

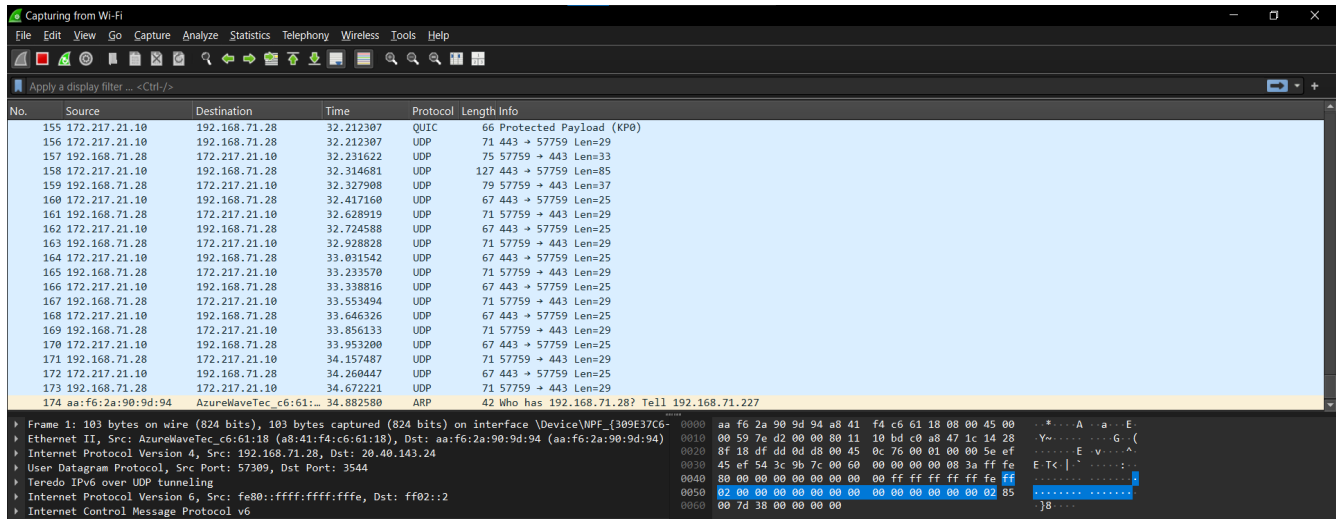
TP 5 – Trames ARP, ICMP et DNS

Sommaire

- 1. *Capture de trames ARP et ICMP*.....2
 - 1.2. Capture de trames ARP, DNS et ICMP.....6
- 2. *Commande Tracert et capture de trames ICMP*.....12

1. Capture de trames ARP et ICMP

→ On ouvre WireShark et on démarre une **capture de trame** :



→ On **ping** le serveur :

```
C:\Users\Noah>ping 192.168.71.227

Pinging 192.168.71.227 with 32 bytes of data:
Reply from 192.168.71.227: bytes=32 time=12ms TTL=64
Reply from 192.168.71.227: bytes=32 time=161ms TTL=64
Reply from 192.168.71.227: bytes=32 time=65ms TTL=64
Reply from 192.168.71.227: bytes=32 time=14ms TTL=64

Ping statistics for 192.168.71.227:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 12ms, Maximum = 161ms, Average = 63ms
```

→ On applique un **filtre arp / icmp** et on sauvegarde les trames obtenues sous le nom **"CaptureICMP"** :

No.	Source	Destination	Time	Protocol	Length	Info
148	aa:f6:2a:90:9d:94	AzureWaveTec_c6:61:...	41.399443	ARP	42	Who has 192.168.71.28? Tell 192.168.71.227
149	AzureWaveTec_c6:61:...	aa:f6:2a:90:9d:94	41.399472	ARP	42	192.168.71.28 is at a8:41:f4:c6:61:18
177	192.168.71.28	192.168.71.227	49.760155	ICMP	74	Echo (ping) request id=0x0001, seq=1/256, ttl=128 (reply in 178)
178	192.168.71.227	192.168.71.28	49.772094	ICMP	74	Echo (ping) reply id=0x0001, seq=1/256, ttl=64 (request in 177)
179	192.168.71.28	192.168.71.227	50.764733	ICMP	74	Echo (ping) request id=0x0001, seq=2/512, ttl=128 (reply in 180)
180	192.168.71.227	192.168.71.28	50.925876	ICMP	74	Echo (ping) reply id=0x0001, seq=2/512, ttl=64 (request in 179)
181	192.168.71.28	192.168.71.227	51.782936	ICMP	74	Echo (ping) request id=0x0001, seq=3/768, ttl=128 (reply in 182)
182	192.168.71.227	192.168.71.28	51.848067	ICMP	74	Echo (ping) reply id=0x0001, seq=3/768, ttl=64 (request in 181)
215	192.168.71.28	192.168.71.227	52.793041	ICMP	74	Echo (ping) request id=0x0001, seq=4/1024, ttl=128 (reply in 217)
217	192.168.71.227	192.168.71.28	52.807099	ICMP	74	Echo (ping) reply id=0x0001, seq=4/1024, ttl=64 (request in 215)
361	aa:f6:2a:90:9d:94	AzureWaveTec_c6:61:...	90.854325	ARP	42	Who has 192.168.71.28? Tell 192.168.71.227
362	AzureWaveTec_c6:61:...	aa:f6:2a:90:9d:94	90.854351	ARP	42	192.168.71.28 is at a8:41:f4:c6:61:18

File name: CaptureICMP Save

Save as: Wireshark/... - pcapng Cancel

Help

→ On arrête la capture de trames et on visualise le **cache ARP** avec la commande **arp -a** :

```
C:\Windows\system32>arp -a

Interface: 192.168.71.28 --- 0x7
Internet Address      Physical Address      Type
192.168.71.227       aa-f6-2a-90-9d-94    dynamic
```

→ On analyse l'échange de **trames ARP** :

> Frame 362: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)	0000	aa f6 2a 90 9d 94 a8 41 f4 c6 61 18 08 06 00 01	..*...A..a...
> Ethernet II, Src: a8:41:f4:c6:61:18 (a8:41:f4:c6:61:18), Dst: aa:f6:2a:90:9d:94	0010	08 00 06 04 00 02 a8 41 f4 c6 61 18 c0 a8 47 1cA..a...
▼ Address Resolution Protocol (reply)	0020	aa f6 2a 90 9d 94 c0 a8 47 e3	..*...G..
Hardware type: Ethernet (1)			
Protocol type: IPv4 (0x0800)			
Hardware size: 6			
Protocol size: 4			
Opcode: reply (2)			
Sender MAC address: a8:41:f4:c6:61:18 (a8:41:f4:c6:61:18)			
Sender IP address: 192.168.71.28			
Target MAC address: aa:f6:2a:90:9d:94 (aa:f6:2a:90:9d:94)			
Target IP address: 192.168.71.227			

* Les octets de position **0x0C** et **0x0D** ligne **0000** sont le champ **Ethertype** qui représente ici **ARP (0806)**.

* La fonction de la trame ARP Request est de demander quelle est l'**adresse MAC** d'une certaine adresse IP.

- * Les octets de position **0x04** et **0x05** ligne **0010** indiquent si la requête est une **request (00 01)** ou une **reply(00 02)**.
- * La longueur d'un message ARP contenu dans la trame est de **28 octets**.
- * La longueur de la trame ARP Request est de **48 octets**.
- * La longueur de la trame ARP Reply est de **42 octets**.
- * Il n'y a **aucuns** octets utilisés pour le padding.

Trame ARP request
@MAC destination = AA:F6:2A:90:9D:94
@MAC source = A8:41:F4:C6:61:18
Ethernet Type = 08 06
Opcode (valeurs hexa.) = 00 01
@MAC de la cible = 00:00:00:00:00
@IP de la cible = 192.168.71.28

→ On sélectionne une trame **ICMP Echo Request** :

No.	Time	Source	Destination	Protocol	Length	Info
148	41.399443	aa:f6:2a:90:9d:94	a8:41:f4:c6:61:18	ARP	42	Who has 192.168.71.28? Tell 192.168.71.227
149	41.399472	a8:41:f4:c6:61:18	aa:f6:2a:90:9d:94	ARP	42	192.168.71.28 is at a8:41:f4:c6:61:18
177	49.760155	192.168.71.28	192.168.71.227	ICMP	74	Echo (ping) request id=0x0001, seq=1/256, ttl=128 (reply in
178	49.772094	192.168.71.227	192.168.71.28	ICMP	74	Echo (ping) reply id=0x0001, seq=1/256, ttl=64 (request in
179	50.764733	192.168.71.28	192.168.71.227	ICMP	74	Echo (ping) request id=0x0001, seq=2/512, ttl=128 (reply in
180	50.925876	192.168.71.227	192.168.71.28	ICMP	74	Echo (ping) reply id=0x0001, seq=2/512, ttl=64 (request in
181	51.782936	192.168.71.28	192.168.71.227	ICMP	74	Echo (ping) request id=0x0001, seq=3/768, ttl=128 (reply in
182	51.848067	192.168.71.227	192.168.71.28	ICMP	74	Echo (ping) reply id=0x0001, seq=3/768, ttl=64 (request in
215	52.793041	192.168.71.28	192.168.71.227	ICMP	74	Echo (ping) request id=0x0001, seq=4/1024, ttl=128 (reply in
217	52.807099	192.168.71.227	192.168.71.28	ICMP	74	Echo (ping) reply id=0x0001, seq=4/1024, ttl=64 (request in
361	90.854325	aa:f6:2a:90:9d:94	a8:41:f4:c6:61:18	ARP	42	Who has 192.168.71.28? Tell 192.168.71.227
362	90.854351	a8:41:f4:c6:61:18	aa:f6:2a:90:9d:94	ARP	42	192.168.71.28 is at a8:41:f4:c6:61:18
389	121.078610	aa:f6:2a:90:9d:94	a8:41:f4:c6:61:18	ARP	42	Who has 192.168.71.28? Tell 192.168.71.227

> Frame 177: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)	0000	aa f6 2a 90 9d 94	a8 41 f4 c6 61 18 08 00 45 00	..*...A..a..
> Ethernet II, Src: a8:41:f4:c6:61:18 (a8:41:f4:c6:61:18), Dst: aa:f6:2a:90:9d:94 (aa:f6:2a:90:9d:94)	0010	00 3c a7 0e 00 00 80 01	83 62 c0 a8 47 1c c0 a8	<.....b.G.
> Internet Protocol Version 4, Src: 192.168.71.28, Dst: 192.168.71.227	0020	47 e3 08 00 4d 5a 00 01	00 01 61 62 63 64 65 66	G...MZ...abcd
> Internet Control Message Protocol	0030	67 68 69 6a 6b 6c 6d 6e	6f 70 71 72 73 74 75 76	ghijklmn opqrst
	0040	77 61 62 63 64 65 66 67	68 69	wabdefgh i

- * Les octets de position **0x0C** et **0x0D** ligne **0000** signifient que l'**en-tête Ethernet** transporte un paquet **IPv4**.
- * L'octet de position **0x07** ligne **0010** signifie que l'**en-tête IP** transporte le **protocole ICMP**.
- * La longueur de la trame est de **74 octets**.
- * La longueur du paquet IP est de **20 octets**.
- * La longueur du message ICMP est de **40 octets**.
- * L'octet de position **0x02** ligne **00020** signifie que le protocole ICMP transporte un message de type **echo ping request**.
- * Les octets à partir de l'octet **0x0A**, ligne **00020** sont les **données transportées**.

→ On sélectionne une trame **ICMP Echo Reply** :

The screenshot shows a Wireshark capture of network traffic. The main pane displays a list of packets. Packet 177 is selected, showing it is an ICMP Echo (ping) reply from 192.168.71.227 to 192.168.71.28. The details pane for this packet shows the following information:

- Internet Protocol Version 4, Src: 192.168.71.227, Dst: 192.168.71.28
- Internet Control Message Protocol
 - Type: 0 (Echo (ping) reply)
 - Code: 0
 - Checksum: 0x555a [correct] [Checksum Status: Good]
 - Identifier (BE): 1 (0x0001)
 - Identifier (LE): 256 (0x0100)
 - Sequence Number (BE): 1 (0x0001)
 - Sequence Number (LE): 256 (0x0100)
 - [Request frame: 177]
 - [Response time: 11,939 ms]
 - Data (32 bytes)
 - Data: 6162636465666768696a6b6c6d6e6f7071727374757677616263646566676869

The packet bytes pane shows the raw data in hexadecimal and ASCII:

```

0000 a8 41 f4 c6 61 18 aa f6 2a 90 9d 94 08 00 45 00  .A.a...*....
0010 00 3c e2 7d 00 00 40 01 87 f3 c0 a8 47 e3 c0 a8  <.}.@...G.
0020 47 1c 00 00 55 5a 00 01 00 01 61 62 63 64 65 66  G..UZ...abcd
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76  ghijklmn oparst
0040 77 61 62 63 64 65 66 67 68 69  wabdefgh i
  
```

- * L'octet de position **0x02** ligne **00020** renseigne le **type de message** transporté par le protocole ICMP, il vaut ici **00** qui correspond à un message **echo ping reply**.

1.2. Capture de trames ARP, DNS et ICMP

→ On démarre une nouvelle **capture de trames** Wireshark depuis la machine physique :

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	VMware_2a:77:0a	Broadcast	ARP	60	Who has 172.17.246.250? Tell 172.17.245.250
2	0.209698	172.17.106.2	224.0.0.18	VRRP	70	Announcement (v2)
3	1.026531	VMware_2a:77:0a	Broadcast	ARP	60	Who has 172.17.246.250? Tell 172.17.245.250
4	1.190526	VMware_6c:9c:3e	Broadcast	ARP	60	Who has 128.0.255.0? Tell 128.0.3.1
5	1.236573	172.17.106.2	224.0.0.18	VRRP	70	Announcement (v2)
6	1.865164	VMware_6c:9c:3e	Broadcast	ARP	60	Who has 128.0.255.0? Tell 128.0.3.1
7	2.050522	VMware_2a:77:0a	Broadcast	ARP	60	Who has 172.17.246.250? Tell 172.17.245.250
8	2.227248	172.17.2.15	224.0.0.251	MDNS	85	Standard query 0x0000 PTR _microsoft_mcc_tcp.local, "QU" question
9	2.227707	fe80::7606:96f4:c2c...	ff02::fb	MDNS	105	Standard query 0x0000 PTR _microsoft_mcc_tcp.local, "QU" question
10	2.275540	172.17.106.2	224.0.0.18	VRRP	70	Announcement (v2)
11	2.865125	VMware_6c:9c:3e	Broadcast	ARP	60	Who has 128.0.255.0? Tell 128.0.3.1
12	3.074596	VMware_2a:77:0a	Broadcast	ARP	60	Who has 172.17.246.250? Tell 172.17.245.250

→ On vide le **cache ARP** avec la commande **arp -d *** en ouvrant l'invite de commande en tant qu'**administrateur** :

```

Administrateur : Invite de commandes
Microsoft Windows [version 10.0.22631.2715]
(c) Microsoft Corporation. Tous droits réservés.

C:\Windows\System32>arp -d *

```

→ On **ping** le serveur web **www.ac-nice.fr** :

```

C:\Windows\System32>ping www.ac-nice.fr

Envoi d'une requête 'ping' sur cs234.wpc.alphacdn.net [93.184.221.161] avec 32 octets de données :
Réponse de 93.184.221.161 : octets=32 temps=32 ms TTL=56
Réponse de 93.184.221.161 : octets=32 temps=32 ms TTL=56
Réponse de 93.184.221.161 : octets=32 temps=32 ms TTL=56
Réponse de 93.184.221.161 : octets=32 temps=31 ms TTL=56

Statistiques Ping pour 93.184.221.161:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 31ms, Maximum = 32ms, Moyenne = 31ms

```

→ On arrête la capture et on la **sauvegarde** sous le nom "CaptureIcmpDns" :

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Vmware_6c:9c:3e	Broadcast	ARP	60	Who has 128.0.255.0? Tell 128.0.3.1
3	0.685066	Vmware_2a:77:0a	Broadcast	ARP	60	Who has 172.17.246.250? Tell 172.17.245.250
4	0.844141	Giga-Byt_2f:9c:f0	Broadcast	ARP	42	Who has 172.17.250.2? Tell 172.17.2.21
5	0.844299	Cisco_97:2c:56	Giga-Byt_2f:9c:f0	ARP	60	172.17.250.2 is at 00:1f:ca:97:2c:56
6	0.844309	172.17.2.21	93.184.221.161	ICMP	74	Echo (ping) request id=0x0001, seq=17/4352, ttl=128 (repl...
7	0.901612	93.184.221.161	172.17.2.21	ICMP	74	Echo (ping) reply id=0x0001, seq=17/4352, ttl=56 (reque...
8	1.000109	Vmware_6c:9c:3e	Broadcast	ARP	60	Who has 128.0.255.0? Tell 128.0.3.1
10	1.700594	Vmware_2a:77:0a	Broadcast	ARP	60	Who has 172.17.246.250? Tell 172.17.245.250
11	1.848697	172.17.2.21	93.184.221.161	ICMP	74	Echo (ping) request id=0x0001, seq=18/4608, ttl=128 (repl...
12	1.905674	93.184.221.161	172.17.2.21	ICMP	74	Echo (ping) reply id=0x0001, seq=18/4608, ttl=56 (reque...
16	2.724617	Vmware_2a:77:0a	Broadcast	ARP	60	Who has 172.17.246.250? Tell 172.17.245.250
17	2.854261	172.17.2.21	93.184.221.161	ICMP	74	Echo (ping) request id=0x0001, seq=19/4864, ttl=128 (repl...
18	2.907908	93.184.221.161	172.17.2.21	ICMP	74	Echo (ping) reply id=0x0001, seq=19/4864, ttl=56 (reque...
21	3.748611	Vmware_2a:77:0a	Broadcast	ARP	60	Who has 172.17.246.250? Tell 172.17.245.250

> Frame 4: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on
 > Ethernet II, Src: Giga-Byt_2f:9c:f0 (74:56:3c:2f:9c:f0), Dst: Broadca
 > Address Resolution Protocol (request)

```

0000  ff ff ff ff ff ff 74 56 3c 2f 9c f0 08 06 00 01  ....tV </...
0010  08 00 06 04 00 01 74 56 3c 2f 9c f0 ac 11 02 15  ....tV </...
0020  00 00 00 00 00 00 ac 11 fa 02  ....
  
```

* L'adresse MAC recherchée est celle de l'adresse IP **172.17.250.2**.

Trame ARP request
@MAC destination = FF:FF:FF:FF:FF:FF
@MAC source = 74:56:3C:2F:9C:F0
Ethernet Type = 08 06
Opcode (valeurs hexa.) = 00 01
@MAC de la cible = 00:00:00:00:00:00
@IP de la cible = 172.17.250.2

* On trouve une requête DNS avant l'échange de trames ICMP suite à l'exécution de la commande ping car le serveur ROI demande d'abord quelle est l'**adresse IP** du nom de domaine pour pouvoir envoyer le ping à cette adresse.

→ On consulte le **cache DNS** avec la commande **ipconfig /displaydns** et on vérifie que le nom de domaine **ac-nice.fr** est bien enregistré :

```

www.ac-nice.fr
-----
Nom d'enregistrement. : www.ac-nice.fr
Type d'enregistrement : 5
Durée de vie . . . . : 2023
Longueur de données : 8
Section . . . . . : Réponse
Enregistrement CNAME : cs234.wpc.alphacdn.net

```

→ On démarre une capture de trame et on **ping** à nouveau le serveur web **www.ac-nice.fr** :

No.	Time	Source	Destination	Protocol	Length	Info
2	0.195530	VMware_2a:77:0a	Broadcast	ARP	60	Who has 172.17.246.250? Tell 172.17.245.250
3	0.398825	172.17.2.21	93.184.221.161	ICMP	74	Echo (ping) request id=0x0001, seq=21/5376, ttl=128 (reply in 4)
4	0.430407	93.184.221.161	172.17.2.21	ICMP	74	Echo (ping) reply id=0x0001, seq=21/5376, ttl=56 (request in 3)
6	1.219170	VMware_2a:77:0a	Broadcast	ARP	60	Who has 172.17.246.250? Tell 172.17.245.250
7	1.414816	172.17.2.21	93.184.221.161	ICMP	74	Echo (ping) request id=0x0001, seq=22/5632, ttl=128 (reply in 8)
8	1.446575	93.184.221.161	172.17.2.21	ICMP	74	Echo (ping) reply id=0x0001, seq=22/5632, ttl=56 (request in 7)
11	2.338817	Cisco_97:2c:56	IntelCor_67:c8:02	ARP	60	Who has 172.17.1.2? Tell 172.17.250.2
12	2.418108	172.17.2.21	93.184.221.161	ICMP	74	Echo (ping) request id=0x0001, seq=23/5888, ttl=128 (reply in 13)
13	2.449698	93.184.221.161	172.17.2.21	ICMP	74	Echo (ping) reply id=0x0001, seq=23/5888, ttl=56 (request in 12)
14	2.889890	VMware_2f:86:78	Broadcast	ARP	60	Who has 172.17.2.1? Tell 172.17.245.20
17	3.426523	172.17.2.21	93.184.221.161	ICMP	74	Echo (ping) request id=0x0001, seq=24/6144, ttl=128 (reply in 18)
18	3.458400	93.184.221.161	172.17.2.21	ICMP	74	Echo (ping) reply id=0x0001, seq=24/6144, ttl=56 (request in 17)
20	3.675536	VMware_2f:86:78	Broadcast	ARP	60	Who has 172.17.2.1? Tell 172.17.245.20
24	4.338184	Cisco_97:2c:56	Broadcast	ARP	60	Who has 172.17.1.2? Tell 172.17.250.2

* On n'observe aucune **requête DNS** car ce nom de domaine est déjà enregistré dans le **cache DNS**.

→ On vide le **cache DNS** avec la commande **ipconfig /flushdns** et on redémarre une capture pour observer une **requête DNS** :

```

C:\Windows\system32>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

```


No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.16	192.168.1.254	DNS	74	Standard query 0xdd5a A www.ac-nice.fr
2	0.027697	192.168.1.254	192.168.1.16	DNS	126	Standard query response 0xdd5a A www.ac-nice.fr CNAME cs234.wpc.alphacdn.net A 93.184.221.161

* Les **différents protocoles** encapsulés dans une trame DNS sont :

- Le protocole **Ethernet**
- Le protocole **IP**
- Le protocole **UDP**
- Le protocole **DNS**

* Le destinataire de la requête DNS est le **serveur DNS** de la box. Son IP est **192.168.1.254**.

```
DNS Servers . . . . . : 192.168.1.254
```

* Les octets de position **0x0C**, **0x0D** ligne **0000** signifient que l'**en-tête Ethernet** transporte un **paquet IPv4**.

* L'octet de position **0x07** ligne **0010** signifie que l'**en-tête IP** transporte un **datagramme UDP**.

* Les octets de position **0x04** et **0x05** ligne **0020** signifient que le **port de destination** est **53**.

→ On développe la section **Domain Name System (query)** et plus précisément la rubrique **Queries** :

```

▶ Frame 1: 74 bytes on wire (592 bits), 74 bytes 0000 b0 bb e5 11 d5 45 d8 3b bf b7 eb 84 08 00 45 00 .....E; .....E
▶ Ethernet II, Src: Intel_b7:eb:84 (d8:3b:bf:b7: 0010 00 3c a9 16 00 00 80 11 00 00 c0 a8 01 10 c0 a8 <.....
▶ Internet Protocol Version 4, Src: 192.168.1.16 0020 01 fe db e5 00 35 00 28 84 98 dd 5a 01 00 00 01 .....5.(...Z....
▶ User Datagram Protocol, Src Port: 56293, Dst P 0030 00 00 00 00 00 00 03 77 77 77 07 61 63 2d 6e 69 .....w ww.ac-ni
▼ Domain Name System (query) 0040 63 65 02 66 72 00 00 01 00 01 ce.fr.....
  Transaction ID: 0xdd5a
  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 In: 2]

```

* Les valeurs hexadécimales des octets correspondant au nom de domaine internet ac nice.fr sont **03 77 77 77 07 61 63 2d 6e 69 63 65 02 66 72 00 00 01 00 01**.

→ On sélectionne la trame comportant la réponse à la **requête DNS** et on développe la section **Domain Name System (response)**, plus particulièrement la rubrique **Answers** :

```
dns
No.    Time           Source            Destination       Protocol Length Info
--
14 3.417036      192.168.1.16     192.168.1.254    DNS              74 Standard query 0xb99f A www.ac-nice.fr
15 3.429880      192.168.1.254    192.168.1.16     DNS              126 Standard query response 0xb99f A www.ac-nice.fr CNAME cs234.wpc.alphacdn.net A 93.184.221.161

    Frame 15: 126 bytes on wire (1008 bits), 126 bytes captured (1008 bits) on interface \Device\NPF_{8CA11E60-E3BC-4988-A549-8FD409613739}, id 0
    Ethernet II, Src: SagemcomBroa_11:d5:45 (b0:bb:e5:11:d5:45), Dst: Intel_b7:eb:84 (d8:3b:bf:b7:eb:84)
    Internet Protocol Version 4, Src: 192.168.1.254, Dst: 192.168.1.16
    User Datagram Protocol, Src Port: 53, Dst Port: 57335
    Domain Name System (response)
      Transaction ID: 0xb99f
      Flags: 0x8180 Standard query response, No error
      Questions: 1
      Answer RRs: 2
      Authority RRs: 0
      Additional RRs: 0
      Queries
    Answers
      www.ac-nice.fr: type CNAME, class IN, cname cs234.wpc.alphacdn.net
      cs234.wpc.alphacdn.net: type A, class IN, addr 93.184.221.161
    [Request In: 14]
    [Time: 0.012844000 seconds]
```

* Les valeurs hexadécimales et décimales de l'adresse IP du serveur web hébergeant le site de l'académie de Nice sont : **5D:B8:DD:A1 / 93.184.221.161**.

2. Commande Tracert et capture de trames ICMP

→ On démarre une nouvelle **capture de trame** Wireshark sur la machine physique :

The screenshot shows the Wireshark interface with a capture filter applied. The packet list pane displays the following data:

No.	Time	Source	Destination	Protocol	Length	Info
30	6.041718	192.168.1.16	192.168.1.123	TCP	54	54636 → 8009 [ACK] Seq=221 Ack=221 Win=1020 Len=0
31	6.418425	192.168.1.254	224.0.0.1	IGMPv2	52	Membership Query, general
32	6.442190	192.168.1.16	142.250.200.206	UDP	1285	62884 → 443 Len=1243
33	6.442269	192.168.1.16	142.250.200.206	UDP	1292	62884 → 443 Len=1250
34	6.442287	192.168.1.16	142.250.200.206	UDP	848	62884 → 443 Len=806
35	6.449903	142.250.200.206	192.168.1.16	UDP	70	443 → 62884 Len=28
36	6.451922	192.168.1.16	142.250.200.206	UDP	75	62884 → 443 Len=33
37	6.478939	142.250.200.206	192.168.1.16	UDP	67	443 → 62884 Len=25
38	6.494880	142.250.200.206	192.168.1.16	UDP	1287	443 → 62884 Len=1245
39	6.494880	142.250.200.206	192.168.1.16	UDP	795	443 → 62884 Len=753
40	6.495865	142.250.200.206	192.168.1.16	UDP	235	443 → 62884 Len=193
41	6.498959	192.168.1.16	142.250.200.206	UDP	79	62884 → 443 Len=37
42	6.530230	142.250.200.206	192.168.1.16	UDP	67	443 → 62884 Len=25
43	6.655322	192.168.1.16	224.0.0.251	IGMPv2	46	Membership Report group 224.0.0.251
44	6.655402	192.168.1.16	224.0.0.253	IGMPv2	46	Membership Report group 224.0.0.253
45	7.544436	192.168.1.16	192.168.1.98	TCP	164	54635 → 8009 [PSH, ACK] Seq=111 Ack=111 Win=1024 Len=110
46	7.544447	192.168.1.16	192.168.1.98	TCP	164	54832 → 8009 [PSH, ACK] Seq=111 Ack=111 Win=1021 Len=110
47	7.547512	192.168.1.98	192.168.1.16	TCP	164	8009 → 54635 [PSH, ACK] Seq=111 Ack=221 Win=491 Len=110
48	7.547512	192.168.1.98	192.168.1.16	TCP	164	8009 → 54832 [PSH, ACK] Seq=111 Ack=221 Win=388 Len=110
49	7.592354	192.168.1.16	192.168.1.98	TCP	54	54635 → 8009 [ACK] Seq=221 Ack=221 Win=1024 Len=0
50	7.593126	192.168.1.16	192.168.1.98	TCP	54	54832 → 8009 [ACK] Seq=221 Ack=221 Win=1021 Len=0
51	7.958881	192.168.1.16	192.168.1.123	TCP	164	54833 → 8009 [PSH, ACK] Seq=111 Ack=111 Win=1023 Len=110
52	7.964425	192.168.1.123	192.168.1.16	TCP	164	8009 → 54833 [PSH, ACK] Seq=111 Ack=221 Win=411 Len=110
53	8.006240	192.168.1.16	192.168.1.123	TCP	54	54833 → 8009 [ACK] Seq=221 Ack=221 Win=1023 Len=0

The packet details pane shows the following structure for the selected frame:

- Frame 1: 90 bytes on wire (720 bits), 0000 b0 bb e5 11 d5 45 d8 3b bf b7 eb 84 08 00 45 00
- Ethernet II, Src: Intel_b7:eb:84 (d8:00:10:0c:ca:02), Dst: Intel_00:10:00:00:00:00 (00:10:00:00:00:00)
- Internet Protocol Version 4, Src: 192.168.1.16, Dst: 192.168.1.123 (0020:03:ff:b7:33:00:00:00)
- Transmission Control Protocol, Src Port: 54833, Dst Port: 8009 (0000:00:20:31:f4:95:53:b6:73)
- Data (36 bytes) (0040:ef:a5:9a:eb:38:34:86:63:25:25:94:b6:4a:84:8d:01:0050:f6:4f:b9:c9:c6:eb:d7:7f:56:eb)

→ On lance la commande **tracert www.ac-nice.fr** dans l'invite de commande :

```
C:\Windows\system32>tracert www.ac-nice.fr

Tracing route to cs234.wpc.alphacdn.net [93.184.221.161]
over a maximum of 30 hops:

  0  0 ms  0 ms  0 ms  bbox.lan [192.168.1.254]
  1  1778 ms  1664 ms  1724 ms  31-33-160-2.abo.bbox.fr [31.33.160.2]
  2  *  *  *  Request timed out.
  3  *  *  *  Request timed out.
  4  16 ms  16 ms  15 ms  be21.cbr01-poi.net.bbox.fr [212.194.170.74]
  5  17 ms  15 ms  15 ms  212.194.171.9
  6  15 ms  16 ms  15 ms  be5.cbr01-cro.net.bbox.fr [212.194.171.141]
  7  *  *  16 ms  62.34.2.88
  8  16 ms  16 ms  16 ms  ae-130.border1.pam.edgecastcdn.net [152.195.108.200]
  9  21 ms  16 ms  17 ms  ae-65.core1.paa.edgecastcdn.net [152.195.108.129]
 10  16 ms  15 ms  15 ms  93.184.221.161
 11

Trace complete.
```

→ On arrête la capture et la **sauvegarde** sous le nom de "CaptureTracert" puis on applique un **filtre ICMP** :

No.	Time	Source	Destination	Protocol	Length	Info
6	0.634065	192.168.1.16	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=30/7680, ttl=1 (no response found!)
7	0.636413	192.168.1.254	192.168.1.16	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
8	0.636775	192.168.1.16	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=31/7936, ttl=1 (no response found!)
9	0.637854	192.168.1.254	192.168.1.16	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
10	0.638156	192.168.1.16	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=32/8192, ttl=1 (no response found!)
11	0.639752	192.168.1.254	192.168.1.16	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
19257	6.211423	192.168.1.16	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=33/8448, ttl=2 (no response found!)
19277	7.990120	31.33.160.2	192.168.1.16	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
19278	7.990817	192.168.1.16	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=34/8704, ttl=2 (no response found!)
19281	9.655281	31.33.160.2	192.168.1.16	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
19282	9.655887	192.168.1.16	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=35/8960, ttl=2 (no response found!)
19291	11.379827	31.33.160.2	192.168.1.16	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
19292	11.381539	192.168.1.16	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=36/9216, ttl=3 (no response found!)
19410	15.372706	192.168.1.16	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=37/9472, ttl=3 (no response found!)
19562	19.374868	192.168.1.16	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=38/9728, ttl=3 (no response found!)
19597	23.381679	192.168.1.16	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=39/9984, ttl=4 (no response found!)
41984	27.382973	192.168.1.16	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=40/10240, ttl=4 (no response found!)
41991	31.377403	192.168.1.16	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=41/10496, ttl=4 (no response found!)
42008	35.375326	192.168.1.16	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=42/10752, ttl=5 (no response found!)
42013	35.391852	212.194.170.74	192.168.1.16	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)
42014	35.392155	192.168.1.16	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=43/11008, ttl=5 (no response found!)
42015	35.408628	212.194.170.74	192.168.1.16	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)
42016	35.408889	192.168.1.16	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=44/11264, ttl=5 (no response found!)
42017	35.424150	212.194.170.74	192.168.1.16	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)

→ On développe l'en-tête IP de la première trame **ICMP Echo request** :

No.	Time	Source	Destination	Protocol	Length	Info
6	0.634065	192.168.1.16	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=30/7680, ttl=1 (no response found!)
7	0.636413	192.168.1.254	192.168.1.16	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
8	0.636775	192.168.1.16	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=31/7936, ttl=1 (no response found!)
9	0.637854	192.168.1.254	192.168.1.16	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
10	0.638156	192.168.1.16	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=32/8192, ttl=1 (no response found!)

Frame 6: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface 0	0000	b0 bb e5 11 d5 45 d8 3b bf b7 eb 84 08 00 45 00 E ; E
Ethernet II, Src: Intel b7:eb:84 (d8:3b:bf:b7:eb), Dst: 93.184.221.161	0010	00 5c 9e a1 00 00 01 01 00 00 c0 a8 01 10 5d b8]
Internet Protocol Version 4, Src: 192.168.1.16, Dst: 93.184.221.161	0020	dd a1 08 00 f7 e0 00 01 00 1e 00 00 00 00 00 00]
Version: 4	0030	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00]
Header Length: 20 bytes (5)	0040	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00]
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not Set)	0050	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00]
Total Length: 92	0060	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00]
Identification: 0x9eal (40609)			
Flags: 0x0			
Fragment Offset: 0			
Time to Live: 1			
Protocol: ICMP (1)			
Header Checksum: 0x0000 [validation disabled] [Header checksum status: Unverified]			
Source Address: 192.168.1.16			
Destination Address: 93.184.221.161			
Stream index: 2			

* L'adresse IP destination est **93.184.221.161 / 5d b8 dd a1**.

* La valeur portée par le champ TTL est **1 / 01**.

* La valeur portée par le champ Type dans la section message ICMP est **8 / 08**.

* La valeur portée par le champ Type dans la section message ICMP de la première trame comportant le message d'erreur ICMP Time-to-live exceeded est aussi **8 / 08**.