

TP 5 : TRAMES ARP, ICMP ET DNS

Sommaire : COMPTE RENDU

4.1 Capture de trames ARP et ICMP.

4.2 Capture de trames ARP, DNS et ICMP.

4.3 Commande Tracert et capture de trames ICMP.

4.1 Capture de trames ARP et ICMP

Capture des trames **ICMP** par la saisie d'une commande ping depuis votre **machine physique**.

→ J'ai ouvert Wireshark, en sélectionnant ma carte réseau et j'ai démarré une capture de trames.

→ J'ai ensuite ping mon routeur :

```
C:\Windows\System32> ping 192.168.1.1

Envoi d'une requête 'Ping' 192.168.1.1 avec 32 octets de données :
Réponse de 192.168.1.1 : octets=32 temps=8 ms TTL=64
Réponse de 192.168.1.1 : octets=32 temps=13 ms TTL=64
Réponse de 192.168.1.1 : octets=32 temps=7 ms TTL=64
Réponse de 192.168.1.1 : octets=32 temps=7 ms TTL=64

Statistiques Ping pour 192.168.1.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 7ms, Maximum = 13ms, Moyenne = 8ms

C:\Windows\System32>
```

→ L'échange démarre avec une requête et une réponse ARP pour l'adresse MAC du serveur. Ensuite l'échange de trames ICMP a lieu. J'ai arrêté la capture car les 8 trames ICMP sont obtenues :

No.	Time	Source	Destination	Protocol	Length	Info
488	102.124433	CloudNet_4e:23:4f	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.20
489	102.192986	Arcadyan_45:de:86	CloudNet_4e:23:4f	ARP	60	192.168.1.1 is at 4c:22:f3:45:de:86
820	181.528554	192.168.1.20	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=37/9472, ttl=128 (reply in 821)
821	181.536769	192.168.1.1	192.168.1.20	ICMP	74	Echo (ping) reply id=0x0001, seq=37/9472, ttl=64 (request in 820)
822	182.539545	192.168.1.20	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=38/9728, ttl=128 (reply in 823)
823	182.552619	192.168.1.1	192.168.1.20	ICMP	74	Echo (ping) reply id=0x0001, seq=38/9728, ttl=64 (request in 822)
824	183.547616	192.168.1.20	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=39/9984, ttl=128 (reply in 825)
825	183.554798	192.168.1.1	192.168.1.20	ICMP	74	Echo (ping) reply id=0x0001, seq=39/9984, ttl=64 (request in 824)
826	184.556602	192.168.1.20	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=40/10240, ttl=128 (reply in 827)
827	184.563810	192.168.1.1	192.168.1.20	ICMP	74	Echo (ping) reply id=0x0001, seq=40/10240, ttl=64 (request in 826)
884	218.622875	Arcadyan_45:de:86	Broadcast	ARP	60	Who has 192.168.1.18? Tell 192.168.1.1
890	222.821487	Arcadyan_45:de:86	Broadcast	ARP	60	Who has 192.168.1.18? Tell 192.168.1.1
897	227.873731	Arcadyan_45:de:86	Broadcast	ARP	60	Who has 192.168.1.18? Tell 192.168.1.1
904	232.651525	Arcadyan_45:de:86	Broadcast	ARP	60	Who has 192.168.1.18? Tell 192.168.1.1
906	233.877094	Arcadyan_45:de:86	Broadcast	ARP	60	Who has 192.168.1.18? Tell 192.168.1.1

> Frame 488: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0	0000	ff ff ff ff ff 10 6f d9 4e 23 4f 08 06 00 01	o..N#0...
> Ethernet II, Src: CloudNet_4e:23:4f (10:6f:d9:4e:23:4f), Dst: Broadcast (ff:ff:ff:ff:ff:ff)	0010	08 00 06 04 00 01 10 6f d9 4e 23 4f c0 a8 01 14	o..N#0....
> Address Resolution Protocol (request)	0020	00 00 00 00 00 00 c0 a8 01 01	

➔ Après la saisie de la commande ping, j'ai consulté le contenu du cache ARP et vérifié la présence de l'association @IP-@MAC correspondant à mon routeur.

Interface : 192.168.56.1 --- 0x2		
Adresse Internet	Adresse physique	Type
224.0.0.2	01-00-5e-00-00-02	statique
224.0.0.22	01-00-5e-00-00-16	statique
224.0.0.251	01-00-5e-00-00-fb	statique
239.255.255.250	01-00-5e-7f-ff-fa	statique
Interface : 192.168.1.20 --- 0x13		
Adresse Internet	Adresse physique	Type
192.168.1.1	4c-22-f3-45-de-86	dynamique
224.0.0.2	01-00-5e-00-00-02	statique
224.0.0.22	01-00-5e-00-00-16	statique
224.0.0.251	01-00-5e-00-00-fb	statique
224.0.0.252	01-00-5e-00-00-fc	statique
239.255.255.250	01-00-5e-7f-ff-fa	statique

Analyse l'échange de trames ARP précédant l'échange de trames ICMP :

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

Les octets de position 0x0C et 0x0D ligne 0000 ont pour signification le champ Ethertype (0806) qui correspond à ARP :

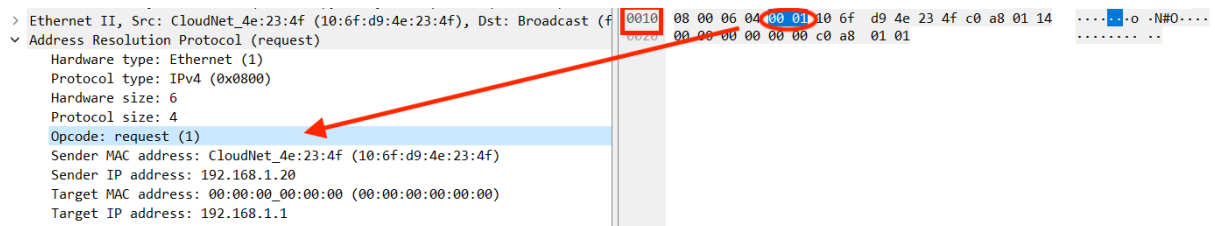
> Frame 488: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0	0000	ff ff ff ff ff 10 6f d9 4e 23 4f 08 06 00 01	o..N#0...
> Destination: Broadcast (ff:ff:ff:ff:ff:ff)	0010	08 00 06 04 00 01 10 6f d9 4e 23 4f c0 a8 01 14	o..N#0....
> Source: CloudNet_4e:23:4f (10:6f:d9:4e:23:4f)	0020	00 00 00 00 00 00 c0 a8 01 01	
> Type: ARP (0x0806)			
> Address Resolution Protocol (request)			

- Quelle est la fonction de la trame ARP Request ?

La fonction de la trame ARP REQUEST est d'envoyer en broadcast. Pour permettre de dire à qui correspond cette @IP. Son but est de recevoir l'adresse MAC de celle qui détient @IP.

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

La signification des octets position 0x04 et 0x05 ligne 0010 est l'Opcode, elle est pour but de demander l'adresse @MAC à partir d'une adresse IP (00 01).



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

La longueur d'un message ARP contenu dans la trame est de 28 octets.

Frame 488: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{D08B8059}	0000	ff ff ff ff ff ff 10 6f d9 4e 23 4f 08 06 00 01	o .NH0....
Ethernet II, Src: CloudNet_4e:23:4f (10:6f:d9:4e:23:4f), Dst: Broadcast (ff:ff:ff:ff:ff:ff)	0010	08 00 06 04 00 01 10 6f d9 4e 23 4f c0 a8 01 14	o .NH0....
Address Resolution Protocol (request)	0020	00 00 00 00 00 00 c0 a8 01 01	

- Quelle est la longueur de la trame ARP Request ?

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

Frame 488: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{D08B8059}	0000	ff ff ff ff ff ff 10 6f d9 4e 23 4f 08 06 00 01	o .NH0....
Ethernet II, Src: CloudNet_4e:23:4f (10:6f:d9:4e:23:4f), Dst: Broadcast (ff:ff:ff:ff:ff:ff)	0010	08 00 06 04 00 01 10 6f d9 4e 23 4f c0 a8 01 14	o .NH0....
Address Resolution Protocol (request)	0020	00 00 00 00 00 00 c0 a8 01 01	

- Quelle est la longueur de la trame ARP Reply ?

La longueur de la trame ARP Reply est de 42 octets.

Frame 489: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{D08B8059}	0000	10 6f d9 4e 23 4f 4c 22 f3 45 de 86 08 06 00 01	..o.NHOL" .E.....
Ethernet II, Src: Arcadyan_45:de:86 (4c:22:f3:45:de:86), Dst: CloudNet_4e:23:4f (10:6f:d9:4e:23:4f)	0010	08 00 06 04 00 02 4c 22 f3 45 de 86 c0 a8 01 01	L" .E.....
Address Resolution Protocol (reply)	0020	10 6f d9 4e 23 4f c0 a8 01 14 00 00 00 00 00 00	..o.NH0... ..
Hardware type: Ethernet (1)	0030	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	

- Combien d'octets sont utilisés pour le padding ?

Aucune padding utilisé. (0000000000000000...)

->

Trame ARP request
@MAC destination = ff : ff : ff : ff : ff : ff
@MAC source = 10 6f d9 4e 23 4f
Ethernet Type = 00 01
Opcode (valeurs hexa.) = 00 01
@MAC de la cible = 00 : 00 : 00 : 00 : 00 : 00
@IP de la cible = 192.168.1.1

J'ai sélectionné une trame ICMP Echo Request.

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

La signification de ces octets de position se reposent au champ Ethertype 08 00 qui correspond à l'IPv4.

> Frame 820: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on in	0000	4c 22 f3 45 de 86 10 6f d9 4e 23 4f 08 00 45 00	L"-E...o .N#O..E-
> Ethernet II, Src: CloudNet_4e:23:4f (10:6f:d9:4e:23:4f), Dst: Arcadyan_45:	0010	00 3c ec 6c 00 00 80 01 ca ee c0 a8 01 14 c0 a8	<..1.... ..
> Destination: Arcadyan_45:de:86 (4c:22:f3:45:de:86)	0020	01 01 08 00 4d 36 00 01 00 25 61 62 63 64 65 66	M6.. .%abcdef
> Source: CloudNet_4e:23:4f (10:6f:d9:4e:23:4f)	0030	67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76	ghijklmn opqrstuv
Type: IPv4 (0x0800)	0040	77 61 62 63 64 65 66 67 68 69	wabcedfg hi

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

La signification a l'octet de position 0x07 ligne 0010 se reposent au protocole utiliser ICMP (1).

> Frame 820: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on in	0000	4c 22 f3 45 de 86 10 6f d9 4e 23 4f 08 00 45 00	L"-E...o .N#O..E-
> Ethernet II, Src: CloudNet_4e:23:4f (10:6f:d9:4e:23:4f), Dst: Arcadyan_45:	0010	00 3c ec 6c 00 00 80 01 ca ee c0 a8 01 14 c0 a8	<..1.... ..
> Destination: Arcadyan_45:de:86 (4c:22:f3:45:de:86)	0020	01 01 08 00 4d 36 00 01 00 25 61 62 63 64 65 66	M6.. .%abcdef
> Source: CloudNet_4e:23:4f (10:6f:d9:4e:23:4f)	0030	67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76	ghijklmn opqrstuv
Type: IPv4 (0x0800)	0040	77 61 62 63 64 65 66 67 68 69	wabcedfg hi

> Frame 820: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{DD88B095}	0000	4c 22 f3 45 de 86 10 6f d9 4e 23 4f 08 00 45 00	L"-E...o .N#O..E-
> Ethernet II, Src: CloudNet_4e:23:4f (10:6f:d9:4e:23:4f), Dst: Arcadyan_45:de:86 (4c:22:f3:45:de:86)	0010	00 3c ec 6c 00 00 80 01 ca ee c0 a8 01 14 c0 a8	<..1.... ..
> Destination: Arcadyan_45:de:86 (4c:22:f3:45:de:86)	0020	01 01 08 00 4d 36 00 01 00 25 61 62 63 64 65 66	M6.. .%abcdef
> Source: CloudNet_4e:23:4f (10:6f:d9:4e:23:4f)	0030	67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76	ghijklmn opqrstuv
Type: IPv4 (0x0800)	0040	77 61 62 63 64 65 66 67 68 69	wabcedfg hi

- Quelle est la longueur de la trame ?

La longueur de la trame est de 74 octets.

> Frame 820: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{DD88B095}	0000	4c 22 f3 45 de 86 10 6f d9 4e 23 4f 08 00 45 00	L"-E...o .N#O..E-
> Ethernet II, Src: CloudNet_4e:23:4f (10:6f:d9:4e:23:4f), Dst: Arcadyan_45:de:86 (4c:22:f3:45:de:86)	0010	00 3c ec 6c 00 00 80 01 ca ee c0 a8 01 14 c0 a8	<..1.... ..
> Destination: Arcadyan_45:de:86 (4c:22:f3:45:de:86)	0020	01 01 08 00 4d 36 00 01 00 25 61 62 63 64 65 66	M6.. .%abcdef
> Source: CloudNet_4e:23:4f (10:6f:d9:4e:23:4f)	0030	67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76	ghijklmn opqrstuv
Type: IPv4 (0x0800)	0040	77 61 62 63 64 65 66 67 68 69	wabcedfg hi

- Quelle est la longueur du paquet IP ?

La longueur du paquet IP est de 20 octets.

> Frame 820: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on	0000	4c 22 f3 45 de 86 10 6f d9 4e 23 4f 08 00 45 00	L".E...o.N#O..E.
> Ethernet II, Src: CloudNet_4e:23:4f (10:6f:d9:4e:23:4f), Dst: Arcadyan_4	0010	00 3c ec 6c 00 00 80 01 ca ee c0 a8 01 14 c0 a8	<.l.....
> Internet Protocol Version 4, Src: 192.168.1.20, Dst: 192.168.1.1	0020	01 01 08 00 4d 36 00 01 00 25 61 62 63 64 65 66	..M6..%abcdef
0100 = Version: 4	0030	67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76	ghijklmn opqrstuv
.... 0101 = Header Length: 20 bytes (5)	0040	77 61 62 63 64 65 66 67 68 69	wabcdefg hi
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)			

- Quelle est la longueur du message ICMP ?

La longueur du message ICMP est de 40 octets.

> Frame 820: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on in	0000	4c 22 f3 45 de 86 10 6f d9 4e 23 4f 08 00 45 00	L".E...o.N#O..E.
> Ethernet II, Src: CloudNet_4e:23:4f (10:6f:d9:4e:23:4f), Dst: Arcadyan_45:	0010	00 3c ec 6c 00 00 80 01 ca ee c0 a8 01 14 c0 a8	<.l.....
> Internet Protocol Version 4, Src: 192.168.1.20, Dst: 192.168.1.1	0020	01 01 08 00 4d 36 00 01 00 25 61 62 63 64 65 66	..M6..%abcdef
> Internet Control Message Protocol	0030	67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76	ghijklmn opqrstuv
	0040	77 61 62 63 64 65 66 67 68 69	wabcdefg hi

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

La signification de l'octet de position 0x02 ligne 0020 correspond au type de message.

> Frame 820: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on in	0000	4c 22 f3 45 de 86 10 6f d9 4e 23 4f 08 00 45 00	L".E...o.N#O..E.
> Ethernet II, Src: CloudNet_4e:23:4f (10:6f:d9:4e:23:4f), Dst: Arcadyan_45:	0010	00 3c ec 6c 00 00 80 01 ca ee c0 a8 01 14 c0 a8	<.l.....
> Internet Protocol Version 4, Src: 192.168.1.20, Dst: 192.168.1.1	0020	01 01 08 00 4d 36 00 01 00 25 61 62 63 64 65 66	..M6..%abcdef
> Internet Control Message Protocol	0030	67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76	ghijklmn opqrstuv
Type: 8 (Echo (ping) request)	0040	77 61 62 63 64 65 66 67 68 69	wabcdefg hi
Code: 0			
Checksum: 0x4d36 [correct]			
[Checksum Status: Good]			

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

> Frame 820: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on in	0000	4c 22 f3 45 de 86 10 6f d9 4e 23 4f 08 00 45 00	L"-E...o..N#0..E.
> Ethernet II, Src: CloudNet_4e:23:4f (10:6f:d9:4e:23:4f), Dst: Arcadyan_45:	0010	00 3c cc 0c 00 00 80 01 ca ee c0 a8 01 14 c0 a8	<-1... ..%abcdef
> Internet Protocol Version 4, Src: 192.168.1.20, Dst: 192.168.1.1	0020	01 01 08 00 4d 36 00 01 00 25 61 62 63 64 65 66	...M6.. ..%abcdef
✓ Internet Control Message Protocol	0030	67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76	ghijklmn opqrstuv
Type: 8 (Echo (ping) request)	0040	77 61 62 63 64 65 66 67 68 69	wabcdefg hi
Code: 0			
Checksum: 0x4d36 [correct]			
[Checksum Status: Good]			
Identifier (BE): 1 (0x0001)			
Identifier (LE): 256 (0x0100)			
Sequence Number (BE): 37 (0x0025)			
Sequence Number (LE): 9472 (0x2500)			
[Response frame: 821]			
✓ Data (32 bytes)			
Data: 6162636465666768696a6b6c6d6e6f70717273747576776162636465666768			
[Length: 32]			

```
C:\Windows\System32> ping 192.168.1.1

Envoi d'une requête 'Ping' 192.168.1.1 avec 32 octets de données :
Réponse de 192.168.1.1 : octets=32 temps=8 ms TTL=64
Réponse de 192.168.1.1 : octets=32 temps=13 ms TTL=64
Réponse de 192.168.1.1 : octets=32 temps=7 ms TTL=64
Réponse de 192.168.1.1 : octets=32 temps=7 ms TTL=64

Statistiques Ping pour 192.168.1.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 7ms, Maximum = 13ms, Moyenne = 8ms

C:\Windows\System32>
```

Je remarque que les octets correspondent à la commande PING que l'on retrouve dans l'invite de commande.

Quelle est le nom et la valeur de l'octet de position 0x02 ligne 0020 ?

Le nom et la valeur de l'octet de position 0x02 ligne 0020 correspond au type de message (type (0)) pour ECHO ping Reply.

> Ethernet II, Src: CloudNet_4e:23:4f (10:6f:d9:4e:23:4f), Dst: Arcadyan_45:	0000	4c 22 f3 45 de 86 10 6f d9 4e 23 4f 08 00 45 00	L"-E...o..N#0..E.
> Internet Protocol Version 4, Src: 192.168.1.20, Dst: 192.168.1.1	0010	00 3c cc 0c 00 00 80 01 ca ee c0 a8 01 14 c0 a8	<-1... ..%abcdef
✓ Internet Control Message Protocol	0020	01 01 08 00 4d 36 00 01 00 25 61 62 63 64 65 66	...M6.. ..%abcdef
Type: 8 (Echo (ping) request)	0030	67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76	ghijklmn opqrstuv
	0040	77 61 62 63 64 65 66 67 68 69	wabcdefg hi

4.2 Capture de trames ARP, DNS et ICMP

→ Démarrez une capture de trames.

→ Ouvrir l'invite de commande, videz le cache ARP, puis effectuez la requête ping vers le serveur web www.ac-nice.fr :

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

Envoi d'une requête 'ping' sur ac-nice.fr [194.167.84.160] avec 32 octets de données :
Réponse de 194.167.84.160 : octets=32 temps=33 ms TTL=48
Réponse de 194.167.84.160 : octets=32 temps=34 ms TTL=48
Réponse de 194.167.84.160 : octets=32 temps=33 ms TTL=48
Réponse de 194.167.84.160 : octets=32 temps=33 ms TTL=48

Statistiques Ping pour 194.167.84.160:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 33ms, Maximum = 34ms, Moyenne = 33ms

C:\Windows\System32>
```

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

L'adresse MAC recherchée lors de la première trame ARP est l'adresse MAC de mon routeur 192.168.1.1.

No.	Time	Source	Destination	Protocol	Length	Info
15	8.674228	2a01:cb1d:7:8d00:cf...	2a01:cb1d:7:8d00:4e...	DNS	116	Standard query 0x27cc HTTPS functional.events.data.microsoft.com
19	8.696332	2a01:cb1d:7:8d00:4e...	2a01:cb1d:7:8d00:cf...	DNS	306	Standard query response 0xd220 AAAA functional.events.data.microsoft.com
20	8.696332	2a01:cb1d:7:8d00:4e...	2a01:cb1d:7:8d00:cf...	DNS	246	Standard query response 0x4049 A functional.events.data.microsoft.com
21	8.697028	2a01:cb1d:7:8d00:4e...	2a01:cb1d:7:8d00:cf...	DNS	306	Standard query response 0x27cc HTTPS functional.events.data.microsoft.com
58	20.244265	CloudNet_4e:23:4f	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.20
59	20.248243	Arcadyan_45:de:86	CloudNet_4e:23:4f	ARP	60	192.168.1.1 is at 4c:22:f3:45:de:86
96	55.036553	2a01:cb1d:7:8d00:cf...	2a01:cb1d:7:8d00:4e...	DNS	90	Standard query 0xb07b A ac-nice.fr
97	55.036909	2a01:cb1d:7:8d00:cf...	2a01:cb1d:7:8d00:4e...	DNS	90	Standard query 0x6ebc AAAA ac-nice.fr
98	55.079525	2a01:cb1d:7:8d00:4e...	2a01:cb1d:7:8d00:cf...	DNS	142	Standard query response 0x6ebc AAAA ac-nice.fr SOA svrs.ac-nice.fr
99	55.080385	2a01:cb1d:7:8d00:4e...	2a01:cb1d:7:8d00:cf...	DNS	106	Standard query response 0xb07b A ac-nice.fr A 194.167.84.160
100	55.093911	192.168.1.20	194.167.84.160	ICMP	74	Echo (ping) request id=0x0001, seq=41/10496, ttl=128 (reply in 101)
101	55.127531	194.167.84.160	192.168.1.20	ICMP	74	Echo (ping) reply id=0x0001, seq=41/10496, ttl=128 (request in 100)



Trame ARP request
@MAC destination = ff : ff : ff : ff : ff : ff
@MAC source = 10 6f d9 4e 23 4f
Ethernet Type = 00 01
Opcode (valeurs hexa.) = 00 0A
@MAC de la cible = 00 : 00 : 00 : 00 : 00 : 00
@IP de la cible = 192.168.1.1

> Frame 58: 42 bytes on wire (336 bits) 42 bytes captured (336 bits) on Interface \Device\NPF... (DD888059-92C...)	0000	ff ff ff ff ff ff 10 6f d9 4e 23 4f 00 00 00 01	0-HMO...
> Ethernet II, Src: CloudNet_4e:23:4f (10:6f:d9:4e:23:4f), Dst: Broadcast (ff:ff:ff:ff:ff:ff)	0010	00 00 06 04 00 01 10 6f d9 4e 23 4f c0 a8 01 14	0-HMO...
> Address Resolution Protocol (request)	0020	00 00 00 00 00 00 c0 a8 01 01	

- Pour quelle raison trouve-t-on ensuite une requête DNS avant l'exécution de la commande ping proprement dit ?

DNS (Domain Name System)

La raison pour laquelle suit une trame DNS est que pour effectuer correctement la commande PING il est nécessaire de posséder l'adresse @IP c'est là que le protocole DNS entre en jeux. Son travail est d'associer l'adresse de la page web a une adresse IP.

- ➔ J'ai consulté le **cache DNS** à l'aide de la commande **ipconfig /displaydns** et j'ai vérifié la présence de **l'enregistrement DNS** ac-nice.fr et de l'adresse IP associée.

```
C:\Windows\System32>ipconfig /displaydns

Configuration IP de Windows

ac-nice.fr
-----
Nom d'enregistrement. : ac-nice.fr
Type d'enregistrement : 1
Durée de vie . . . . : 21216
Longueur de données . : 4
Section . . . . . : Réponse
Enregistrement (hôte) : 194.167.84.160
```

- ➔ J'ai fait une nouvelle capture de trame. J'ai re saisi la commande **ping www.ac-nice.fr** dans l'invite de commandes.

- ➔ J'ai vidé le cache du DNS à l'aide de la commande `ipconfig /flushdns` et j'ai à nouveau fait une nouvelle capture de trame afin de visualiser de nouveau une requête DNS.

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

Envoi d'une requête 'ping' sur ac-nice.fr [194.167.84.160] avec 32 octets de données :
Réponse de 194.167.84.160 : octets=32 temps=33 ms TTL=48
Réponse de 194.167.84.160 : octets=32 temps=33 ms TTL=48
Réponse de 194.167.84.160 : octets=32 temps=33 ms TTL=48
Réponse de 194.167.84.160 : octets=32 temps=35 ms TTL=48

Statistiques Ping pour 194.167.84.160:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 33ms, Maximum = 35ms, Moyenne = 33ms

C:\Windows\System32> ipconfig /flushdns

Configuration IP de Windows

Cache de résolution DNS vidé.

C:\Windows\System32>
```

No.	Time	Source	Destination	Protocol	Length	Info
22	21.054235	2a01:cb1d:7:8d00:cf...	2a01:cb1d:7:8d00:4e...	DNS	90	Standard query 0x43a6 AAAA ac-nice.fr
23	21.056749	2a01:cb1d:7:8d00:4e...	2a01:cb1d:7:8d00:cf...	DNS	90	Standard query response 0x43a6 AAAA ac-nice.fr
24	21.064775	192.168.1.20	194.167.84.160	ICMP	74	Echo (ping) request id=0x0001, seq=57/14592, ttl=128 (reply in 25)
25	21.098679	194.167.84.160	192.168.1.20	ICMP	74	Echo (ping) reply id=0x0001, seq=57/14592, ttl=48 (request in 24)
26	22.085651	192.168.1.20	194.167.84.160	ICMP	74	Echo (ping) request id=0x0001, seq=58/14848, ttl=128 (reply in 27)
27	22.119051	194.167.84.160	192.168.1.20	ICMP	74	Echo (ping) reply id=0x0001, seq=58/14848, ttl=48 (request in 26)
28	23.101784	192.168.1.20	194.167.84.160	ICMP	74	Echo (ping) request id=0x0001, seq=59/15104, ttl=128 (reply in 29)
29	23.139687	194.167.84.160	192.168.1.20	ICMP	74	Echo (ping) reply id=0x0001, seq=59/15104, ttl=48 (request in 28)
30	24.117346	192.168.1.20	194.167.84.160	ICMP	74	Echo (ping) request id=0x0001, seq=60/15360, ttl=128 (reply in 31)
31	24.154545	194.167.84.160	192.168.1.20	ICMP	74	Echo (ping) reply id=0x0001, seq=60/15360, ttl=48 (request in 30)
113	48.698187	Apple_8c:0d:99	Broadcast	ARP	42	Who has 192.168.1.11? Tell 192.168.1.13
318	121.367745	192.168.1.20	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=61/15616, ttl=128 (reply in 319)
319	121.375905	192.168.1.1	192.168.1.20	ICMP	74	Echo (ping) reply id=0x0001, seq=61/15616, ttl=64 (request in 318)
320	122.378639	192.168.1.20	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=62/15872, ttl=128 (reply in 321)
321	122.382715	192.168.1.1	192.168.1.20	ICMP	74	Echo (ping) reply id=0x0001, seq=62/15872, ttl=64 (request in 320)
324	123.389355	192.168.1.20	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=63/16128, ttl=128 (reply in 325)
325	123.393236	192.168.1.1	192.168.1.20	ICMP	74	Echo (ping) reply id=0x0001, seq=63/16128, ttl=64 (request in 324)
327	124.406102	192.168.1.20	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=64/16384, ttl=128 (reply in 328)
328	124.410921	192.168.1.1	192.168.1.20	ICMP	74	Echo (ping) reply id=0x0001, seq=64/16384, ttl=64 (request in 327)

```
> Frame 22: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface \Device\NPF_{DD8B8059-92CA-4D00-A60D-36B61BEE4579}, id 0
> Ethernet II, Src: CloudNet_4e:23:4f (10:6f:d9:4e:23:4f), Dst: Arcadyan_45:de:86 (4c:22:f3:45:de:86)
> Internet Protocol Version 6, Src: 2a01:cb1d:7:8d00:cfe:13af:6baf:16a9, Dst: 2a01:cb1d:7:8d00:4e22:f3ff:fe45:de86
v User Datagram Protocol, Src Port: 61292, Dst Port: 53
  Source Port: 61292
  Destination Port: 53
```

- Quels sont les différents protocoles encapsulés dans une trame DNS ?

Les différents protocoles encapsulés dans une trame DNS est l'UDP, IP, Ethernet.

- Quelle est la machine destinataire de la requête DNS ?

La machine destinataire de la requête DNS est mon routeur 192.168.1.1

- Quelle est l'adresse IP de la machine destinataire de la requête DNS ?

L'adresse IP de la machine destinataire de la requête DNS est 192.168.1.1

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

La signification que les octets de position 0x0C, 0x0D ligne 0000 et 0x07 ligne 0010 est qu'ils correspondent au protocole UDP. Valeur 17 :

```
> Frame 227: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface \Device\NPF_{D08B8059-92CA-4D...
> Ethernet II, Src: CloudNet_4e:23:4f (10:6f:d9:4e:23:4f), Dst: Arcadyan_45:de:86 (4c:22:f3:45:de:86)
> Internet Protocol Version 6, Src: 2a01:cbid:7:8d00:cfe:13af:6baf:16a9, Dst: 2a01:cbid:7:8d00:4e22:f3ff:fe45:de8
0110 .... = Version: 6
> .... 0000 0000 .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
Payload Length: 36
Next Header: UDP (17)
```

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

La signification que les octets de position 0x04 et 0x05 ligne 0020 est qu'ils correspondent au port DNS de destination. Valeur 53 :

```
> Frame 227: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface \Device\NPF_{D08B8059-92CA-4D...
> Ethernet II, Src: CloudNet_4e:23:4f (10:6f:d9:4e:23:4f), Dst: Arcadyan_45:de:86 (4c:22:f3:45:de:86)
> Internet Protocol Version 6, Src: 2a01:cbid:7:8d00:cfe:13af:6baf:16a9, Dst: 2a01:cbid:7:8d00:4e22:f3ff:fe45:de8
> User Datagram Protocol, Src Port: 64304, Dst Port: 53
Source Port: 64304
Destination Port: 53
```

- Développez la section **Domain Name System (query)** et plus précisément la rubrique **Queries**. Quels sont les valeurs hexadécimales des octets correspondant au nom de domaine internet ac- nice.fr ?

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

arp or dns or icmp

No.	Time	Source	Destination	Protocol	Length	Info
22	21.054235	2a01:cb1d:7:8d00:cf...	2a01:cb1d:7:8d00:4e...	DNS	90	Standard query 0x43a6 AAAA ac-nice.fr
23	21.056749	2a01:cb1d:7:8d00:4e...	2a01:cb1d:7:8d00:cf...	DNS	90	Standard query response 0x43a6 AAAA ac-nice.fr
24	21.064775	192.168.1.20	194.167.84.160	ICMP	74	Echo (ping) request id=0x0001, seq=57/14592, ttl=128 (reply in
25	21.098679	194.167.84.160	192.168.1.20	ICMP	74	Echo (ping) reply id=0x0001, seq=57/14592, ttl=48 (request in
26	22.085651	192.168.1.20	194.167.84.160	ICMP	74	Echo (ping) request id=0x0001, seq=58/14848, ttl=128 (reply in
27	22.119051	194.167.84.160	192.168.1.20	ICMP	74	Echo (ping) reply id=0x0001, seq=58/14848, ttl=48 (request in
28	23.101784	192.168.1.20	194.167.84.160	ICMP	74	Echo (ping) request id=0x0001, seq=59/15104, ttl=128 (reply in
29	23.139687	194.167.84.160	192.168.1.20	ICMP	74	Echo (ping) reply id=0x0001, seq=59/15104, ttl=48 (request in
30	24.117346	192.168.1.20	194.167.84.160	ICMP	74	Echo (ping) request id=0x0001, seq=60/15360, ttl=128 (reply in
31	24.154545	194.167.84.160	192.168.1.20	ICMP	74	Echo (ping) reply id=0x0001, seq=60/15360, ttl=48 (request in
113	48.698187	Apple_8c:0d:99	Broadcast	ARP	42	Who has 192.168.1.11? Tell 192.168.1.13
318	121.367745	192.168.1.20	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=61/15616, ttl=128 (reply in
319	121.375905	192.168.1.1	192.168.1.20	ICMP	74	Echo (ping) reply id=0x0001, seq=61/15616, ttl=64 (request in
320	122.378639	192.168.1.20	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=62/15872, ttl=128 (reply in
321	122.382715	192.168.1.1	192.168.1.20	ICMP	74	Echo (ping) reply id=0x0001, seq=62/15872, ttl=64 (request in
324	123.389355	192.168.1.20	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=63/16128, ttl=128 (reply in
325	123.393236	192.168.1.1	192.168.1.20	ICMP	74	Echo (ping) reply id=0x0001, seq=63/16128, ttl=64 (request in
327	124.406102	192.168.1.20	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=64/16384, ttl=128 (reply in
328	124.410021	192.168.1.1	192.168.1.20	ICMP	74	Echo (ping) reply id=0x0001, seq=64/16384, ttl=64 (request in

> User Datagram Protocol, Src Port: 61292, Dst Port: 53

> Domain Name System (query)

Transaction ID: 0x43a6

> Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

> Queries

> ac-nice.fr: type AAAA, class IN

Name: ac-nice.fr

[Name Length: 10]

[Label Count: 2]

Type: AAAA (IPv6 Address) (28)

Class: IN (0x0001)

[Response In: 23]

Internet Protocol Version 6, Src: 2a01:cb1d:7:8d00:cfe:13af:6baf:16a9, Dst: 2a01:cb1d:7:8d00:4e22:f3ff:fe45:d

User Datagram Protocol, Src Port: 64304, Dst Port: 53

> Domain Name System (query)

Transaction ID: 0x5f54

> Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

> Queries

> ac-nice.fr: type AAAA, class IN

Name: ac-nice.fr

0000 13 41 00 41 10 89 48 01 c0 10 00 01 80 00 4e 22
0030 f3 ff fe 45 de 86 fb 30 00 35 00 24 2c c9 5f 54
0040 01 00 00 01 00 00 00 00 00 00 07 61 63 2d 6e 60
0050 63 65 02 66 72 00 00 1c 00 01

- 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. (Je n'ai pas de rubrique Answers)

No.	Time	Source	Destination	Protocol	Length	Info
22	21.054235	2a01:cb1d:7:8d00:cf...	2a01:cb1d:7:8d00:4e...	DNS	90	Standard query 0x43a6 AAAA ac-nice.fr
23	21.056749	2a01:cb1d:7:8d00:4e...	2a01:cb1d:7:8d00:cf...	DNS	90	Standard query response 0x43a6 AAAA ac-nice.fr
24	21.064775	192.168.1.20	194.167.84.160	ICMP	74	Echo (ping) request id=0x0001, seq=57/14592, ttl=128 (reply in 25)
25	21.098679	194.167.84.160	192.168.1.20	ICMP	74	Echo (ping) reply id=0x0001, seq=57/14592, ttl=48 (request in 24)
26	22.085651	192.168.1.20	194.167.84.160	ICMP	74	Echo (ping) request id=0x0001, seq=58/14848, ttl=128 (reply in 27)
27	22.119051	194.167.84.160	192.168.1.20	ICMP	74	Echo (ping) reply id=0x0001, seq=58/14848, ttl=48 (request in 26)
28	23.101784	192.168.1.20	194.167.84.160	ICMP	74	Echo (ping) request id=0x0001, seq=59/15104, ttl=128 (reply in 29)
29	23.139687	194.167.84.160	192.168.1.20	ICMP	74	Echo (ping) reply id=0x0001, seq=59/15104, ttl=48 (request in 28)
30	24.117346	192.168.1.20	194.167.84.160	ICMP	74	Echo (ping) request id=0x0001, seq=60/15360, ttl=128 (reply in 31)
31	24.154545	194.167.84.160	192.168.1.20	ICMP	74	Echo (ping) reply id=0x0001, seq=60/15360, ttl=48 (request in 30)
113	48.698187	Apple_8c:0d:99	Broadcast	ARP	42	Who has 192.168.1.11? Tell 192.168.1.13
318	121.367745	192.168.1.20	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=61/15616, ttl=128 (reply in 319)
319	121.375905	192.168.1.1	192.168.1.20	ICMP	74	Echo (ping) reply id=0x0001, seq=61/15616, ttl=64 (request in 318)
320	122.378639	192.168.1.20	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=62/15872, ttl=128 (reply in 321)
321	122.382715	192.168.1.1	192.168.1.20	ICMP	74	Echo (ping) reply id=0x0001, seq=62/15872, ttl=64 (request in 320)
324	123.389355	192.168.1.20	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=63/16128, ttl=128 (reply in 325)
325	123.393236	192.168.1.1	192.168.1.20	ICMP	74	Echo (ping) reply id=0x0001, seq=63/16128, ttl=64 (request in 324)
327	124.406102	192.168.1.20	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=64/16384, ttl=128 (reply in 328)
328	124.410021	192.168.1.1	192.168.1.20	ICMP	74	Echo (ping) reply id=0x0001, seq=64/16384, ttl=64 (request in 327)

> Frame 23: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface Ve

> Ethernet II, Src: Arcadyan_45:de:86 (4c:22:f3:45:de:86), Dst: CloudNet_4e:23:4f (10:

> Internet Protocol Version 6, Src: 2a01:cb1d:7:8d00:4e22:3fff:fe45:de86, Dst: 2a01:cb

> User Datagram Protocol, Src Port: 53, Dst Port: 61292

> Domain Name System (response)

Transaction ID: 0x43a6

Flags: 0x8180 Standard query response, No error

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

Queries

> ac-nice.fr: type AAAA, class IN

[Request In: 22]

[Time: 0.002514000 seconds]

```

0000 10 f6 d9 4e 23 4f 4c 22 f3 45 de 86 86 dd 60 00 00 00 00 24 11 ff 2a 01 cb 1d 00 07 8d 00 4e 22
0010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0020 f3 ff fe 45 de 86 2a 01 cb 1d 00 07 8d 00 0c fe 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0030 13 af 6b af 16 a9 00 35 ef 6c 00 24 d3 ba 43 a6 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0040 81 80 00 01 00 00 00 00 00 00 00 00 07 61 63 2d 6e 69 00 00 00 00 00 00 00 00 00 00
0050 63 65 02 66 72 00 00 1c 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

```

4.3 Commande Tracert et capture de trames ICMP

° La commande **tracert** permet de connaître tous les **routeurs** entre la machine locale et une destination donnée, par exemple le site web de l'Académie de Nice (**tracert www.ac-nice.fr**) :

- ➔ Démarrez une capture de trames **depuis votre machine physique**.
- ➔ Ouvrez une invite de commandes et saisissez la commande **tracert www.ac-nice.fr**.

No.	Time	Source	Destination	Protocol	Length	Info
782	39.417669	192.168.1.20	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=65/16640, ttl=128
783	39.422054	192.168.1.1	192.168.1.20	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
784	39.422484	192.168.1.20	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=66/16896, ttl=128
785	39.435815	192.168.1.1	192.168.1.20	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
786	39.436766	192.168.1.20	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=67/17152, ttl=128
787	39.440830	192.168.1.1	192.168.1.20	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
795	40.457231	192.168.1.20	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=68/17408, ttl=128
796	40.463333	90.116.48.1	192.168.1.20	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
797	40.465717	192.168.1.20	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=69/17664, ttl=128
798	40.471699	90.116.48.1	192.168.1.20	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
799	40.474041	192.168.1.20	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=70/17920, ttl=128
800	40.480071	90.116.48.1	192.168.1.20	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
805	41.510330	192.168.1.20	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=71/18176, ttl=128
806	41.517585	193.253.86.30	192.168.1.20	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
807	41.519974	192.168.1.20	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=72/18432, ttl=128
808	41.525766	193.253.86.30	192.168.1.20	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
809	41.528322	192.168.1.20	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=73/18688, ttl=128
810	41.534986	193.253.86.30	192.168.1.20	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
815	42.564546	192.168.1.20	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=74/18944, ttl=128

- Sélectionnez la **première trame ICMP Echo request**. Développez l'en-tête IP. Quelle est l'adresse IP **Destination** (valeurs déci. Et hexa.) ?

L'adresse de destination dans la première trame ICMP Echo Request en hexa est 5d b8 dd a1 et en décimale 93.184.221.161

Internet Protocol Version 4, Src: 192.168.1.20, Dst: 93.184.221.161	0000	4c 22 f3 45 de 86 10 6f	d9 4e 23 4f 08 00 45 00	L" E...
0100 = Version: 4	0010	00 5c fd be 00 00 01 01	be cc c0 a8 01 14 5d b8	..\\.....
.... 0101 = Header Length: 20 bytes (5)	0020	dd a1 08 00 f7 bd 00 01	00 41 00 00 00 00 00 00	
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)	0030	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
Total Length: 92	0040	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
Identification: 0xfdb6 (64958)	0050	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
> 000. = Flags: 0x0	0060	00 00 00 00 00 00 00 00	00 00	
...0 0000 0000 0000 = Fragment Offset: 0				
> Time to Live: 1				
Protocol: ICMP (1)				
Header Checksum: 0xbecc [validation disabled]				
[Header checksum status: Unverified]				
Source Address: 192.168.1.20				
Destination Address: 93.184.221.161				

- Sélectionnez le champ **TTL**. Quelle est la valeur portée par ce champ (valeurs déci. Et hexa.) ?

La valeur portée par le champ TTL est 1.

Internet Protocol Version 4, Src: 192.168.1.20, Dst: 93.184.221.161	0000	4c 22 f3 45 de 86 10 6f	d9 4e 23 4f 08 00 45 00	L" E...
0100 = Version: 4	0010	00 5c fd be 00 00 01 01	be cc c0 a8 01 14 5d b8	..\\.....
.... 0101 = Header Length: 20 bytes (5)	0020	dd a1 08 00 f7 bd 00 01	00 41 00 00 00 00 00 00	
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)	0030	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
Total Length: 92	0040	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
Identification: 0xfdb6 (64958)	0050	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
> 000. = Flags: 0x0	0060	00 00 00 00 00 00 00 00	00 00	
...0 0000 0000 0000 = Fragment Offset: 0				
> Time to Live: 1				

- Sélectionnez la trame, comportant un message d'erreur ICMP **Time-to-live exceeded**, envoyée par le premier routeur rencontré. Développez la section correspondant au message ICMP. Quelle est la valeur portée par le champ Type ?

La valeur portée par le champ Type est 11 en décimale et en hexa 0b.

Internet Control Message Protocol	0010	00 78 54 95 00 00 40 01	a0 9e c0 a8 01 fe c0 a8	-xT...@.....
Type: 11 (Time-to-live exceeded)	0020	01 43 0b 00 f4 ff 00 00	00 00 45 00 00 5c 1b 8c	-C.....E.....
Code: 0 (Time to live exceeded in transit)	0030	00 00 01 01 a0 d0 c0 a8	01 43 5d b8 dd a1 08 00	[C].....
Checksum: 0xf4ff [correct]	0040	f7 be 00 01 00 40 00 00	00 00 00 00 00 00 00 00	@.....