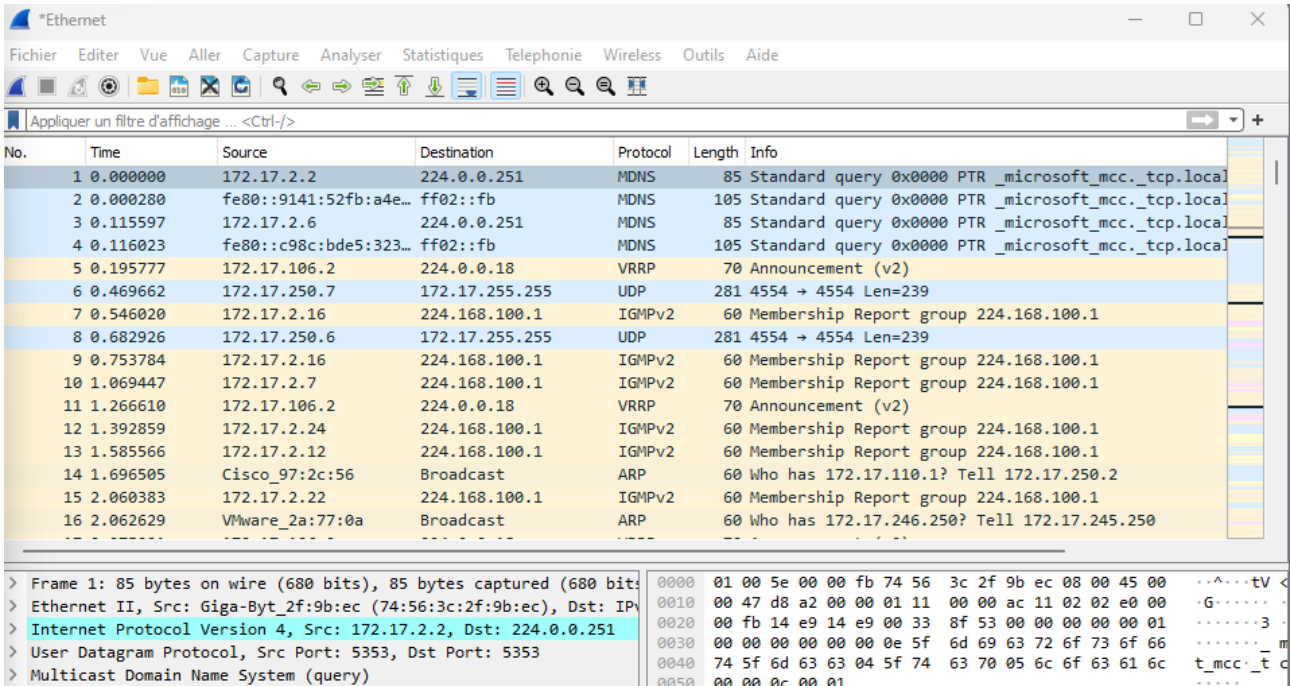


TP 5 – Trames ARP, ICMP et DNS

- 4.1. Capture de trames ARP et ICMP. 1
- 4.2. Capture de trames ARP, DNS et ICMP 3
- 4.3. Commande Tracert et capture de trames ICMP..... 5

4.1. Capture de trames ARP et ICMP.

- Ouvrez Wireshark et démarrez une capture de trames.



- Pinguez le serveur ROI (172.17.254.1). Effectuez une capture d’écran.

```
C:\Users\rcroquelois>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
Réponse de 172.17.254.1 : octets=32 temps<1ms TTL=128
Réponse de 172.17.254.1 : octets=32 temps<1ms TTL=128
Réponse de 172.17.254.1 : octets=32 temps=1 ms 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 = 1ms, Moyenne = 0ms
```

- L'échange démarre avec une requête et une réponse ARP pour obtenir l'adresse MAC du serveur ROI. Ensuite l'échange de trames ICMP a lieu. Arrêtez la capture une fois les 8 trames ICMP obtenues. Sauvegardez la sous le nom « CaptureICMP ».

Si vous ne visualisez pas d'échange ARP, videz le cache ARP (ouvrir une invite de commandes en tant qu'administrateur et saisir la commande arp -d *) puis recommencez une nouvelle capture et ressaisissez la commande ping.

```
C:\Windows\System32>arp -d *
C:\Windows\System32>arp -a

Interface : 172.17.2.2 --- 0xe
  Adresse Internet      Adresse physique      Type
  224.0.0.2             01-00-5e-00-00-02     statique

Interface : 192.168.56.1 --- 0x10
  Adresse Internet      Adresse physique      Type
  224.0.0.22            01-00-5e-00-00-16     statique

Interface : 172.23.48.1 --- 0x12
  Adresse Internet      Adresse physique      Type
```

- Après la saisie de la commande ping et la capture des trames ARP/ICMP, arrêtez cette dernière et consultez le contenu du cache ARP : vérifiez la présence de l'association @IP-@MAC correspondant à ROI (capture d'écran à réaliser).

| | | | | | |
|----|----------|-------------------|-------------------|------|---|
| 16 | 3.722684 | Giga-Byt_2f:9b:ec | Broadcast | ARP | 42 Who has 172.17.254.1? Tell 172.17.2.2 |
| 17 | 3.722862 | Dell_7d:0e:2b | Giga-Byt_2f:9b:ec | ARP | 60 172.17.254.1 is at d4:ae:52:7d:0e:2b |
| 18 | 3.722873 | 172.17.2.2 | 172.17.254.1 | ICMP | 74 Echo (ping) request id=0x0001, seq=53/13568, ttl=128 (re |
| 19 | 3.723104 | 172.17.254.1 | 172.17.2.2 | ICMP | 74 Echo (ping) reply id=0x0001, seq=53/13568, ttl=128 (re |
| 21 | 4.386749 | VWware_2a:77:0a | Broadcast | ARP | 60 Who has 172.17.246.250? Tell 172.17.245.250 |
| 24 | 4.728929 | 172.17.2.2 | 172.17.254.1 | ICMP | 74 Echo (ping) request id=0x0001, seq=54/13824, ttl=128 (re |
| 25 | 4.729228 | 172.17.254.1 | 172.17.2.2 | ICMP | 74 Echo (ping) reply id=0x0001, seq=54/13824, ttl=128 (re |
| 30 | 5.413464 | VWware_2a:77:0a | Broadcast | ARP | 60 Who has 172.17.246.250? Tell 172.17.245.250 |
| 33 | 5.741179 | 172.17.2.2 | 172.17.254.1 | ICMP | 74 Echo (ping) request id=0x0001, seq=55/14080, ttl=128 (re |
| 34 | 5.741486 | 172.17.254.1 | 172.17.2.2 | ICMP | 74 Echo (ping) reply id=0x0001, seq=55/14080, ttl=128 (re |
| 35 | 6.437403 | VWware_2a:77:0a | Broadcast | ARP | 60 Who has 172.17.246.250? Tell 172.17.245.250 |
| 37 | 6.758314 | 172.17.2.2 | 172.17.254.1 | ICMP | 74 Echo (ping) request id=0x0001, seq=56/14336, ttl=128 (re |
| 38 | 6.758991 | 172.17.254.1 | 172.17.2.2 | ICMP | 74 Echo (ping) reply id=0x0001, seq=56/14336, ttl=128 (re |
| 40 | 7.461570 | VWware_2a:77:0a | Broadcast | ARP | 60 Who has 172.17.246.250? Tell 172.17.245.250 |

- A l'aide du Chapitre 5 (page 2), analysez l'échange de trames ARP (Request et Reply) précédant l'échange de trames ICMP :

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

Ici on peut voir que les octets de position 0x0C et 0x0D sont le champ Ethertype et la valeur est 0806 ce qui signifie que c'est le protocole ARP

Quelle est la fonction de la trame ARP Request ?

La trame ARP request sert à demander l'adresse MAC d'une machine dont on connaît l'adresse IP.

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

Ici les octets de position 0x04 et 0x05 sont la requête.

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

28 octets

Quelle est la longueur de la trame ARP Request ?

42 octets

Quelle est la longueur de la trame ARP Reply ?

60 octets

Combien d'octets sont utilisés pour le padding ?

18 octets

▪ Complétez les rubriques ci-dessous :

| Trame ARP Request |
|--|
| @MAC destination = ff: ff: ff: ff: ff: ff @MAC source = 74: 56: 3c: 2f: 9b: ec Ethernet Type = 0806 |
| Opcode (valeurs hexa.) =00 01 @MAC de la cible = 00 : 00 : 00 : 00 : 00 : 00 @IP de la cible =172.17.254.1 |

▪ Sélectionnez une trame ICMP Echo Request. A l'aide du Chapitre 5 (pages 4 et 5), répondez aux questions suivantes :

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

Les octets de position 0x0C et 0x0D sont 08 00 ce qui veut dire que c'est le protocole IPv4.

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

L'octet de position 0x07 est 01 ce qui veut dire que c'est le protocole ICMP.

Quelle est la longueur de la trame ?

74 octets

Quelle est la longueur du paquet IP ?

20 octets

Quelle est la longueur du message ICMP ?

40 octets

Quelle signification a l'octet de position 0x02 ligne 00020 ?

L'octet de position 0x02 est ici 08 qui est le Type de ICMP qui correspond ici au ping request.

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

Les octets à partir de l'octet 0x0A sont les Data.

▪ Sélectionnez une trame ICMP Echo Reply. Quelle est le nom et la valeur de l'octet de position 0x02 ligne 00020 ?

L'octet de position 0x02 est 00 qui est également le Type de ICMP qui est ici le ping reply.

4.2. Capture de trames ARP, DNS et ICMP

▪ Démarrez une capture de trames depuis votre machine physique.

- Ouvrez une invite de commandes, videz le cache ARP (commande arp -d *) puis effectuez une requête ping vers le serveur web www.ac-nice.fr (ping « nom » et non plus ping « @IP ») :

```
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=67 ms TTL=56
Réponse de 93.184.221.161 : octets=32 temps=32 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 = 32ms, Maximum = 67ms, Moyenne = 40ms
```

- Arrêtez la capture et sauvegardez la sous le nom « CaptureIcmpDns »

| | | | | | |
|----|-----------|-------------------|-------------------|------|--|
| 35 | 3.244129 | 172.17.2.2 | 172.17.254.1 | DNS | 74 Standard query 0x44c6 A www.ac-nice.fr |
| 36 | 3.244424 | 172.17.254.1 | 172.17.2.2 | DNS | 126 Standard query response 0x44c6 A www.ac-nice.fr CN |
| 37 | 3.251351 | Giga-Byt_2f:9b:ec | Broadcast | ARP | 42 Who has 172.17.250.2? Tell 172.17.2.2 |
| 38 | 3.251499 | Cisco_97:2c:56 | Giga-Byt_2f:9b:ec | ARP | 60 172.17.250.2 is at 00:1f:ca:97:2c:56 |
| 39 | 3.251509 | 172.17.2.2 | 93.184.221.161 | ICMP | 74 Echo (ping) request id=0x0001, seq=113/28928, ttl= |
| 40 | 3.283614 | 93.184.221.161 | 172.17.2.2 | ICMP | 74 Echo (ping) reply id=0x0001, seq=113/28928, ttl= |
| 45 | 4.168866 | VNware_6c:9c:3e | Broadcast | ARP | 60 Who has 128.0.255.0? Tell 128.0.3.1 |
| 47 | 4.264875 | 172.17.2.2 | 93.184.221.161 | ICMP | 74 Echo (ping) request id=0x0001, seq=114/29184, ttl= |
| 48 | 4.326497 | 93.184.221.161 | 172.17.2.2 | ICMP | 74 Echo (ping) reply id=0x0001, seq=114/29184, ttl= |
| 49 | 4.817840 | VNware_6c:9c:3e | Broadcast | ARP | 60 Who has 128.0.255.0? Tell 128.0.3.1 |
| 51 | 5.278235 | 172.17.2.2 | 93.184.221.161 | ICMP | 74 Echo (ping) request id=0x0001, seq=115/29440, ttl= |
| 52 | 5.350459 | 93.184.221.161 | 172.17.2.2 | ICMP | 74 Echo (ping) reply id=0x0001, seq=115/29440, ttl= |
| 53 | 5.502554 | VNware_2a:77:0a | Broadcast | ARP | 60 Who has 172.17.246.250? Tell 172.17.245.250 |
| 54 | 5.661811 | Giga-Byt_2f:9c:f0 | Broadcast | ARP | 60 Who has 172.17.250.2? Tell 172.17.2.21 |
| 55 | 5.817511 | VNware_6c:9c:3e | Broadcast | ARP | 60 Who has 128.0.255.0? Tell 128.0.3.1 |
| 57 | 6.287574 | 172.17.2.2 | 93.184.221.161 | ICMP | 74 Echo (ping) request id=0x0001, seq=116/29696, ttl= |
| 58 | 6.369241 | 93.184.221.161 | 172.17.2.2 | ICMP | 74 Echo (ping) reply id=0x0001, seq=116/29696, ttl= |
| 59 | 6.517946 | VNware_2a:77:0a | Broadcast | ARP | 60 Who has 172.17.246.250? Tell 172.17.245.250 |
| 63 | 7.541980 | VNware_2a:77:0a | Broadcast | ARP | 60 Who has 172.17.246.250? Tell 172.17.245.250 |
| 66 | 8.565979 | VNware_2a:77:0a | Broadcast | ARP | 60 Who has 172.17.246.250? Tell 172.17.245.250 |
| 69 | 9.590184 | VNware_2a:77:0a | Broadcast | ARP | 60 Who has 172.17.246.250? Tell 172.17.245.250 |
| 70 | 10.034307 | Giga-Byt_2f:7b:46 | Broadcast | ARP | 60 Who has 172.17.2.20? Tell 172.17.2.24 |


```
> Frame 6: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
> Ethernet II, Src: VNware_2a:77:0a (00:0c:29:2a:77:0a), Dst: Broadcast
> Address Resolution Protocol (request)
0000 ff ff ff ff ff ff 00 0c 29 2a 77 0a 08 06 00 01 .....
0010 08 00 06 04 00 01 00 0c 29 2a 77 0a ac 11 f5 fa .....
0020 00 00 00 00 00 00 ac 11 f6 fa 00 00 00 00 00 00 .....
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
```

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

Ici c'est celle de www.ac-nice.fr.

- Complétez les rubriques ci-dessous :

| |
|--|
| Trame ARP request |
| @MAC destination = ff : ff : ff : ff : ff : ff |
| @MAC source = 74: 56: 3c: 2f: 9b: ec |

| |
|--|
| Ethernet Type = 0806 |
| Opcode (valeurs hexa.) = 00 01 |
| @MAC de la cible = 00 : 00 : 00 : 00 : 00 : 00 |
| @IP de la cible = 172.17.254.1 |

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

C'est pour pouvoir connaître l'adresse IP de www.ac-nice.fr.

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

```
www.ac-nice.fr
-----
Nom d'enregistrement. : www.ac-nice.fr
Type d'enregistrement : 5
Durée de vie . . . . . : 2830
Longueur de données . : 8
Section . . . . . : Réponse
Enregistrement CNAME : cs234.wpc.alphacdn.net

Nom d'enregistrement. : cs234.wpc.alphacdn.net
Type d'enregistrement : 1
Durée de vie . . . . . : 2830
Longueur de données . : 4
Section . . . . . : Réponse
Enregistrement (hôte) : 93.184.221.161
```

- Démarrez une nouvelle capture et ressaisissez la commande `ping www.ac-nice.fr` dans l'invite de commandes. Vous ne devriez pas constater de requête DNS puisque l'enregistrement est présent dans le cache DNS.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------|-------------------|-------------------|----------|--------|--|
| 56 | 6.126504 | Vmware_2a:77:0a | Broadcast | ARP | 60 | Who has 172.17.246.250? Tell 172.17.245.250 |
| 59 | 7.137721 | Giga-Byt_2f:9d:13 | Broadcast | ARP | 60 | Who has 172.17.110.19? Tell 172.17.2.13 |
| 60 | 7.150299 | Vmware_2a:77:0a | Broadcast | ARP | 60 | Who has 172.17.246.250? Tell 172.17.245.250 |
| 69 | 7.879767 | Giga-Byt_2f:9b:ec | Broadcast | ARP | 42 | Who has 172.17.250.2? Tell 172.17.2.2 |
| 70 | 7.879938 | Cisco_97:2c:56 | Giga-Byt_2f:9b:ec | ARP | 60 | 172.17.250.2 is at 00:1f:ca:97:2c:56 |
| 71 | 7.879949 | 172.17.2.2 | 93.184.221.161 | ICMP | 74 | Echo (ping) request id=0x0001, seq=101/25856, ttl= |
| 73 | 7.912871 | 93.184.221.161 | 172.17.2.2 | ICMP | 74 | Echo (ping) reply id=0x0001, seq=101/25856, ttl= |
| 74 | 8.174297 | Vmware_2a:77:0a | Broadcast | ARP | 60 | Who has 172.17.246.250? Tell 172.17.245.250 |
| 78 | 8.892407 | 172.17.2.2 | 93.184.221.161 | ICMP | 74 | Echo (ping) request id=0x0001, seq=102/26112, ttl= |
| 79 | 8.925035 | 93.184.221.161 | 172.17.2.2 | ICMP | 74 | Echo (ping) reply id=0x0001, seq=102/26112, ttl= |
| 83 | 9.908808 | 172.17.2.2 | 93.184.221.161 | ICMP | 74 | Echo (ping) request id=0x0001, seq=103/26368, ttl= |
| 84 | 9.958855 | 93.184.221.161 | 172.17.2.2 | ICMP | 74 | Echo (ping) reply id=0x0001, seq=103/26368, ttl= |
| 85 | 9.971379 | Giga-Byt_2f:9d:13 | Broadcast | ARP | 60 | Who has 172.17.110.19? Tell 172.17.2.13 |
| 90 | 10.627814 | Giga-Byt_2f:9d:13 | Broadcast | ARP | 60 | Who has 172.17.110.19? Tell 172.17.2.13 |
| 91 | 10.911446 | 172.17.2.2 | 93.184.221.161 | ICMP | 74 | Echo (ping) request id=0x0001, seq=104/26624, ttl= |
| 92 | 10.958390 | 93.184.221.161 | 172.17.2.2 | ICMP | 74 | Echo (ping) reply id=0x0001, seq=104/26624, ttl= |
| 96 | 11.639406 | Giga-Byt_2f:9d:13 | Broadcast | ARP | 60 | Who has 172.17.110.19? Tell 172.17.2.13 |
| 99 | 13.069823 | Vmware_2a:77:0a | Broadcast | ARP | 60 | Who has 172.17.246.250? Tell 172.17.245.250 |
| 104 | 13.563950 | Vmware_6c:9c:3e | Broadcast | ARP | 60 | Who has 128.0.255.0? Tell 128.0.3.1 |
| 109 | 13.971833 | Giga-Byt_2f:9d:13 | Broadcast | ARP | 60 | Who has 172.17.110.19? Tell 172.17.2.13 |

• Videz le cache DNS à l'aide de la commande ipconfig /flushdns et redémarrez une nouvelle capture afin de visualiser de nouveau une requête DNS (capture d'écran à faire) :

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|-----------------------|-----------------------|----------|--------|---|
| 6 | 0.598015 | Vmware_2a:77:0a | Broadcast | ARP | 60 | Who has 172.17.246.250? Tell 172.17.245.250 |
| 11 | 1.779560 | GigaByteTech_2f:9b:ec | Broadcast | ARP | 42 | Who has 172.17.254.1? Tell 172.17.2.2 |
| 12 | 1.779761 | Dell_7d:0e:2b | GigaByteTech_2f:9b:ec | ARP | 60 | 172.17.254.1 is at d4:ae:52:7d:0e:2b |
| 13 | 1.779771 | 172.17.2.2 | 172.17.254.1 | DNS | 76 | Standard query 0xa09d A roi.prince.local |
| 14 | 1.780036 | 172.17.254.1 | 172.17.2.2 | DNS | 92 | Standard query response 0xa09d A roi.prince.local A 172.17.254.1 |
| 35 | 3.244129 | 172.17.2.2 | 172.17.254.1 | DNS | 74 | Standard query 0x44c6 A www.ac-nice.fr |
| 36 | 3.244424 | 172.17.254.1 | 172.17.2.2 | DNS | 126 | Standard query response 0x44c6 A www.ac-nice.fr CNAME cs234.wpc.alphacdn.net A 93.184.221.161 |
| 37 | 3.251351 | GigaByteTech_2f:9b:ec | Broadcast | ARP | 42 | Who has 172.17.250.2? Tell 172.17.2.2 |
| 38 | 3.251499 | Cisco_97:2c:56 | GigaByteTech_2f:9b:ec | ARP | 60 | 172.17.250.2 is at 00:1f:ca:97:2c:56 |
| 39 | 3.251509 | 172.17.2.2 | 93.184.221.161 | ICMP | 74 | Echo (ping) request id=0x0001, seq=113/28928, ttl=128 (reply in 40) |
| 40 | 3.283614 | 93.184.221.161 | 172.17.2.2 | ICMP | 74 | Echo (ping) reply id=0x0001, seq=113/28928, ttl=56 (request in 39) |
| 45 | 4.168866 | Vmware_6c:9c:3e | Broadcast | ARP | 60 | Who has 128.0.255.0? Tell 128.0.3.1 |
| 47 | 4.264875 | 172.17.2.2 | 93.184.221.161 | ICMP | 74 | Echo (ping) request id=0x0001, seq=114/29184, ttl=128 (reply in 48) |
| 48 | 4.326497 | 93.184.221.161 | 172.17.2.2 | ICMP | 74 | Echo (ping) reply id=0x0001, seq=114/29184, ttl=56 (request in 47) |
| 49 | 4.817840 | Vmware_6c:9c:3e | Broadcast | ARP | 60 | Who has 128.0.255.0? Tell 128.0.3.1 |
| 51 | 5.278235 | 172.17.2.2 | 93.184.221.161 | ICMP | 74 | Echo (ping) request id=0x0001, seq=115/29440, ttl=128 (reply in 52) |
| 52 | 5.350459 | 93.184.221.161 | 172.17.2.2 | ICMP | 74 | Echo (ping) reply id=0x0001, seq=115/29440, ttl=56 (request in 51) |
| 53 | 5.502554 | Vmware_2a:77:0a | Broadcast | ARP | 60 | Who has 172.17.246.250? Tell 172.17.245.250 |

Frame 35: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface {Device\NPF_{A6A9C54A-A1CD-4F5E-A7DE-FE996EB45D98}, id 0

Ethernet II, Src: GigaByteTech_2f:9b:ec (74:56:3c:2f:9b:ec), Dst: Dell_7d:0e:2b (d4:ae:52:7d:0e:2b)

Destination: Dell_7d:0e:2b (d4:ae:52:7d:0e:2b)

Source: GigaByteTech_2f:9b:ec (74:56:3c:2f:9b:ec)

Type: IPv4 (0x0800)

[Stream index: 0]

Internet Protocol Version 4, Src: 172.17.2.2, Dst: 172.17.254.1

User Datagram Protocol, Src Port: 52027, Dst Port: 53

Source Port: 52027

Destination Port: 53

Length: 40

Checksum: 0x5860 [unverified]

[Checksum Status: Unverified]

[Stream index: 1]

[Stream Packet Number: 3]

[Timestamps]

UDP payload (32 bytes)

Domain Name System (query)

Transaction ID: 0x44c6

Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

Queries

- www.ac-nice.fr: type A, class IN
 - Name: www.ac-nice.fr
 - [Name Length: 14]
 - [Label Count: 3]
 - Type: A (1) (Host Address)
 - Class: IN (0x0001)

[Response in: 36]

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

Ici ce sont les protocoles IPv4 et UDP.

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

La machine destinataire de la requête DNS sera le serveur ROI qui a comme IP 172.17.254.1

- Quelle signification ont les octets de position 0×0C, 0×0D ligne 0000 et 0×07 ligne 0010 ?

Les octets de position 0×0C et 0×0D appartiennent au champ Ethertype qui sont 08 00 ce qui veut dire que nous sommes sous IPv4 et l'octet 0×07 qui appartient au champ réseau et qui est 11 ce qui veut dire que nous sommes sous UDP.

- Quelle signification ont les octets de position 0×04 et 0×05 ligne 0020 ?

Les octets de position 0×04 et 0×05 sont 00 35 qui sont le port de destination. Ce qui correspond au 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 acnice.fr ?

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

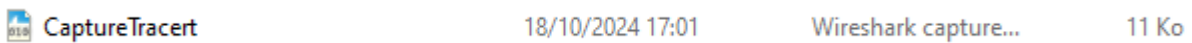
- Sélectionnez la trame comportant la réponse à la requête DNS et développez la section Domain Name System (response) et plus particulièrement la rubrique Answers. Recherchez les valeurs hexadécimales et décimales de l'adresse IP du serveur web hébergeant le site de l'académie de Nice.

Les valeurs hexa sont c0 2c 00 01 00 01 00 00 09 be 00 01 5d b8 dd a1.

Et l'adresse IP est 93.184.221.161

4.3. Commande Tracert et capture de trames ICMP.

- Démarrez une capture de trames depuis votre machine physique.
- Ouvrez une invite de commandes et saisissez la commande tracert www.ac-nice.fr.
- Une fois l’itinéraire déterminé, arrêtez la capture et sauvegardez la sous le nom « CaptureTracert ».



- Limitez l’affichage des trames à celles encapsulant le protocole ICMP (zone Filter) :

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------|----------------|----------------|----------|--------|---|
| 5 | 0.193416 | 192.168.187.46 | 93.184.221.161 | ICMP | 106 | Echo (ping) request id=0x0001, seq=268/3073, ttl=3 |
| 6 | 3.741066 | 192.168.187.46 | 93.184.221.161 | ICMP | 106 | Echo (ping) request id=0x0001, seq=269/3329, ttl=3 |
| 9 | 7.741820 | 192.168.187.46 | 93.184.221.161 | ICMP | 106 | Echo (ping) request id=0x0001, seq=270/3585, ttl=3 |
| 10 | 11.741795 | 192.168.187.46 | 93.184.221.161 | ICMP | 106 | Echo (ping) request id=0x0001, seq=271/3841, ttl=3 |
| 11 | 15.746932 | 192.168.187.46 | 93.184.221.161 | ICMP | 106 | Echo (ping) request id=0x0001, seq=272/4097, ttl=3 |
| 12 | 19.746598 | 192.168.187.46 | 93.184.221.161 | ICMP | 106 | Echo (ping) request id=0x0001, seq=273/4353, ttl=3 |
| 19 | 23.745570 | 192.168.187.46 | 93.184.221.161 | ICMP | 106 | Echo (ping) request id=0x0001, seq=274/4609, ttl=3 |
| 20 | 23.843371 | 10.2.0.123 | 192.168.187.46 | ICMP | 70 | Time-to-live exceeded (Time to live exceeded in tra |
| 21 | 23.844068 | 192.168.187.46 | 93.184.221.161 | ICMP | 106 | Echo (ping) request id=0x0001, seq=275/4865, ttl=3 |
| 22 | 23.915607 | 10.2.0.123 | 192.168.187.46 | ICMP | 70 | Time-to-live exceeded (Time to live exceeded in tra |
| 23 | 23.916374 | 192.168.187.46 | 93.184.221.161 | ICMP | 106 | Echo (ping) request id=0x0001, seq=276/5121, ttl=3 |
| 24 | 23.948526 | 10.2.0.123 | 192.168.187.46 | ICMP | 70 | Time-to-live exceeded (Time to live exceeded in tra |
| 29 | 25.417846 | 192.168.187.46 | 93.184.221.161 | ICMP | 106 | Echo (ping) request id=0x0001, seq=277/5377, ttl=4 |
| 30 | 29.240528 | 192.168.187.46 | 93.184.221.161 | ICMP | 106 | Echo (ping) request id=0x0001, seq=278/5633, ttl=4 |
| 31 | 29.299261 | 10.202.226.1 | 192.168.187.46 | ICMP | 70 | Time-to-live exceeded (Time to live exceeded in tra |
| 32 | 29.300117 | 192.168.187.46 | 93.184.221.161 | ICMP | 106 | Echo (ping) request id=0x0001, seq=279/5889, ttl=4 |
| 33 | 29.337973 | 10.202.226.1 | 192.168.187.46 | ICMP | 70 | Time-to-live exceeded (Time to live exceeded in tra |
| 36 | 30.735619 | 192.168.187.46 | 93.184.221.161 | ICMP | 106 | Echo (ping) request id=0x0001, seq=280/6145, ttl=5 |
| 37 | 30.790785 | 194.6.143.75 | 192.168.187.46 | ICMP | 70 | Time-to-live exceeded (Time to live exceeded in tra |
| 38 | 30.791512 | 192.168.187.46 | 93.184.221.161 | ICMP | 106 | Echo (ping) request id=0x0001, seq=281/6401, ttl=5 |
| 39 | 30.818125 | 194.6.143.75 | 192.168.187.46 | ICMP | 70 | Time-to-live exceeded (Time to live exceeded in tra |
| 40 | 30.818691 | 192.168.187.46 | 93.184.221.161 | ICMP | 106 | Echo (ping) request id=0x0001, seq=282/6657, ttl=5 |
| 41 | 30.839893 | 194.6.143.75 | 192.168.187.46 | ICMP | 70 | Time-to-live exceeded (Time to live exceeded in tra |
| 42 | 31.828253 | 192.168.187.46 | 93.184.221.161 | ICMP | 106 | Echo (ping) request id=0x0001, seq=283/6913, ttl=6 |
| 43 | 31.884995 | 194.6.145.252 | 192.168.187.46 | ICMP | 70 | Time-to-live exceeded (Time to live exceeded in tra |
| 44 | 31.886114 | 192.168.187.46 | 93.184.221.161 | ICMP | 106 | Echo (ping) request id=0x0001, seq=284/7169, ttl=6 |
| 45 | 31.910843 | 194.6.145.252 | 192.168.187.46 | ICMP | 70 | Time-to-live exceeded (Time to live exceeded in tra |
| 46 | 31.911689 | 192.168.187.46 | 93.184.221.161 | ICMP | 106 | Echo (ping) request id=0x0001, seq=285/7425, ttl=6 |
| 47 | 31.939705 | 194.6.145.252 | 192.168.187.46 | ICMP | 70 | Time-to-live exceeded (Time to live exceeded in tra |
| 48 | 32.920693 | 192.168.187.46 | 93.184.221.161 | ICMP | 106 | Echo (ping) request id=0x0001, seq=286/7681, ttl=7 |
| 49 | 32.990155 | 37.77.39.138 | 192.168.187.46 | ICMP | 70 | Time-to-live exceeded (Time to live exceeded in tra |
| 50 | 32.998857 | 192.168.187.46 | 93.184.221.161 | ICMP | 106 | Echo (ping) request id=0x0001, seq=287/7937, ttl=7 |
| 51 | 33.018341 | 37.77.39.138 | 192.168.187.46 | ICMP | 70 | Time-to-live exceeded (Time to live exceeded in tra |
| 52 | 33.018930 | 192.168.187.46 | 93.184.221.161 | ICMP | 106 | Echo (ping) request id=0x0001, seq=288/8193, ttl=7 |
| 53 | 33.048541 | 37.77.39.138 | 192.168.187.46 | ICMP | 70 | Time-to-live exceeded (Time to live exceeded in tra |
| 54 | 34.037204 | 192.168.187.46 | 93.184.221.161 | ICMP | 106 | Echo (ping) request id=0x0001, seq=289/8449, ttl=8 |
| 55 | 34.143005 | 37.77.39.141 | 192.168.187.46 | ICMP | 70 | Time-to-live exceeded (Time to live exceeded in tra |
| 56 | 34.143705 | 192.168.187.46 | 93.184.221.161 | ICMP | 106 | Echo (ping) request id=0x0001, seq=290/8705, ttl=8 |
| 57 | 34.179478 | 37.77.39.141 | 192.168.187.46 | ICMP | 70 | Time-to-live exceeded (Time to live exceeded in tra |
| 58 | 34.180323 | 192.168.187.46 | 93.184.221.161 | ICMP | 106 | Echo (ping) request id=0x0001, seq=291/8961, ttl=8 |
| 59 | 34.209514 | 37.77.39.141 | 192.168.187.46 | ICMP | 70 | Time-to-live exceeded (Time to live exceeded in tra |
| 60 | 35.197304 | 192.168.187.46 | 93.184.221.161 | ICMP | 106 | Echo (ping) request id=0x0001, seq=292/9217, ttl=8 |
| 61 | 35.319132 | 64.12.68.129 | 192.168.187.46 | ICMP | 70 | Time-to-live exceeded (Time to live exceeded in tra |
| 62 | 35.319868 | 192.168.187.46 | 93.184.221.161 | ICMP | 106 | Echo (ping) request id=0x0001, seq=293/9473, ttl=8 |
| 63 | 35.384109 | 64.12.68.129 | 192.168.187.46 | ICMP | 70 | Time-to-live exceeded (Time to live exceeded in tra |
| 64 | 35.384828 | 192.168.187.46 | 93.184.221.161 | ICMP | 106 | Echo (ping) request id=0x0001, seq=294/9729, ttl=8 |
| 65 | 35.422968 | 64.12.68.129 | 192.168.187.46 | ICMP | 70 | Time-to-live exceeded (Time to live exceeded in tra |
| 68 | 36.808911 | 192.168.187.46 | 93.184.221.161 | ICMP | 106 | Echo (ping) request id=0x0001, seq=295/9985, ttl=1 |

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

L'adresse IP destination en décimale est 93.184.221.161 et en hexadécimale c'est 5d b8 dd a1.

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

La valeur déci du champ TTL est 1 et en hexa c'est 01.

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

La valeur du champ Type en déci. est 8 et en hexa sa valeur est 08.

- 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 du champ Type est 11 en déci et 0b en hexa.