

## TP 3 - Analyse de flux TCP/IP

On se sert d'un poste de travail à l'Efrei, sur une VM Debian.

### 1. Analyse de trames

#### 1.2.1. Capture de flux associés à la commande ping

The screenshot displays the Wireshark interface with the following details:

- Filter:** (Empty)
- Packet List:**

No.	Time	Source	Destination	Protocol	Length	Info
2	2.001722000	10.0.2.15	91.121.34.166	NIP	90	NIP Version 4, client
3	2.007118000	CadmusCo_c0:ec:59	RealtekU_12:35:02	ARP	42	Who has 10.0.2.2? Tell 10.0.2.
4	2.007324000	RealtekU_12:35:02	CadmusCo_c0:ec:59	ARP	60	10.0.2.2 is at 52:54:00:12:35:(
5	13.000638000	10.0.2.15	178.32.216.71	NTP	90	NTP Version 4, client
6	14.548901000	10.0.2.15	192.102.224.41	ICMP	98	Echo (ping) request id=0x0923,
7	14.549900000	192.102.224.41	10.0.2.15	ICMP	98	Echo (ping) reply id=0x0923,
8	15.557436000	10.0.2.15	192.102.224.41	ICMP	98	Echo (ping) request id=0x0923,
9	15.558312000	192.102.224.41	10.0.2.15	ICMP	98	Echo (ping) reply id=0x0923,
10	16.556435000	10.0.2.15	192.102.224.41	ICMP	98	Echo (ping) request id=0x0923,
11	16.557409000	192.102.224.41	10.0.2.15	ICMP	98	Echo (ping) reply id=0x0923,
- Packet 11 Details:**
  - Frame 11: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
  - Ethernet II, Src: RealtekU\_12:35:02 (52:54:00:12:35:02), Dst: CadmusCo\_c0:ec:59 (08:00:27:c0:ec:59)
    - Destination: CadmusCo\_c0:ec:59 (08:00:27:c0:ec:59)
      - Address: CadmusCo\_c0:ec:59 (08:00:27:c0:ec:59)
      - .....0. .... = LG bit: Globally unique address (factory default)
      - .....0 .... = IG bit: Individual address (unicast)
    - Source: RealtekU\_12:35:02 (52:54:00:12:35:02)
      - Address: RealtekU\_12:35:02 (52:54:00:12:35:02)
- Packet Bytes:**

```

0000 08 00 27 c0 ec 59 52 54 00 12 35 02 08 00 45 00  ..'.YRT ..5...E.
0010 00 54 14 57 00 00 3e 01 bb b3 c0 66 e0 29 0a 00  .T.W...>. ...f.)..
0020 02 0f 00 00 1f fb 09 23 00 03 58 80 8b 56 00 00  .....# ..X..V..
0030 00 00 2d 35 07 00 00 00 00 00 10 11 12 13 14 15  ...-5.... ....
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25  ..... .. !"#4%
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35  &'()*+,- ./012345
0060 36 37 67
    
```

### 1.2.2 Capture de flux associés à la commande ping

The screenshot shows a Wireshark capture of network traffic on the interface \*eth0. The capture contains 35 packets. The first four packets are DNS queries and responses between 10.0.2.15 and 10.0.1.1. The next 15 packets (5-15) are UDP traffic from 10.0.2.15 to 23.206.41.209, with source ports ranging from 42414 to 35854 and destination ports from 33434 to 33444. Packet 16 is an ICMP Echo (ping) request from 10.0.2.2 to 10.0.2.15. Packet 17 is a UDP response from 23.206.41.209 to 10.0.2.15, source port 52157, destination port 33445. Packet 18 is an ICMP Echo (ping) request from 10.0.2.2 to 10.0.2.15. Packet 19 is an ICMP Echo (ping) response from 10.0.2.15 to 10.0.2.2. The bottom pane shows the raw data for packet 19, including the Ethernet II header and the IP header with destination address 10.0.2.2.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.15	10.0.1.1	DNS	73	Standard query 0xf55d A www.cisco.com
2	0.000186000	10.0.2.15	10.0.1.1	DNS	73	Standard query 0x15d7 AAAA www.cisco.com
3	0.123963000	10.0.1.1	10.0.2.15	DNS	550	Standard query response 0xf55d CNAME www.cisco.com
4	0.124010000	10.0.1.1	10.0.2.15	DNS	542	Standard query response 0x15d7 CNAME www.cisco.com
5	0.124567000	10.0.2.15	23.206.41.209	UDP	74	Source port: 42414 Destination port: 33434
6	0.124628000	10.0.2.15	23.206.41.209	UDP	74	Source port: 33809 Destination port: 33435
7	0.124670000	10.0.2.15	23.206.41.209	UDP	74	Source port: 35557 Destination port: 33436
8	0.124734000	10.0.2.15	23.206.41.209	UDP	74	Source port: 49955 Destination port: 33437
9	0.124780000	10.0.2.15	23.206.41.209	UDP	74	Source port: 48464 Destination port: 33438
10	0.124834000	10.0.2.15	23.206.41.209	UDP	74	Source port: 56964 Destination port: 33439
11	0.124896000	10.0.2.15	23.206.41.209	UDP	74	Source port: 54702 Destination port: 33440
12	0.124964000	10.0.2.15	23.206.41.209	UDP	74	Source port: 38507 Destination port: 33441
13	0.125104000	10.0.2.15	23.206.41.209	UDP	74	Source port: 41977 Destination port: 33442
14	0.125170000	10.0.2.15	23.206.41.209	UDP	74	Source port: 59402 Destination port: 33443
15	0.125216000	10.0.2.15	23.206.41.209	UDP	74	Source port: 35854 Destination port: 33444
16	0.125263000	10.0.2.2	10.0.2.15	ICMP	70	Time-to-live exceeded (Time to live exceeded)
17	0.125272000	10.0.2.15	23.206.41.209	UDP	74	Source port: 52157 Destination port: 33445
18	0.125287000	10.0.2.2	10.0.2.15	ICMP	70	Time-to-live exceeded (Time to live exceeded)
19	0.125291000	10.0.2.2	10.0.2.15	ICMP	70	Time-to-live exceeded (Time to live exceeded)

Address: RealtekU\_12:35:02 (52:54:00:12:35:02)  
 .... .1. .... = LG bit: Locally administered address (this is NOT the factory default)

```

0000 52 54 00 12 35 02 08 00 27 c0 ec 59 08 00 45 00  RT..S... '..Y..E.
0010 00 3b 5d 89 40 00 40 11 c6 19 0a 00 02 0f 0a 00  .;].@.@. ....
0020 01 01 c8 50 00 35 00 27 17 48 f5 5d 01 00 00 01  ...P.S'.H.]....
0030 00 00 00 00 00 00 03 77 77 77 05 63 69 73 63 6f  ....w ww.cisco
0040 03 63 6f 6d 00 00 01 00 01                               .com....
    
```

File: "/tmp/wireshark\_pcapng\_e... Packets: 35 · Displayed: 35 (100,0%) · Dropped: 0 (0,0%) Profile: Default

### 1.2.3 Capture de flux associés à la commande tcptraceroute

The screenshot shows the Wireshark interface with a capture on interface `eth0`. The packet list pane displays the following packets:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.15	10.0.1.1	DNS	74	Standard query 0x07f4 A www.google.com
2	0.000120000	10.0.2.15	10.0.1.1	DNS	74	Standard query 0xb7fc AAAA www.google.com
3	0.000893000	10.0.1.1	10.0.2.15	DNS	154	Standard query response 0x07f4 A 173.194.4
4	0.000942000	10.0.1.1	10.0.2.15	DNS	102	Standard query response 0xb7fc AAAA 2a00:1
5	0.001872000	10.0.2.15	173.194.45.82	TCP	74	1024->80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460
6	0.003026000	10.0.2.2	10.0.2.15	ICMP	70	Time-to-live exceeded (Time to live exceede
7	0.003447000	10.0.2.15	10.0.1.1	DNS	81	Standard query 0x5702 PTR 2.2.0.10.in-addr
8	0.004135000	10.0.1.1	10.0.2.15	DNS	175	Standard query response 0x5702 No such name
9	0.004409000	10.0.2.15	173.194.45.82	TCP	74	[TCP Port numbers reused] 1024->80 [SYN] Seq
10	0.004544000	10.0.2.2	10.0.2.15	ICMP	70	Time-to-live exceeded (Time to live exceede
11	0.005220000	10.0.2.15	173.194.45.82	TCP	74	[TCP Port numbers reused] 1024->80 [SYN] Seq
12	0.005503000	10.0.2.2	10.0.2.15	ICMP	70	Time-to-live exceeded (Time to live exceede
13	0.005628000	10.0.2.15	173.194.45.82	TCP	74	[TCP Port numbers reused] 1024->80 [SYN] Seq
14	0.006989000	173.194.45.82	10.0.2.15	TCP	60	80->1024 [SYN, ACK] Seq=0 Ack=1 Win=65535 Le
15	0.007042000	10.0.2.15	173.194.45.82	TCP	54	1024->80 [RST] Seq=1 Win=0 Len=0
16	0.007874000	10.0.2.15	10.0.1.1	DNS	86	Standard query 0x9ce8 PTR 2.2.45.194.173.ir
17	0.238701000	10.0.1.1	10.0.2.15	DNS	271	Standard query response 0x9ce8 PTR par03s]
18	0.238943000	10.0.2.15	173.194.45.82	TCP	74	[TCP Port numbers reused] 1024->80 [SYN] Seq
19	0.239636000	173.194.45.82	10.0.2.15	TCP	60	80->1024 [SYN, ACK] Seq=0 Ack=1 Win=65535 Le

Packet 19 details:

```

Destination: RealtekU_12:35:02 (52:54:00:12:35:02)
.....1..... = LG bit: Locally administered address (this is NOT the factory default)
0000 52 54 00 12 35 02 08 00 27 c0 ec 59 08 00 45 00  RT...S...'.Y..E.
0010 00 3c 7b 08 40 00 40 11 a8 99 0a 00 02 0f 0a 00  .<{.@. ....
0020 01 01 b5 54 00 35 00 28 17 49 07 f4 01 00 00 01  ...T.S.(.I.....
0030 00 00 00 00 00 00 03 77 77 77 06 67 6f 6f 67 6c  ....w ww.googl
0040 65 03 63 6f 6d 00 00 01 00 01                      e.com... ..
  
```

File: "/tmp/wireshark\_pcapng\_e... Packets: 23 · Displayed: 23 (100,0%) · Dropped: 1 (4,3%) Profile: Default

L'adresse physique de l'hôte de réception.

Caractéristiques ARP :

- Quelle est la taille l'en-tête ?

Taille de l'en-tête : 42 bytes (336 bits)

- Quelle est la valeur du champ Protocol Type contenu dans le message ARP?

Protocol Type : IP (0x0800)

- Quelle est l'adresse IP Source du paquet ARP?

10.0.2.15

- Quelle est l'adresse IP destination du paquet ?

10.0.2.2

- Quelle est l'adresse MAC Source incluse dans le message ARP ?

Source : CadmusCo\_c0 :ec :59 d'adresse 08:00:27:c0:ec:59

- *Quelle est l'adresse MAC destination incluse dans le message ARP ?*

Destination : 00 :00 :00\_00 :00 :00

### **1.3.2. Étude du paquet IP correspondant au second message ARP Reply**

*Caractéristiques Ethernet :*

- *Quelle est l'adresse MAC source de la trame Ethernet ?*

Source : 59Realtek\_U12 :35 :02 d'adresse 52:54:00:12:35:02

- *Quelle est l'adresse MAC destination trame Ethernet ?*

Destination : CadmusCo\_c0 :ec :59 d'adresse 08:00:27:c0:ec:59

*Caractéristiques ARP :*

- *Quelle est la taille l'en-tête ?*

60 bytes

- *Quelle est la valeur du champ Protocol Type contenu dans le message ARP?*

Protocol Type : IP (0x0800)

- *Quelle est l'adresse IP Source du paquet ARP?*

10.0.2.2

- *Quelle est l'adresse IP destination du paquet ?*

10.0.2.15

- *Quelle est l'adresse MAC Source incluse dans le message ARP ?*

Source : 59Realtek\_U12 :35 :02 d'adresse 52:54:00:12:35:02

- *Quelle est l'adresse MAC destination incluse dans le message ARP ?*

Destination : CadmusCo\_c0 :ec :59 d'adresse 08:00:27:c0:ec:59

- *Quelle action effectue la station émettrice après réception du message ARP reply ?*

Elle peut effectuer la suite de ses requêtes. Par exemple, elle peut se synchroniser (paquet NTP)

## **1.4 Analyse du message ICMP**

### **1.4.1. Message ICMP «Echo Request»**

- *Quelle est la taille l'en-tete ?*

20 bytes

- *Quel est le type de message ICMP ?*

Type : 8 (Echo (ping) request)

- *Quel est son identificateur ?*

Identifiant (BE) : 2421 (0x0975)

Identifiant (LE) : 29961 (0x7509)

- *Quel est le numéro de séquence ?*

Sequence number (BE) : 1 (0x0001)

Sequence number (LE) : 256(0x0100)

- *Quelle est l'adresse IP destination du paquet ?*

192.102.224.41

- *Quelle est la valeur du champ Protocol Type ?*

IP

- *Quelle est la valeur du champ Time to Live ?*

64

#### **1.4.2. Message ICMP «Echo Reply»**

- *Quel est le type de message ICMP ?*

Type : 0 (Echo (ping) reply)

- *Quel est son identificateur ? (A comparer à la requête question)*

Identifiant (BE) : 2421 (0x0975)

Identifiant (LE) : 29961 (0x7509)

C'est le même que précédemment.

- *Quel est le numéro de séquence ?*

Sequence number (BE) : 1 (0x0001)

Sequence number (LE) : 256(0x0100)

- *Quelle est l'adresse IP destination du paquet ?*

10.0.2.15

- *Quelle est la valeur du champ Protocol Type ?*

IP

- *Quelle est la valeur du champ Time to Live ?*

62

#### **1.4.3. Étude du message ICMP – Compléments**

- *Comparer ces données avec celles affichées dans le message de requête avec celles affichées dans le message de requête.*

Elles sont semblables à l'exception du TTL et l'IP de destination

- *Comment les champs d'identification et numéro de séquence évoluent dans le temps ?*

Ils restent identiques.

- Est-ce que les séquences de données des requêtes et des réponses changent ?

Non

- Calculer l'écart de temps entre l'émission de chaque message Echo Request et la réception de chaque message Echo Reply.

Il se passe environ 0.002 secondes. Cohérent avec une moyenne de ping à 150ms.

## 1.5 Analyse avec (tcp) traceroute

### 1.5.1 Protocoles capturés

- Quels sont les protocoles indiqués dans la colonne Protocol de la fenêtre de liste des trames capturées ? Il est probable que les paquets ICMP soient précédés d'un jeu de questions/réponses DNS, UDP, ICMP.

Les protocoles en question sont ICMP, DNS, UDP (pour la demande de traceroute) ainsi que ARP.

- Relever l'adresse IP renvoyée avec la réponse DNS. @I associé à [www.google.fr](http://www.google.fr)

```
Answers
  v www.google.fr: type A, class IN, addr 216.58.208.195
    Name: www.google.fr
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 202
    Data length: 4
    Address: 216.58.208.195
    . . . . .
```

### 1.5.2 Message UDP

- Quelle est l'adresse IP destination du premier paquet contenant le message UDP

L'adresse IP destination est : 216.58.208.195

- Quelles sont les valeurs des champs Protocol Type et Time to Live ?

Protocole : ICMP

Time to live : 1

- Comparer l'adresse IP destination relevée avec celle de la réponse DNS. Noter les valeurs caractéristiques de l'en-tête IP en vue d'une utilisation ultérieure.

Il s'agit de l'adresse IP retournée par le serveur DNS.

```

Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0
  Checksum: 0xf7f4 [correct]
  Identifiant (BE): 1 (0x0001)
  Identifiant (LE): 256 (0x0100)
  Sequence number (BE): 10 (0x000a)
  Sequence number (LE): 2560 (0x0a00)
> [No response seen]
> Data (64 bytes)

```

- Combien d'octets de données sont présents dans ce message de requête ?

Il y en a 106

### 1.5.3 Message ICMP « Time Exceeded »

- Quelles sont les @ IP source et destination du paquet de la première réponse ICMP Time Exceeded?

Source : 192.168.8.1

Destination : 192.168.8.192 (client)

- Quel est le type de message ICMP ? (Les champs Type, message ICMP Echo Request.) Comparer les valeurs caractéristiques de cet en-tête avec celles notées ci-avant.

```

Internet Control Message Protocol
  Type: 11 (Time-to-live exceeded)
  Code: 0 (Time to live exceeded in transit)
  Checksum: 0xf4ff [correct]
  Internet Protocol Version 4, Src: 192.168.8.192, Dst: 216.58.208.195
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 92
    Identification: 0x289d (10397)
  > Flags: 0x00
    Fragment offset: 0
  > Time to live: 1
    Protocol: ICMP (1)
  > Header checksum: 0x1e9e [validation disabled]
    Source: 192.168.8.192
    Destination: 216.58.208.195
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
  Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xf7f4 [in ICMP error packet]
    Identifiant (BE): 1 (0x0001)
    Identifiant (LE): 256 (0x0100)
    Sequence number (BE): 10 (0x000a)
    Sequence number (LE): 2560 (0x0a00)
  > Data (64 bytes)

```

Réponse Time-to-live Exceeded sur une demande de Echo (ping)

Le Time-to-live est passé de 1 à 0 ;

- *Est-ce que le message ICMP contient de nouveaux octets de données ?*

Oui, on passe de 106 octets à 134 octets.

#### **1.5.4 Évolution du champ TTL**

- *Combien de messages UDP sont émis avec la même valeur de champ TTL dans l'en-tête de paquet IP ?*

3 messages sont émis avec la même valeur de champ TTL

- *Quelles sont les adresses IP source des paquets ICMP Time Exceeded ?  
Comparer ces adresses avec celles données lors de l'exécution de la commande traceroute.*

Il s'agit des adresses de chaque nœud du réseau entre ma machine et l'adresse IP de www.google.fr

Il s'agit aussi des adresses affichées dans le terminal

- *Quel est le type du message ICMP reçu lorsque l'hôte destinataire est atteint ?*

Type : 0 (Echo (ping) reply)

- *Comment calculer les temps affichés par la commande traceroute à partir des valeurs données dans la colonne Time de la fenêtre des trames capturées ?*

Il suffit de faire la différence entre le time de la réponse et le temps de la demande.

## 2. Analyse des flux web

### 2.3. Protocoles capturés

- *Quels sont les protocoles indiqués dans la colonne Protocol de la fenêtre de liste des trames capturées ?*

TCP, HTTP, TLSv1.2

- *Quelle est l'utilité de la requête N°1 ?*

Elle permet d'établir la connexion avec le proxy Efrei

### 2.4. Trame Ethernet, paquet IP et datagramme UDP

#### 2.4.1. Analyser la trame correspondant au premier message DNS émis par le client Web.

- *Quelles sont les adresses (MAC/Ethernet) et IP du client ?*

MAC : CadmusCo\_c0 :ec :59 d'adresse 08:00:27:c0:ec:59

Ethernet :

IP : 10.0.2.15

- *Quel est le contenu du champ type de la trame Ethernet ?*

Type : IP

- *Quelles sont les adresses destination (MAC/Ethernet) et IP ?*

MAC : 59Realtek\_U12 :35 :02 d'adresse 52:54:00:12:35:02

Ethernet :

IP : 192.102.224.14

- *À quelles machines correspondent ces adresses ?*

Il s'agit du proxy de l'Efrei, permettant la connexion au web

#### 2.4.2. Analyser l'en-tête IP du premier message DNS émis par le client Web.

- *Quelle est la taille de l'en-tête ? Quelle est la longueur totale du paquet ?*

Taille en tête : 20, longueur totale 60

- *Repérer le champ « type de protocole » dans l'en-tête. Quel est le numéro et le type de protocole présent dans les données du paquet ?*

Protocole en-tête : IP

Protocole dans le paquet : UDP (17)

#### 2.4.3. Analyser l'en-tête UDP du premier message DNS émis par le client Web.

- *Quels sont les numéros de ports du client et du serveur ?*

Client : 56856

Serveur : 53

- *Quelles sont les particularités de ces valeurs ?*

53 est le port utilisé classiquement par DNS alors que le port client est généré à la volée

- *Quel est le protocole de couche application présent dans les données du message ?*

IP

- *Quelle est la valeur indiquée dans le champ longueur de l'en-tête UDP ?*

Longueur 40

- *Est-ce qu'elle correspond à l'information donnée dans l'en-tête du paquet IP ?*

Oui, elle correspond à la longueur totale – l'en-tête

## 2.5. Service DNS

### 2.5.1. Analyser le message de requête DNS émis par le client Web.

- *Quel est le champ qui indique si le message est une requête ou une réponse ?*

Champ Info de Wireshark : « Standard query **response** », et « Flags » dans le détail du paquet

- *Quelle est l'information transportée dans le corps de la requête ? Identifier le type et la classe de la requête.*

L'adresse IP correspondant au nom de domaine demandé, type A et classe IN

- *Quel est l'identificateur de transaction de la requête ?*

Identification : 0x3595

- *Quelles devraient être les adresses (MAC|Ethernet) et IP de ce paquet ? Vérifier que les adresses attendues sont présentes.*

On devrait avoir :

MAC : 59Realtek\_U12 :35 :02 d'adresse 52:54:00:12:35:02

Ethernet :

IP : 10.0.1.1

Ce qu'on a

- *Quelles sont les tailles du paquet IP et du message UDP ? Sont-elles supérieures aux messages requêtes ?*

IP : taille totale 95, header 20 = taille effective de 75

UDP : taille de 75

- *Quel est l'identificateur de transaction de la réponse ? Est-ce qu'il correspond à la requête ?*

Transaction ID : 0x3369, c'est le même que pour la requête

- Combien de réponses sont disponibles dans le message de réponse ? Comparer les réponses et leurs valeurs TTL (Time-to-live).

Time to live = 3600 et time to live = 300

## 2.6. Connexion TCP

- Quelles sont les adresses (MAC/Ethernet) et IP attendues pour cette trame ?

MAC : CadmusCo\_C0 :ec :59 (d'adresse 08 :00 :27 :c0 :ec :59)

Ethernet :

IP : 10.0.2.15

- Quelles sont les valeurs des champs type et protocole respectivement attendus pour cette trame et ce paquet ?

Type : IP (0x0800)

- Expliquer les valeurs des adresses destination (MAC/Ethernet) et IP ? À quels hôtes correspondent ces adresses ?

MAC : Realtek\_U12 :35 :02 d'adresse 52 :54 :00 :12 :35 :02

Ethernet :

IP : 192.102.224.14

Il s'agit du proxy de l'Efrei

- Identifier les numéros de ports utilisés par le client. Pourquoi ces valeurs sont-elles utilisées ?

Source port : 33544

Destination port : 3128

Le port source est utilisé à la volée, le port de destination est classiquement utilisé pour du TCP

- Quelle est la longueur du segment TCP ?

34 (70 – header de 40)

- Quel est le numéro de séquence initial (Initial Sequence Number ou ISN) émis par le client vers le serveur ?

0

- Quelle est la taille de fenêtre initiale ?

29200

- Quelle est la taille maximale de segment (Maximum Segment Size ou MSS) ?

1460

- Trouver la valeur hexadécimale de l'octet qui contient l'indicateur d'état SYN ?

A0 02

- Combien de temps s'est écoulé entre la capture du premier et du second segment TCP ?

Environ 0.0001 seconde

- Relever les valeurs des champs suivants de cette trame :

- Adresses MAC source et destination de la trame Ethernet.

Source : Realtek\_U12 :35 :02 d'adresse 52 :54 :00 :12 :35 :02

Destination: CadmusCo\_C0 :ec :59 (d'adresse 08 :00 :27 :c0 :ec :59)

- Adresses source et destination du paquet IP.

Source : 192.102.224.14

Destination : 10.0.2.15

- Numéros de séquence et d'acquittement du segment TCP.

Seq = 0

Ack = 1

- Valeurs des indicateurs d'état.

60 12

- Quelle est la longueur du segment TCP ?

Longueur totale : 44

- Quel est le numéro de séquence initial (Initial Sequence Number ou ISN émis par le serveur vers le client ?

0

Quelle est la taille de fenêtre initiale ?

29200

Quelle est la taille maximale de segment (Maximum Segment Size ou MSS) ?

1460

- Combien de temps s'est écoulé entre la capture du second et du troisième segment TCP ?

Environ 0.00001 seconde

- Comparer cette valeur avec celle relevée entre le premier et le second segment et expliquer la différence.

Elle est beaucoup plus faible, du fait que le client sait qui contacter et que le serveur s'attend à une telle requête de la part du client.

- Relever les valeurs des champs suivants de cette trame :

- Numéros de séquence et d'acquittement du segment TCP

Seq = 1

Ack = 1

- *Valeurs des indicateurs d'état*

50 10

- *Taille de fenêtre*

37376

- *Quelle est la longueur du segment TCP ?*

Longueur totale 54 – header 20 = 34