- Les valeurs hexadecimales des octets correspondant au nom de domaine internet ac-nice.fr sont : 61 63 2D 6E 69 63 65 02 66 72

Sélectionnez la trame comportant la réponse à la requête DNS et développez la section Domain Name System (response) et plus particulièrement la rubrique Answers. Recherchez les valeurs hexadécimales et décimales de l'adresse IP du serveur web hébergeant le site de l'académie de Nice :

Adresse décimale	Adresse hexadécimale
141.101.90.104	8D 65 5A 68
141.101.90.105	8D 65 5A 69
141.101.90.106	8D 65 5A 6A
141.101.90.107	8D 65 5A 6B

Commande Tracert et capture de trames ICMP

Capture de trame + saisie de la commande tracert www.ac-nice.fr dans l'invite de commande et filtrage des trames :

No.	Time	Source	Destination	Protocol	Length	Info
88	2.851714	172.17.2.18	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=93/23808, ttl=1 (no response found!)
89	2.853762	10.73.23.242	172.17.2.18	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
90	2.854248	172.17.2.18	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=94/24064, ttl=1 (no response found!)
91	2.856170	10.73.23.242	172.17.2.18	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
92	2.856484	172.17.2.18	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=95/24320, ttl=1 (no response found!)
93	2.858129	10.73.23.242	172.17.2.18	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
144	4.298386	172.17.2.18	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=96/24576, ttl=2 (no response found!)
145	4.299719	10.73.27.3	172.17.2.18	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
146	4.300157	172.17.2.18	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=97/24832, ttl=2 (no response found!)
147	4.301260	10.73.27.3	172.17.2.18	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
148	4.301528	172.17.2.18	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=98/25088, ttl=2 (no response found!)
149	4.302700	10.73.27.3	172.17.2.18	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
198	5.735054	172.17.2.18	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=99/25344, ttl=3 (no response found!)
199	5.750349	10.20.2.9	172.17.2.18	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
201	5.751307	172.17.2.18	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=100/25600, ttl=3 (no response found!)
202	5.766468	10.20.2.9	172.17.2.18	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
203	5.767018	172.17.2.18	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=101/25856, ttl=3 (no response found!)
205	5.782456	10.20.2.9	172.17.2.18	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
251	7.206077	172.17.2.18	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=102/26112, ttl=4 (no response found!)
253	7.221032	10.20.2.14	172.17.2.18	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
254	7.222016	172.17.2.18	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=103/26368, ttl=4 (no response found!)
257	7.236617	10.20.2.14	172.17.2.18	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
258	7.237276	172.17.2.18	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=104/26624, ttl=4 (no response found!)
259	7.252097	10.20.2.14	172.17.2.18	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
309	8.679246	172.17.2.18	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=105/26880, ttl=5 (no response found!)
310	8.695156	194.199.240.253	172.17.2.18	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
311	8.695795	172.17.2.18	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=106/27136, ttl=5 (no response found!)
312	8.711358	194.199.240.253	172.17.2.18	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
313	8.711905	172.17.2.18	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=107/27392, ttl=5 (no response found!)
315	8.727175	194.199.240.253	172.17.2.18	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
376	10.149441	172.17.2.18	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=108/27648, ttl=6 (no response found!)

Quelle est l'adresse IP Destination (valeurs déci. et hexa.) ? :

- L'adresse IP destination est 141.101.90.107 en décimal et 8D 65 5A 6B en hexadécimal

Quelle est la valeur portée par ce champ (valeurs déci. et hexa.) ? :

- La valeur portée par ce champ est 1 en décimal et 01 en hexadécimal

Quelle est la valeur portée par le champ Type (valeurs déci. et hexa.) ? :

- La valeur portée par le champ Type est 8 en décimal et 08 en hexadécimal

Quelle est la valeur portée par le champ Type (valeurs déci. et hexa.) ? :

- La valeur portée par le champ Type est 11 en décimal et 0b en hexadécimal