

TP3: Trames ARP, ICMP et DNS

1) Capture de trames ARP et ICMP

*Ethernet

Fichier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide

arp or icmp

No.	Time	Source	Destination	Protocol	Length	Info
4	0.015300	Vmware_22:87:6d	Broadcast	ARP	60	Who has 172.17.244.15? Tell 172.17.243.11
41	0.607948	Vmware_22:87:6d	Broadcast	ARP	60	Who has 172.17.244.15? Tell 172.17.243.11
104	1.607974	Vmware_22:87:6d	Broadcast	ARP	60	Who has 172.17.244.15? Tell 172.17.243.11
193	2.963201	172.17.2.140	172.17.254.1	ICMP	74	Echo (ping) request id=0x0001, seq=21/5376, ttl=128 (reply in 194)
194	2.963511	172.17.254.1	172.17.2.140	ICMP	74	Echo (ping) reply id=0x0001, seq=21/5376, ttl=128 (request in 193)
204	3.045444	Vmware_22:87:6d	Broadcast	ARP	60	Who has 172.17.244.15? Tell 172.17.243.11
252	3.607911	Vmware_22:87:6d	Broadcast	ARP	60	Who has 172.17.244.15? Tell 172.17.243.11
261	3.971238	172.17.2.140	172.17.254.1	ICMP	74	Echo (ping) request id=0x0001, seq=22/5632, ttl=128 (reply in 262)
262	3.971518	172.17.254.1	172.17.2.140	ICMP	74	Echo (ping) reply id=0x0001, seq=22/5632, ttl=128 (request in 261)
317	4.607940	Vmware_22:87:6d	Broadcast	ARP	60	Who has 172.17.244.15? Tell 172.17.243.11
367	4.986624	172.17.2.140	172.17.254.1	ICMP	74	Echo (ping) request id=0x0001, seq=23/5888, ttl=128 (reply in 368)
368	4.986865	172.17.254.1	172.17.2.140	ICMP	74	Echo (ping) reply id=0x0001, seq=23/5888, ttl=128 (request in 367)
427	6.002002	172.17.2.140	172.17.254.1	ICMP	74	Echo (ping) request id=0x0001, seq=24/6144, ttl=128 (reply in 428)
428	6.002310	172.17.254.1	172.17.2.140	ICMP	74	Echo (ping) reply id=0x0001, seq=24/6144, ttl=128 (request in 427)
487	7.061198	Vmware_22:87:6d	Broadcast	ARP	60	Who has 172.17.244.15? Tell 172.17.243.11
515	7.607943	Vmware_22:87:6d	Broadcast	ARP	60	Who has 172.17.244.15? Tell 172.17.243.11
535	7.848839	Dell_7d:0e:2b	Dell_12:d6:a7	ARP	60	Who has 172.17.2.140? Tell 172.17.254.1

1ère étape: Une capture de trames à été lancée en même temps que nous effectuons un ping sur le Serveur ROI. Nous observons donc avec le filtre les échanges de trames ARP et ICMP.

Administrator : Invite de commandes

```
C:\WINDOWS\system32>ping 172.17.254.1

Envoi d'une requête 'Ping' 172.17.254.1 avec 32 octets de données :
Réponse de 172.17.254.1 : octets=32 temps<1ms TTL=128

Statistiques Ping pour 172.17.254.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms

C:\WINDOWS\system32>
```

2ème étape:
Voici une

capture d'écran effectuer lors d'une ping du Serveur ROI.

Administrateur : invite de commandes

C:\WINDOWS\system32>arp -a

Interface : 172.17.2.140 --- 0xa	Adresse Internet	Adresse physique	Type
	172.17.2.5	d8-9e-f3-12-bd-b4	dynamique
	172.17.2.11	d8-9e-f3-11-08-a9	dynamique
	172.17.2.15	d8-9e-f3-12-d6-1d	dynamique
	172.17.2.20	d8-9e-f3-12-e0-7f	dynamique
	172.17.2.132	d8-9e-f3-12-d2-d9	dynamique
	172.17.2.141	d8-9e-f3-12-da-64	dynamique
	172.17.244.1	00-0c-29-76-e3-f7	dynamique
	172.17.250.2	b8-26-6c-af-27-76	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

3ème étape: On observe par la suite avec la commande “arp -a” qu’une fois les échanges ARP effectuer entre la machine et le serveur ROI, l’adresse MAC et l’adresse IP de ROI apparaît donc dans le cache ARP.

4 0.015300	Vmware_22:87:6d	Broadcast	ARP	60 Who has 172.17.244.15? Tell 172.17.243.11
41 0.087948	Vmware_22:87:6d	Broadcast	ARP	60 Who has 172.17.244.15? Tell 172.17.243.11
104 1.087948	Vmware_22:87:6d	Broadcast	ARP	60 Who has 172.17.244.15? Tell 172.17.243.11
+ 193 2.963201	172.17.2.140	172.17.254.1	ICMP	74 Echo (ping) request id=0x0001, seq=21/5376, ttl=128 (reply in 194)
+ 194 2.963511	172.17.254.1	172.17.2.140	ICMP	74 Echo (ping) reply id=0x0001, seq=21/5376, ttl=128 (request in 193)
204 3.045444	Vmware_22:87:6d	Broadcast	ARP	60 Who has 172.17.244.15? Tell 172.17.243.11
252 3.607911	Vmware_22:87:6d	Broadcast	ARP	60 Who has 172.17.244.15? Tell 172.17.243.11
261 3.971238	172.17.2.140	172.17.254.1	ICMP	74 Echo (ping) request id=0x0001, seq=22/5632, ttl=128 (reply in 262)
262 3.971518	172.17.254.1	172.17.2.140	ICMP	74 Echo (ping) reply id=0x0001, seq=22/5632, ttl=128 (request in 261)
317 4.607940	Vmware_22:87:6d	Broadcast	ARP	60 Who has 172.17.244.15? Tell 172.17.243.11
367 4.986624	172.17.2.140	172.17.254.1	ICMP	74 Echo (ping) request id=0x0001, seq=23/5888, ttl=128 (reply in 368)
368 4.986865	172.17.254.1	172.17.2.140	ICMP	74 Echo (ping) reply id=0x0001, seq=23/5888, ttl=128 (request in 367)
427 6.002002	172.17.2.140	172.17.254.1	ICMP	74 Echo (ping) request id=0x0001, seq=24/6144, ttl=128 (reply in 428)
428 6.002310	172.17.254.1	172.17.2.140	ICMP	74 Echo (ping) reply id=0x0001, seq=24/6144, ttl=128 (request in 427)
487 7.061198	Vmware_22:87:6d	Broadcast	ARP	60 Who has 172.17.244.15? Tell 172.17.243.11
515 7.607943	Vmware_22:87:6d	Broadcast	ARP	60 Who has 172.17.244.15? Tell 172.17.243.11
535 7.848839	Dell_7d:0e:2b	Dell_12:d6:a7	ARP	60 Who has 172.17.2.140? Tell 172.17.254.1

> Frame 193: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
> Ethernet II, Src: Dell_12:d6:a7 (d8:9e:f3:12:d6:a7), Dst: Dell_7d:0e:2b (d4:ae:52:7d:0e:2b)
> Internet Protocol Version 4, Src: 172.17.2.140, Dst: 172.17.254.1
> Internet Control Message Protocol

0000 d4 ae 52 7d 0e 2b d8 9e f3 12 d6 a7 08 00 45 00 ..R}+...E
0010 00 3c 31 31 00 00 80 01 00 00 ac 11 02 8c ac 11 <11....
0020 fe 01 08 00 4d 46 00 01 00 15 61 62 63 64 65 66MF... .abcdef
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 wabcde fg hi

31 / 4.60/940	VMware_22:87:6d	Broadcast	ARP	60 Who has 172.17.244.15? tell 172.17.243.11
367 4.986624	172.17.2.140	172.17.254.1	ICMP	74 Echo (ping) request id=0x0001, seq=23/5888, ttl=128 (reply in 368)
368 4.986865	172.17.254.1	172.17.2.140	ICMP	74 Echo (ping) reply id=0x0001, seq=23/5888, ttl=128 (request in 367)
> Frame 4: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{A2E487D7-0741-460A-9C66-CD889043CD0}, id 0				
< Ethernet II, Src: VMware_22:87:6d (00:0c:29:22:87:6d), Dst: Broadcast (ff:ff:ff:ff:ff:ff)				
> Destination: Broadcast (ff:ff:ff:ff:ff:ff)				
> Source: VMware_22:87:6d (00:0c:29:22:87:6d)				
Type: ARP (0x0806)				
Padding: 00				
> Address Resolution Protocol (request)				
0000	ff ff ff ff ff ff	00 0c 29 22 87 6d	08 06 00 01)"m-
0010	08 00 06 04 00 01	00 0c 29 22 87 6d	ac 11 f3 0b)"m-
0020	00 00 00 00 00 00	ac 11 f4 0f	00 00 00 00 00 00
0030	00 00 00 00 00 00	00 00 00 00 00 00	00 00 00 00 00 00

Analysez l'échange de trames ARP (Request et Reply) précédent l'échange de trames ICMP :

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

Les octets 13 et 14 signifient que le champ Ethertype est 0806 (ARP)

Quelle est la fonction de la trame ARP Request ?

La trame ARP Request permet d'obtenir l'adresse MAC d'une machine locale.

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

Les octets numéro 5 et 6 de la ligne 0010 sont 00 01 ce qui signifie que c'est une requête ARP.

Quelle est la longueur d'un message ARP ?

Le message ARP est sur 16 bits.

Quelle est la longueur de la trame ARP Request ?

La trame ARP Request est d'une longueur de 60 octets

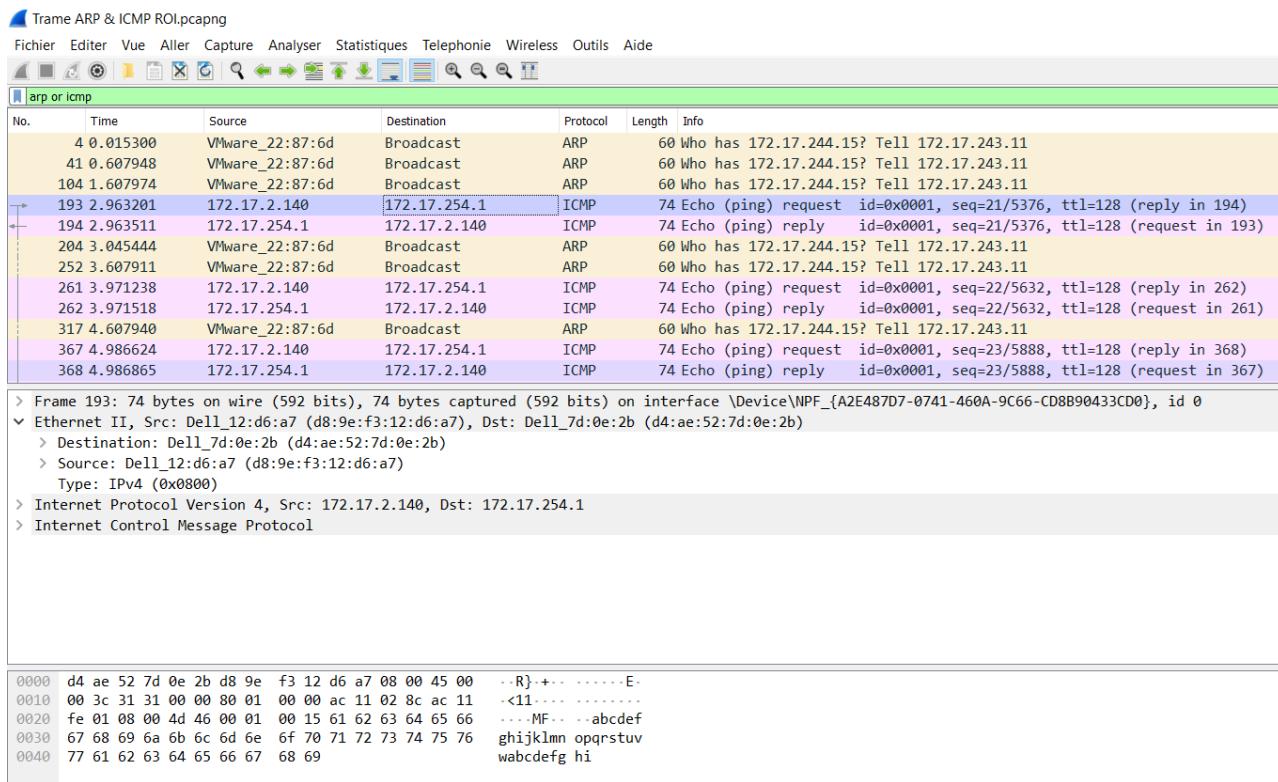
Quelle est la longueur de la trame ARP Reply ?

La trame ARP Reply est d'une longueur de 60 octets

Combien d'octets sont utilisés pour le padding ?

18 octets sont utilisés pour le padding

Trame ARP request	
@MAC destination =	ff ff ff ff ff ff
@MAC source =	d4 ae 52 7d 0e 2b
Ethernet Type =	0806
Opcode (valeurs hexa.) =	00 01
@MAC de la cible =	00 00 00 00 00 00
@IP de la cible =	Ac 11 f4 0f



Sélectionnez une trame ICMP Echo Request:

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

Le 13 et 14ème octet de la ligne 0000 ont comme valeur 0800 ce qui signifie qu'ils représentent tout deux le champ Ethertype (IPv4).

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

Le 8ème octet représente la valeur 01 donc le protocole de transport Datagramme UDP.

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 20 octets

Quelle est la longueur du message ICMP ?

Le message ICMP avec les données est de 40 octets

Quelle signification ont les octets de position 0x02 et 0x03, ligne 00020 ?

Le 3ème octet de la ligne 00020 représente le type 08, le 4ème le code 0. Cela signifie donc que c'est une trame ICMP echo request.

A quoi correspondent les octets à partir de l'octet 0x0A, ligne 00020 ?

A partir du 11ème octet, les octets représentent les données de la trame.

Trame ARP & ICMP ROI.pcapng

Fichier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide

arp or icmp

No.	Time	Source	Destination	Protocol	Length	Info
4	0.015300	VMware_22:87:6d	Broadcast	ARP	60	Who has 172.17.244.15? Tell 172.17.243.11
41	0.607948	VMware_22:87:6d	Broadcast	ARP	60	Who has 172.17.244.15? Tell 172.17.243.11
104	1.607974	VMware_22:87:6d	Broadcast	ARP	60	Who has 172.17.244.15? Tell 172.17.243.11
193	2.963201	172.17.2.140	172.17.254.1	ICMP	74	Echo (ping) request id=0x0001, seq=21/5376, ttl=128 (reply in 194)
194	2.963511	172.17.254.1	172.17.2.140	ICMP	74	Echo (ping) reply id=0x0001, seq=21/5376, ttl=128 (request in 193)
204	3.045444	VMware_22:87:6d	Broadcast	ARP	60	Who has 172.17.244.15? Tell 172.17.243.11
252	3.607911	VMware_22:87:6d	Broadcast	ARP	60	Who has 172.17.244.15? Tell 172.17.243.11
261	3.971238	172.17.2.140	172.17.254.1	ICMP	74	Echo (ping) request id=0x0001, seq=22/5632, ttl=128 (reply in 262)
262	3.971518	172.17.254.1	172.17.2.140	ICMP	74	Echo (ping) reply id=0x0001, seq=22/5632, ttl=128 (request in 261)
317	4.607940	VMware_22:87:6d	Broadcast	ARP	60	Who has 172.17.244.15? Tell 172.17.243.11
367	4.986624	172.17.2.140	172.17.254.1	ICMP	74	Echo (ping) request id=0x0001, seq=23/5888, ttl=128 (reply in 368)
368	4.986865	172.17.254.1	172.17.2.140	ICMP	74	Echo (ping) reply id=0x0001, seq=23/5888, ttl=128 (request in 367)

Destination Address: 172.17.2.140

Internet Control Message Protocol

Type: 0 (Echo (ping) reply)
 Code: 0
 Checksum: 0x5546 [correct]
 [Checksum Status: Good]
 Identifier (BE): 1 (0x0001)
 Identifier (LE): 256 (0x0100)
 Sequence Number (BE): 21 (0x0015)
 Sequence Number (LE): 5376 (0x1500)
 [Request frame: 193]
 [Response time: 0,310 ms]

Data (32 bytes)

```

0000 d8 9e f3 12 d6 a7 d4 ae 52 7d 0e 2b 08 00 45 00  . . . . . R} .+ .E.
0010 00 3c cd 9d 00 00 80 01 14 73 ac 11 fe 01 ac 11  .< . . . . S . . . .
0020 02 8c 00 00 55 46 00 01 00 15 61 62 63 64 65 66  . . . UF . . . abcdef
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76  ghi jklmn opqrstuv
0040 77 61 62 63 64 65 66 67 68 69  wabcdefg hi

```

Sélectionnez une trame ICMP Echo Reply:

Quelles sont les noms et valeurs des octets de position 0x02 et 0x03, ligne 00020 ?
 L'octet de position 0x02 est d'une valeur hexa de 00, il signifie que le type ici présent est le Type 0, et l'octet de position 0x03 à comme valeur hexa 00 et représente lui le Code 0. Cela signifie donc que c'est une trame ICMP echo reply.

2) Capture de trames ARP, DNS et ICMP

Administrator : Invité de commandes

```
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=526 ms TTL=56
Réponse de 93.184.221.161 : octets=32 temps=301 ms TTL=56
Réponse de 93.184.221.161 : octets=32 temps=291 ms TTL=56
Réponse de 93.184.221.161 : octets=32 temps=272 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 = 272ms, Maximum = 526ms, Moyenne = 347ms

1ère étape: En démarrant une capture de trames, nous effectuons un ping vers le serveur web de www.ac-nice.fr

CapturelcmpDns.pcapng

Fichier Editer Vue Aller Capture Analyser Statistiques Téléphonie Wireless Outils Aide

arp or dns or icmp

No.	Time	Source	Destination	Protocol	Length	Info
2	0.053480	AnovFran_af:27:76	Broadcast	ARP	60	Who has 172.17.2.132? Tell 172.17.250.2
66	0.679636	Dell_12:da:64	Broadcast	ARP	60	Who has 169.254.144.92? Tell 0.0.0.0
184	1.680733	Dell_12:da:64	Broadcast	ARP	60	Gratuitous ARP for 169.254.144.92 (Request)
190	2.888794	172.17.2.140	172.17.2.140	DNS	74	Standard query 0xe42a A www.ac-nice.fr
191	2.889206	172.17.2.140	172.17.2.140	DNS	126	Standard query response 0xe42a A www.ac-nice.fr CNAME cs234.wpc.alphacdn.net A 93.184.221.161
192	2.893165	172.17.2.140	93.184.221.161	ICMP	74	Echo (ping) request id=0x0001, seq=25/6400, ttl=128 (reply in 198)
198	3.419375	93.184.221.161	172.17.2.140	ICMP	74	Echo (ping) reply id=0x0001, seq=25/6400, ttl=56 (request in 192)
202	3.682933	Dell_12:da:64	Broadcast	ARP	60	Who has 172.17.2.141? Tell 0.0.0.0
224	3.903988	172.17.2.140	93.184.221.161	ICMP	74	Echo (ping) request id=0x0001, seq=26/6656, ttl=128 (reply in 233)
233	4.205381	93.184.221.161	172.17.2.140	ICMP	74	Echo (ping) reply id=0x0001, seq=26/6656, ttl=56 (request in 224)
243	4.682624	Dell_12:da:64	Broadcast	ARP	60	Who has 172.17.2.141? Tell 0.0.0.0
246	4.841716	Dell_12:d6:a7	AnovFran_af:27:76	ARP	42	Who has 172.17.250.2? Tell 172.17.2.140
247	4.845832	AnovFran_af:27:76	Dell_12:d6:a7	ARP	60	172.17.250.2 is at b8:26:6c:af:27:76
248	4.919932	172.17.2.140	93.184.221.161	ICMP	74	Echo (ping) request id=0x0001, seq=27/6912, ttl=128 (reply in 255)
251	4.950298	Dell_12:da:64	Broadcast	ARP	60	Who has 172.17.250.2? Tell 172.17.2.141
255	5.211435	93.184.221.161	172.17.2.140	ICMP	74	Echo (ping) reply id=0x0001, seq=27/6912, ttl=56 (request in 248)
260	5.935308	172.17.2.140	93.184.221.161	ICMP	74	Echo (ping) request id=0x0001, seq=28/7168, ttl=128 (reply in 283)
278	6.182282	Dell_12:da:64	Broadcast	ARP	60	Who has 172.17.2.141? Tell 0.0.0.0
283	6.207694	93.184.221.161	172.17.2.140	ICMP	74	Echo (ping) reply id=0x0001, seq=28/7168, ttl=56 (request in 260)
288	6.291724	Dell_12:da:64	Broadcast	ARP	60	Who has 172.17.244.1? Tell 172.17.2.141

2ème étape: Ici on remarque que la liste des trames commence par une requête et une réponse ARP.

Quelle est l'adresse MAC recherchée ?

L'adresse MAC recherché est celle qui correspond également à l'adresse IP 172.17.2.132

Complétez les rubriques ci-dessous :

Trame ARP request
@MAC destination = ff ff ff ff ff ff
@MAC source = B8 26 6c af 27 76
Ethernet Type = ARP
Opcode (valeurs hexa.) = 01
@MAC de la cible = 00 00 00 00 00 00
@IP de la cible = ac 11 02 84

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

La requête DNS nous permet d'obtenir l'adresse d'un serveur DNS sur lequel le nom du domaine du site internt peut y figurer. Par la suite nous pouvons donc obetenir l'adresse IP du site.

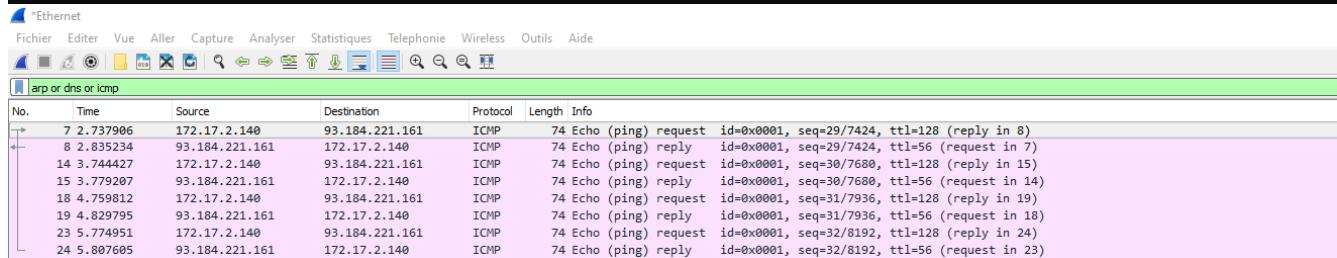
```
www.ac-nice.fr
-----
Nom d'enregistrement. : www.ac-nice.fr
Type d'enregistrement : 5
Durée de vie . . . . . : 3010
Longueur de données . : 8
Section . . . . . . . . : Réponse
Enregistrement CNAME : cs234.wpc.alphacd.net
```

3ème étape: Ici nous constatons donc la présence de l'enregistrement DNS www.ac-nice.fr via la commande “**ipconfig /displaydns**” qui nous permet d'obtenir tout les caches DNS.

Administateur : Invité de commandes

```
C:\WINDOWS\system32>ping www.ac-nice.fr
```

```
Envoi d'une requête 'ping' sur cs234.wpc.alphacd.net [93.184.221.161] avec 32 octets de données :  
Réponse de 93.184.221.161 : octets=32 temps=97 ms TTL=56  
Réponse de 93.184.221.161 : octets=32 temps=34 ms TTL=56  
Réponse de 93.184.221.161 : octets=32 temps=70 ms TTL=56  
Réponse de 93.184.221.161 : octets=32 temps=32 ms TTL=56
```



4ème étape: Si nous effectuons donc de nouveau un ping de ce domaine avec une capture de trame en même temps, nous constatons donc qu'il n'y a plus de requête DNS puisque les informations DNS pour ce nom de domaine sont déjà présentent dans le cache DNS.

```
C:\WINDOWS\system32>ipconfig /flushdns  
Configuration IP de Windows  
Cache de résolution DNS vidé.
```

```
C:\WINDOWS\system32>ping www.ac-nice.fr
```

```
Envoi d'une requête 'ping' sur cs234.wpc.alphacd.net [93.184.221.161] avec 32 octets de données :  
Réponse de 93.184.221.161 : octets=32 temps=316 ms TTL=56  
Réponse de 93.184.221.161 : octets=32 temps=123 ms TTL=56  
Réponse de 93.184.221.161 : octets=32 temps=83 ms TTL=56  
Réponse de 93.184.221.161 : octets=32 temps=169 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 = 83ms, Maximum = 316ms, Moyenne = 172ms
```

5ème étape: Avec la commande “ipconfig /flushdns” nous vidons donc le cache DNS. Une fois cette manipulation effectuer une nouvelle capture de trames est lancé accompagner d'un nouveau ping du domaine ac-nice.fr

*Ethernet

Fichier Editer Vue Aller Capture Analyser Statistiques Téléphonie Wireless Outils Aide

arp or dns or icmp

No.	Time	Source	Destination	Protocol	Length	Info
106	2.091483	172.17.2.140	172.17.254.1	DNS	74	Standard query 0xb6fc A www.ac-nice.fr
107	2.091951	172.17.254.1	172.17.2.140	DNS	126	Standard query response 0xb6fc A www.ac-nice.fr CNAME cs234.wpc.alphcdn.net A 93.184.221.161
109	2.098641	172.17.2.140	93.184.221.161	ICMP	74	Echo (ping) request id=0x0001, seq=33/8448, ttl=128 (reply in 123)
116	2.225620	172.17.2.140	172.17.254.1	DNS	87	Standard query 0xf0cf A fp-vp-nocache.azureedge.net
123	2.415437	93.184.221.161	172.17.2.140	ICMP	74	Echo (ping) reply id=0x0001, seq=33/8448, ttl=56 (request in 109)
127	2.483461	172.17.254.1	172.17.2.140	DNS	162	Standard query response 0xf0cf A fp-vp-nocache.azureedge.net CNAME fp-vp-nocache.ec.azureedge.net CNAME cs9.wpc.v0cdn.net A 152.199.19.161
182	3.108846	172.17.2.140	93.184.221.161	ICMP	74	Echo (ping) request id=0x0001, seq=34/8704, ttl=128 (reply in 189)
189	3.232321	93.184.221.161	172.17.2.140	ICMP	74	Echo (ping) reply id=0x0001, seq=34/8704, ttl=56 (request in 182)
200	3.422535	AnovFran_af:27:76	Dell_12:d6:a7	ARP	60	Who has 172.17.2.140? Tell 172.17.250.2
201	3.422542	Dell_12:d6:a7	AnovFran_af:27:76	ARP	42	172.17.2.140 is at d8:9e:f3:12:d6:a7
232	4.124196	172.17.2.140	93.184.221.161	ICMP	74	Echo (ping) request id=0x0001, seq=35/8960, ttl=128 (reply in 237)
237	4.207876	93.184.221.161	172.17.2.140	ICMP	74	Echo (ping) reply id=0x0001, seq=35/8960, ttl=56 (request in 232)
244	4.406981	172.17.2.140	172.17.254.1	DNS	78	Standard query 0x134e A edge.microsoft.com
245	4.407399	172.17.254.1	172.17.2.140	DNS	160	Standard query response 0x134e A edge.microsoft.com CNAME edge-microsoft-com.a-0016.a-msedge.net CNAME a-0016.a-msedge.net A 204.79.197.219
299	5.139631	172.17.2.140	93.184.221.161	ICMP	74	Echo (ping) request id=0x0001, seq=36/9216, ttl=128 (reply in 311)
299	5.156825	Vmware_22:87:6d	Broadcast	ARP	60	Who has 172.17.244.1? Tell 172.17.243.11
311	5.309548	93.184.221.161	172.17.2.140	ICMP	74	Echo (ping) reply id=0x0001, seq=36/9216, ttl=56 (request in 298)
420	6.730544	Dell_12:d6:a7	Dell_7d:0e:2b	ARP	42	Who has 172.17.254.1? Tell 172.17.2.140
421	6.730783	Dell_7d:0e:2b	Dell_12:d6:a7	ARP	60	Who has 172.17.2.140? Tell 172.17.250.2
422	6.898996	Dell_7d:0e:2b	Dell_12:d6:a7	ARP	60	Who has 172.17.2.140? Tell 172.17.250.2
423	6.899009	Dell_12:d6:a7	Dell_7d:0e:2b	ARP	42	172.17.2.140 is at d8:9e:f3:12:d6:a7

6ème étape: Cette fois-ci avec le cache DNS vidé les requête DNS font leur apparition.

106	2.091483	172.17.2.140	172.17.254.1	DNS	74	Standard query 0xb6fc A www.ac-nice.fr
107	2.091951	172.17.254.1	172.17.2.140	DNS	126	Standard query response 0xb6fc A www.ac-nice.fr CNAME cs234.wpc.alphcdn.net A 93.184.221.161
109	2.098641	172.17.2.140	93.184.221.161	ICMP	74	Echo (ping) request id=0x0001, seq=33/8448, ttl=128 (reply in 123)
116	2.225620	172.17.2.140	172.17.254.1	DNS	87	Standard query 0xf0cf A fp-vp-nocache.azureedge.net
123	2.415437	93.184.221.161	172.17.2.140	ICMP	74	Echo (ping) reply id=0x0001, seq=33/8448, ttl=56 (request in 109)
127	2.483461	172.17.254.1	172.17.2.140	DNS	162	Standard query response 0xf0cf A fp-vp-nocache.azureedge.net CNAME fp-vp-nocache.ec.azureedge.net CNAME cs9.wpc.v0cdn.net A 152.199.19.161
182	3.108846	172.17.2.140	93.184.221.161	ICMP	74	Echo (ping) request id=0x0001, seq=34/8704, ttl=128 (reply in 189)
189	3.232321	93.184.221.161	172.17.2.140	ICMP	74	Echo (ping) reply id=0x0001, seq=34/8704, ttl=56 (request in 182)
200	3.422535	AnovFran_af:27:76	Dell_12:d6:a7	ARP	60	Who has 172.17.2.140? Tell 172.17.250.2
201	3.422542	Dell_12:d6:a7	AnovFran_af:27:76	ARP	42	172.17.2.140 is at d8:9e:f3:12:d6:a7
232	4.124196	172.17.2.140	93.184.221.161	ICMP	74	Echo (ping) request id=0x0001, seq=35/8960, ttl=128 (reply in 237)
237	4.207876	93.184.221.161	172.17.2.140	ICMP	74	Echo (ping) reply id=0x0001, seq=35/8960, ttl=56 (request in 232)

```
> Frame 106: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{A2E487D7-0741-460A-9C
> Ethernet II, Src: Dell_12:d6:a7 (d8:9e:f3:12:d6:a7), Dst: Dell_7d:0e:2b (d4:ae:52:7d:0e:2b)
> Internet Protocol Version 4, Src: 172.17.2.140, Dst: 172.17.254.1
> User Datagram Protocol, Src Port: 50904, Dst Port: 53
> Domain Name System (query)
```

0000	d4 ae 52 7d 0e 2b d8 9e	f3 12 d6 a7 08 00 45 00	..R}+...E-
0010	00 3c 31 5c 00 00 80 11	00 00 ac 11 02 8c ac 11	<1\.....
0020	fe 01 c6 d8 00 35 00 28	58 ea b6 fc 01 00 00 015-(X.....
0030	00 00 00 00 00 00 03 77	77 77 07 61 63 2d 6e 69W ww.ac-ni
0040	63 65 02 66 72 00 00 01	00 01	ce.fr....

Quels sont les différents protocoles encapsulés dans une trame DNS ?

Dans une trame DNS on retrouve donc le champ ethertype IPv4, le protocole de transport Datagramme UDP ainsi que le protocole applicatif 00 35.

Quelle est la machine destinataire de la requête DNS ?

La machine destinataire de la requête DNS est le roteur qui contacte donc par la suite un serveur DNS.

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

172.17.254.1

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

Ils ont comme valeur 0800, ce qui signifie qu'ils représentent le champ Ethertype IPv4. Le 8ème octet représente la valeur 11 donc le Datagramme UDP.

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

Les octets 5 et 6 de la valeur 0020 ont la valeur 00 35 donc ils représentent à eux deux le port DNS 53.

> Ethernet II, Src: Dell_12:d6:a7 (d8:9e:f3:12:d6:a7), Dst: Dell_7d:0e:2b (d4:ae:52:7d:0e:2b)
> Internet Protocol Version 4, Src: 172.17.2.140, Dst: 172.17.254.1
> User Datagram Protocol, Src Port: 50904, Dst Port: 53
Domain Name System (query)
Transaction ID: 0xb6fc
> 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: 107]
0000 d4 ae 52 7d 0e 2b d8 9e f3 12 d6 a7 08 00 45 00 ..R}+.....E.
0010 00 3c 31 5c 00 00 80 11 00 00 ac 11 02 8c ac 11 .<1\.....
0020 fe 01 c6 d8 00 35 00 28 58 ea b6 fc 01 00 00 015.(X.....
0030 00 00 00 00 00 00 03 77 77 77 07 61 63 2d 6e 69w ww-ac-ni
0040 63 65 02 66 72 00 00 01 00 01 ce.fr....

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 acnice.fr ?

03 77 77 77 07 61 63 2d 6e 69 63 65 02 66 72 00 00 01 00 01

Sélectionnez la trame comportant la réponse à la requête 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 IP serveur web hébergeur en hexa : 5d b8 dd a1

Adresse IP serveur web hébergeur en deci : 93.184.221.161

3) Commande tracert et capture de trames ICMP

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

```
Détermination de l'itinéraire vers cs234.wpc.alphacdn.net [93.184.221.161]
avec un maximum de 30 sauts :
```

```
 1      1 ms    <1 ms    <1 ms  172.17.250.2
 2     35 ms    53 ms    78 ms  radius.lnput658.lnput658.rbc1.orange.net [80.10.115.220]
 3     88 ms    76 ms    91 ms  10.123.205.178
 4     35 ms    41 ms    35 ms  ae46-0.niidf201.rbc1.orange.net [193.252.98.249]
 5     34 ms    34 ms    37 ms  81.253.184.182
 6     33 ms    41 ms    41 ms  bundle-ether311.partr1.paris.opentransit.net [193.251.131.0]
 7     55 ms    56 ms    45 ms  verizondigitalmedia-11.gw.opentransit.net [193.251.255.52]
 8     34 ms    34 ms    34 ms  ae-65.core1.paa.edgecastcdn.net [152.195.108.129]
 9     33 ms    47 ms    66 ms  93.184.221.161
```

```
Itinéraire déterminé.
```

```
C:\WINDOWS\system32>
```

1ère étape: La commande tracert nous permet de connaître tous les routeurs se trouvant sur le chemin entre la machine locale qui effectue la commande et une destination donnée, comme dans notre cas ici présent avec le site internet de l'Académie de Nice.

*Ethernet

Fichier Editer Vue Aller Capture Analyser Statistiques Telephone Wireless Outils Aide

icmp

No.	Time	Source	Destination	Protocol	Length	Info
226	9.509347	172.17.2.140	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=37/9472, ttl=1 (no response found!)
227	9.510938	172.17.2.140	172.17.2.140	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
228	9.511326	172.17.2.140	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=38/9728, ttl=1 (no response found!)
229	9.512028	172.17.2.140	172.17.2.140	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
230	9.512368	172.17.2.140	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=39/9984, ttl=1 (no response found!)
231	9.513032	172.17.2.140	172.17.2.140	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
237	9.515313	172.17.2.140	172.17.2.140	ICMP	120	Destination unreachable (Port unreachable)
254	11.042168	172.17.2.140	172.17.2.140	ICMP	120	Destination unreachable (Port unreachable)
267	12.558649	172.17.2.140	172.17.2.140	ICMP	120	Destination unreachable (Port unreachable)
354	15.088308	172.17.2.140	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=40/10240, ttl=2 (no response found!)
362	15.123643	80.10.115.220	172.17.2.140	ICMP	94	Time-to-live exceeded (Time to live exceeded in transit)
363	15.124896	172.17.2.140	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=41/10496, ttl=2 (no response found!)
364	15.178488	80.10.115.220	172.17.2.140	ICMP	94	Time-to-live exceeded (Time to live exceeded in transit)
365	15.179710	172.17.2.140	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=42/10752, ttl=2 (no response found!)
366	15.258431	80.10.115.220	172.17.2.140	ICMP	94	Time-to-live exceeded (Time to live exceeded in transit)
375	16.197163	172.17.2.140	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=43/11008, ttl=3 (no response found!)
376	16.286097	10.123.205.178	172.17.2.140	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
377	16.287302	172.17.2.140	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=44/11264, ttl=3 (no response found!)
378	16.363278	10.123.205.178	172.17.2.140	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
379	16.364430	172.17.2.140	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=45/11520, ttl=3 (no response found!)
384	16.456292	10.123.205.178	172.17.2.140	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

```

> Frame 226: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface 0
> Ethernet II, Src: Dell_12:d6:a7 (d8:9e:f3:12:d6:a7), Dst: AnovFran_af:27:76 (08:26:6c:af:27:76)
> Internet Protocol Version 4, Src: 172.17.2.140, Dst: 93.184.221.161
> Internet Control Message Protocol

```

2ème étape: Ici nous avons donc démarrer une capture de trames en effectuant simultanément la commande tracert vue précédemment, et en saisissant dans la zone de filtre seulement les trames ICMP.

CaptureTracerert.pcapng

Fichier Editer Vue Aller Capture Analyser Statistiques Téléphonie Wireless Outils Aide

icmp

No.	Time	Source	Destination	Protocol	Length	Info
226	9.509347	172.17.2.140	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=37/9472, ttl=1 (no response found!)
227	9.510938	172.17.250.2	172.17.2.140	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
228	9.511326	172.17.2.140	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=38/9728, ttl=1 (no response found!)
229	9.512028	172.17.250.2	172.17.2.140	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
230	9.512368	172.17.2.140	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=39/9984, ttl=1 (no response found!)
231	9.513032	172.17.250.2	172.17.2.140	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
237	9.515313	172.17.250.2	172.17.2.140	ICMP	120	Destination unreachable (Port unreachable)
254	11.042168	172.17.250.2	172.17.2.140	ICMP	120	Destination unreachable (Port unreachable)
267	12.558649	172.17.250.2	172.17.2.140	ICMP	120	Destination unreachable (Port unreachable)
354	15.088308	172.17.2.140	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=40/10240, ttl=2 (no response found!)
362	15.123643	80.10.115.220	172.17.2.140	ICMP	94	Time-to-live exceeded (Time to live exceeded in transit)
363	15.124896	172.17.2.140	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=41/10496, ttl=2 (no response found!)

> Frame 226: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{A2E487D7-0741-460A-9C66-CD8B90433CD0}, id 0

> Ethernet II, Src: Dell_12:d6:a7 (d8:9e:f3:12:d6:a7), Dst: AIOVFran_af:27:76 (b8:26:6c:af:27:76)

Internet Protocol Version 4, Src: 172.17.2.140, Dst: 93.184.221.161

0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 92
Identification: 0x4dd1 (19921)
> Flags: 0x00
Fragment Offset: 0
> Time to Live: 1
Protocol: ICMP (1)
Header Checksum: 0x0000 [validation disabled]

```

0000 b8 26 6c af 27 76 d8 9e f3 12 d6 a7 08 00 45 00  &1.'v.....E.
0010 00 5c 4d d1 00 00 01 01 00 00 ac 11 02 8c 5d b8  .M.....].
0020 dd a1 08 00 f7 d9 00 01 00 25 00 00 00 00 00 00 00  .....%.....
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....

```

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

Deci : 93.184.221.161

Hexa : 5d b8 dd a1

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

La valeur portée par le champ TTL (Time to Live) est égal à 01 en hexa et donc 1 en décimal.

Développez la section correspondant au message ICMP. Quelle est la valeur portée par le champ Type (valeurs déci. et hexa.) ?

La valeur portée par le champ Type est 08 en hexa et 8 en décimal.

icmp						
No.	Time	Source	Destination	Protocol	Length	Info
226	9.509347	172.17.2.140	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=37/9472, ttl=1 (no response found!)
227	9.510938	172.17.250.2	172.17.2.140	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
228	9.511326	172.17.2.140	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=38/9728, ttl=1 (no response found!)
229	9.512028	172.17.250.2	172.17.2.140	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
230	9.512368	172.17.2.140	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=39/9984, ttl=1 (no response found!)
231	9.513032	172.17.250.2	172.17.2.140	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
237	9.515313	172.17.250.2	172.17.2.140	ICMP	120	Destination unreachable (Port unreachable)
254	11.042168	172.17.250.2	172.17.2.140	ICMP	120	Destination unreachable (Port unreachable)
267	12.558649	172.17.250.2	172.17.2.140	ICMP	120	Destination unreachable (Port unreachable)
354	15.088308	172.17.2.140	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=40/10240, ttl=2 (no response found!)
362	15.123643	80.10.115.220	172.17.2.140	ICMP	94	Time-to-live exceeded (Time to live exceeded in transit)
363	15.124896	172.17.2.140	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=41/10496, ttl=2 (no response found!)

> Frame 227: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits) on interface \Device\NPF_{A2E487D7-0741-460A-9C66-CD8B90433CD0}, id 0

> Ethernet II, Src: ANOVFran_af:27:76 (b8:26:6c:af:27:76), Dst: Dell_12:d6:a7 (d8:9e:f3:12:d6:a7)

> Internet Protocol Version 4, Src: 172.17.250.2, Dst: 172.17.2.140

Internet Control Message Protocol

Type: 11 (Time-to-live exceeded)
 Code: 0 (Time to live exceeded in transit)
 Checksum: 0xf4ff [correct]
 [Checksum Status: Good]
 Unused: 00000000

Internet Protocol Version 4, Src: 172.17.2.140, Dst: 93.184.221.161

0100 = Version: 4
 0101 = Header Length: 20 bytes (5)

Differentiated Services Field: 0x00 (DSFP: CS0, ECN: Not-ECT)

0000	d8 9e f3 12 d6 a7 b8 26	6c af 27 76 08 00 45 c0& 1.'v..E.
0010	00 78 f0 d2 00 00 40 01	34 41 ac 11 fa 02 ac 11	.x....@. 4A.....
0020	02 8c 0b 00 f4 ff 00 00	00 00 45 00 00 5c 4d d1E.. \M.
0030	00 00 01 01 81 d9 ac 11	02 8c 5d b8 dd a1 08 00].....
0040	f7 d9 00 01 00 25 00 00	00 00 00 00 00 00 00 00%.....
0050	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
0060	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
0070	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
0080	00 00 00 00 00 00 00 00		

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 (valeurs déci. et hexa.) ?

La valeur portée par le champ Type est cette fois-ci 11 en hexa et donc 17 en décimal.