



Université Sultan Moulay Slimane Faculté Polydisciplinaire Béni Mellal
Département INFORMATIQUE (MIP)

Filière : Science de données et sécurité des systèmes
d'information
A.U : 2023-2024
Module : Réseaux Informatiques

Sujet

Rapport TP01

Présenté Par :
MAFTOUH Omar
KHADIM Mohamed Hamza

Encadré Par :
Pr : FARISS Meriam

Partie Pratique1 : ICMP

Commande ping :

➤ Command `ping -n 10 www.google.fr`

```
C:\Users\HP>ping -n 10 www.google.fr
```

Envoi d'une requête 'ping' sur www.google.fr [172.217.168.163] avec 32 octets de données :

Réponse de 172.217.168.163 : octets=32 temps=227 ms TTL=116

Réponse de 172.217.168.163 : octets=32 temps=194 ms TTL=116

Réponse de 172.217.168.163 : octets=32 temps=92 ms TTL=116

Réponse de 172.217.168.163 : octets=32 temps=223 ms TTL=116

Réponse de 172.217.168.163 : octets=32 temps=203 ms TTL=116

Réponse de 172.217.168.163 : octets=32 temps=112 ms TTL=116

Réponse de 172.217.168.163 : octets=32 temps=160 ms TTL=116

Délai d'attente de la demande dépassé.

Réponse de 172.217.168.163 : octets=32 temps=144 ms TTL=116

Réponse de 172.217.168.163 : octets=32 temps=295 ms TTL=116

Statistiques Ping pour 172.217.168.163:

Paquets : envoyés = 10, reçus = 9, perdus = 1 (perte 10%),

Durée approximative des boucles en millisecondes :

Minimum = 92ms, Maximum = 295ms, Moyenne = 183ms

➤ Capture lorsque l'invite de commande réapparaît à la console

44	9.435973	172.217.168.163	192.168.137.235	ICMP	74 Echo (ping) reply	id=0x0001, seq=22/5632, ttl=116 (request in 37)
45	10.262517	192.168.137.235	172.217.168.163	ICMP	74 Echo (ping) request	id=0x0001, seq=23/5888, ttl=128 (reply in 46)
46	10.354755	172.217.168.163	192.168.137.235	ICMP	74 Echo (ping) reply	id=0x0001, seq=23/5888, ttl=116 (request in 45)
47	10.656130	fe80::122c:88f4:23c...	ff02::1:3	LUMNR	106 Standard query 0x630b PTR 1.192.104.100.in-addr.arpa	
48	10.666802	192.168.137.1	224.0.0.252	LUMNR	86 Standard query 0x630b PTR 1.192.104.100.in-addr.arpa	
49	11.292828	192.168.137.235	172.217.168.163	ICMP	74 Echo (ping) request	id=0x0001, seq=24/6144, ttl=128 (reply in 50)
50	11.515618	172.217.168.163	192.168.137.235	ICMP	74 Echo (ping) reply	id=0x0001, seq=24/6144, ttl=116 (request in 49)
51	12.300107	192.168.137.235	172.217.168.163	ICMP	74 Echo (ping) request	id=0x0001, seq=25/6400, ttl=128 (reply in 52)
52	12.502994	172.217.168.163	192.168.137.235	ICMP	74 Echo (ping) reply	id=0x0001, seq=25/6400, ttl=116 (request in 51)
53	13.308002	192.168.137.235	172.217.168.163	ICMP	74 Echo (ping) request	id=0x0001, seq=26/6656, ttl=128 (reply in 54)
54	13.420730	172.217.168.163	192.168.137.235	ICMP	74 Echo (ping) reply	id=0x0001, seq=26/6656, ttl=116 (request in 53)
55	14.322334	192.168.137.235	172.217.168.163	ICMP	74 Echo (ping) request	id=0x0001, seq=27/6912, ttl=128 (reply in 56)
56	14.482280	172.217.168.163	192.168.137.235	ICMP	74 Echo (ping) reply	id=0x0001, seq=27/6912, ttl=116 (request in 55)
57	14.893162	172.64.155.141	192.168.137.235	TLSv1.2	78 Application Data	
58	14.893570	192.168.137.235	172.64.155.141	TLSv1.2	82 Application Data	
59	14.956881	172.64.155.141	192.168.137.235	TCP	54 443 → 50640 [ACK] Seq=25 Ack=29 Win=8 Len=0	
60	15.344710	192.168.137.235	172.217.168.163	ICMP	74 Echo (ping) request	id=0x0001, seq=28/7168, ttl=128 (no response found!)
61	20.164025	192.168.137.235	172.64.155.141	TLSv1.2	121 Application Data	
62	20.282007	172.64.155.141	192.168.137.235	TCP	54 443 → 50634 [ACK] Seq=1 Ack=135 Win=8 Len=0	
63	20.348839	192.168.137.235	172.217.168.163	ICMP	74 Echo (ping) request	id=0x0001, seq=29/7424, ttl=128 (reply in 64)
64	20.493239	172.217.168.163	192.168.137.235	ICMP	74 Echo (ping) reply	id=0x0001, seq=29/7424, ttl=116 (request in 63)
65	21.361211	192.168.137.235	172.217.168.163	ICMP	74 Echo (ping) request	id=0x0001, seq=30/7680, ttl=128 (reply in 66)
66	21.656685	172.217.168.163	192.168.137.235	ICMP	74 Echo (ping) reply	id=0x0001, seq=30/7680, ttl=116 (request in 65)
67	21.871117	192.168.137.235	34.117.188.166	TLSv1.2	93 Application Data	
68	22.166225	34.117.188.166	192.168.137.235	TCP	54 443 → 50723 [ACK] Seq=1 Ack=40 Win=277 Len=0	
69	22.329666	34.117.188.166	192.168.137.235	TLSv1.2	93 Application Data	
70	22.373466	192.168.137.235	34.117.188.166	TCP	54 50723 → 443 [ACK] Seq=40 Ack=40 Win=508 Len=0	
71	22.571886	34.117.188.166	192.168.137.235	TCP	93 [TCP Spurious Retransmission] 443 → 50723 [PSH, ACK] Seq=1 Ack=40 Win=277 Len=39	
72	22.571967	192.168.137.235	34.117.188.166	TCP	66 [TCP Dup ACK 70#1] 50723 → 443 [ACK] Seq=40 Ack=40 Win=508 Len=0 SLE=1 SRE=40	

Analyse avec ping :

1. Les protocoles indiqués dans la colonne Protocol de la fenêtre de liste des trames capturées sont comme suit :

1868	190.230175	192.168.137.235	192.168.137.1	DNS	85 Standard query 0xec93 A lh3.googleusercontent.com
1869	190.268256	192.168.137.235	192.168.137.1	DNS	75 Standard query 0xc27c A apis.google.com
1870	190.272387	192.168.137.235	192.168.137.1	DNS	86 Standard query 0x5044 A waa-pa.clients6.google.com
1871	190.527926	192.168.137.235	192.168.137.1	DNS	75 Standard query 0xc27c A apis.google.com
1872	190.527961	192.168.137.235	192.168.137.1	DNS	86 Standard query 0x5044 A waa-pa.clients6.google.com
1873	190.772472	142.250.201.78	192.168.137.235	TCP	1420 443 → 50890 [ACK] Seq=4099 Ack=663 Win=65536 Len=1366 [TCP segment of a reassembled PDU]
1874	190.772694	192.168.137.1	192.168.137.235	DNS	104 Standard query response 0x9d70 A www.google.com A 216.58.209.68
1875	190.772831	192.168.137.1	192.168.137.235	DNS	104 Standard query response 0x9d70 A www.google.com A 216.58.209.68

Il est possible que les paquets ICMP soient précédés par un échange de requêtes et de réponses DNS.

2. L'adresse IP renvoyée avec la réponse DNS

Internet Protocol Version 4, Src: 192.168.137.235, Dst: 192.168.137.1 0100 = Version: 4 0101 = Header Length: 20 bytes (5) > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) Total length: 59 Identification: 0x2903 (10499) 000. = Flags: 0x0 ...0 0000 0000 0000 = Fragment Offset: 0 Time to Live: 128 Protocol: UDP (17) Header Checksum: 0x7d71 [validation disabled] [Header checksum status: Unverified] Source Address: 192.168.137.235 Destination Address: 192.168.137.1 > User Datagram Protocol, Src Port: 53816, Dst Port: 53 > Domain Name System (query)	
---	--

Message ICMP « Echo Request »

43	5.472786	192.168.137.235	172.217.168.163	ICMP	74	Echo (ping) request	id=0x0001, seq=33/8448, ttl=128 (reply in 44)
44	5.632677	172.217.168.163	192.168.137.235	ICMP	74	Echo (ping) reply	id=0x0001, seq=33/8448, ttl=116 (request in 43)
45	6.491546	192.168.137.235	172.217.168.163	ICMP	74	Echo (ping) request	id=0x0001, seq=34/8704, ttl=128 (reply in 46)
46	6.554631	172.217.168.163	192.168.137.235	ICMP	74	Echo (ping) reply	id=0x0001, seq=34/8704, ttl=116 (request in 45)
47	7.518992	192.168.137.235	172.217.168.163	ICMP	74	Echo (ping) request	id=0x0001, seq=35/8960, ttl=128 (reply in 48)
48	7.611305	172.217.168.163	192.168.137.235	ICMP	74	Echo (ping) reply	id=0x0001, seq=35/8960, ttl=116 (request in 47)
49	8.545966	192.168.137.235	172.217.168.163	ICMP	74	Echo (ping) request	id=0x0001, seq=36/9216, ttl=128 (reply in 50)
50	8.704974	172.217.168.163	192.168.137.235	ICMP	74	Echo (ping) reply	id=0x0001, seq=36/9216, ttl=116 (request in 49)
51	9.574767	192.168.137.235	172.217.168.163	ICMP	74	Echo (ping) request	id=0x0001, seq=37/9472, ttl=128 (reply in 54)

Question 01 :

- ❖ L'adresse IP de destination du paquet est : **172.217.168.163**
- ❖ La valeur du champ Protocol Type et la valeur du champ Time to Live :

```
> Frame 43: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{BCE582C6-A5CD-46D6-B494-7B88622491BA}, id 0
> Ethernet II, Src: Intel_a6:60:17 (64:80:99:a6:60:17), Dst: 92:78:41:6d:78:b0 (92:78:41:6d:78:b0)
> Internet Protocol Version 4, Src: 192.168.137.235, Dst: 172.217.168.163
  0000 ... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 60
  Identification: 0xc625 (50725)
> 0000 ... = Flags: 0x0
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 128
  Protocol: ICMP (1)
  Header Checksum: 0xd48a [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.137.235
  Destination Address: 172.217.168.163
> Internet Control Message Protocol
```

Question 02 :

- ❖ Le type de message ICMP est octale, l'identificateur de message 0x0001 et le numéro de séquence 1/256

Question 03 :

- ❖ Utilisez la souris pour sélectionner les octets de données du message de requête, puis comparez-les avec les données affichées dans la fenêtre d'affichage brut

```
> Frame 43: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Dev...
> Ethernet II, Src: Intel_a6:60:17 (64:80:99:a6:60:17), Dst: 92:78:41:6d:78:b0 (92:78:41:6d:78:b0)
> Internet Protocol Version 4, Src: 192.168.137.235, Dst: 172.217.168.163
> Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0
  Checksum: 0xd48a [correct]
  [Checksum Status: Good]
  Identifier (BE): 1 (0x0001)
  Identifier (LE): 256 (0x0100)
  Sequence Number (BE): 33 (0x0021)
  Sequence Number (LE): 8448 (0x2100)
  [Response frame: 44]
> Data (32 bytes)
  Data: 6162636465666768696a6b6c6d6e6f7071727374757677616263646566676869
  [Length: 32]
```

```
0000  92 78 41 6d 78 b0 64 80 99 a6 60 17 08 00 45 00  <XAmc d...E:
0010  00 3c c6 25 00 00 00 01 d4 8a c0 a8 89 eb ac d9  <C %.....
0020  a8 a5 08 00 ad 3a 00 01 00 21 62 63 64 65 66 67  <..Hj...[abcd
0030  67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76  ghijklm opqrst
0040  77 61 62 63 64 65 66 67 68 69                      wabcdefg hi
```

Message ICMP « Echo Reply »

Question 01 :

- ❖ L'adresse IP source du paquet : **172.217.168.163**
- ❖ L'adresse IP destination du paquet : **192.168.137.235**
- ❖ La valeur du champ Protocol Type : **ICMP**

Question 02 :

- ❖ La valeur du champ Time to Live du message ICMP : **116**

```
Internet Protocol Version 4, Src: 172.217.168.163, Dst: 192.168.137.235
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x0000 (0)
  > 0000 .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 116
    Protocol: ICMP (1)
    Header Checksum: 0xa6b0 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 172.217.168.163
    Destination Address: 192.168.137.235
  > Internet Control Message Protocol
```

Question 03 :

```
Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0
  Checksum: 0x4d3b [correct]
  [Checksum Status: Good]
  Identifier (BE): 1 (0x0001)
  Identifier (LE): 256 (0x0100)
  Sequence Number (BE): 32 (0x0020)
  Sequence Number (LE): 8192 (0x2000)
  [Response frame: 41]
  > Data (32 bytes)
```

Question 04 :

```
Internet Protocol Version 4, Src: 192.168.137.235, Dst: 172.217.168.163
Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0
  Checksum: 0x4d3b [correct]
  [Checksum Status: Good]
  Identifier (BE): 1 (0x0001)
  Identifier (LE): 256 (0x0100)
  Sequence Number (BE): 32 (0x0020)
  Sequence Number (LE): 8192 (0x2000)
  [Response frame: 41]
  > Data (32 bytes)
    Data: 6162636465666768696a6b6c6d6e6f707172737475767778797a7b7c7d7e7f80818283848586878889
    [Length: 32]
```

0000	92 78 41 6d 78 b0 64 80 99 a6 60 17 08 00 45 00	-xAmx d- - - - - E-
0010	00 3c c6 24 00 00 80 01 d4 8b c0 a8 89 eb ac d9	-< \$ - - - - -
0020	a8 a3 08 00 4d 3b 00 01 00 20 61 62 63 64 65 66	- - - - M; - - - - abcdef
0030	67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76	ghijklm nopqrstuv
0040	77 78 79 7a 7b 7c 7d 7e 7f 80 81 82 83 84 85 86	wxyzdefg h i

Commande tracer

Commande **tracert** www.google.fr

```
C:\Users\HP>tracert www.google.fr
```

```
Détermination de l'itinéraire vers www.google.fr [172.217.168.163]  
avec un maximum de 30 sauts :
```

1	2 ms	*	2 ms	DESKTOP-HGSEJA0.mshome.net [192.168.137.1]
2	*	*	*	Délai d'attente de la demande dépassé.
3	24 ms	12 ms	7 ms	100.104.192.1
4	19 ms	17 ms	4 ms	172.31.253.1
5	26 ms	14 ms	17 ms	192.168.100.1
6	28 ms	27 ms	93 ms	105.73.33.158
7	49 ms	58 ms	39 ms	172.20.14.198
8	31 ms	29 ms	42 ms	142.250.174.134
9	92 ms	32 ms	59 ms	142.250.213.243
10	40 ms	66 ms	104 ms	74.125.253.201
11	32 ms	29 ms	42 ms	mad07s10-in-f3.1e100.net [172.217.168.163]

```
Itinéraire déterminé.
```

Protocoles capturés	
---------------------	--

1. Les protocoles indiqués dans la colonne protocol de la fenêtre de la list des trames capturées sont : **DNS , TCP , NBNS , ICMP , TLSv1.2 , TLSv1.3 , DHCPv6 , UDP**

75	27.476394	192.168.137.1	192.168.137.235	DNS	141 Standard query response 0xff6a No such name PTR 1.192.104.100.in-addr.arpa SOA 104.100.IN-ADDR.ARPA
76	27.478849	192.168.137.1	192.168.137.235	DNS	141 Standard query response 0xff6a No such name PTR 1.192.104.100.in-addr.arpa SOA 104.100.IN-ADDR.ARPA
77	28.698105	192.168.137.235	172.21.253.1	NBNS	92 Name query NBSTAT <00><00><00><00><00><00><00><00><00><00><00><00><00><00><00><00><00><00>
78	30.115908	192.168.137.235	172.21.253.1	NBNS	92 Name query NBSTAT <00><00><00><00><00><00><00><00><00><00><00><00><00><00><00><00><00><00>
79	30.127017	192.168.137.1	192.168.137.235	DNS	139 Standard query response 0xb2ee No such name PTR 1.253.31.172.in-addr.arpa SOA 31.172.IN-ADDR.ARPA
80	30.127017	192.168.137.1	192.168.137.235	DNS	139 Standard query response 0xb2ee No such name PTR 1.253.31.172.in-addr.arpa SOA 31.172.IN-ADDR.ARPA
81	30.470319	192.168.137.1	192.168.137.235	DNS	141 Standard query response 0xff6a No such name PTR 1.192.104.100.in-addr.arpa SOA 104.100.IN-ADDR.ARPA
82	30.470319	192.168.137.1	192.168.137.235	DNS	141 Standard query response 0xff6a No such name PTR 1.192.104.100.in-addr.arpa SOA 104.100.IN-ADDR.ARPA
83	30.879065	104.18.32.115	192.168.137.235	TLSv1.2	78 Application Data
84	30.879719	192.168.137.235	104.18.32.115	TLSv1.2	82 Application Data
85	30.900442	192.168.137.235	192.168.137.1	DNS	77 Standard query 0x2055 A sirius.mwbsys.com
86	30.926501	104.18.32.115	192.168.137.235	TCP	54 443 + 60413 [ACK] Seq=25 Ack=29 Win=8 Len=0
87	30.995515	192.168.137.1	192.168.137.235	DNS	77 Standard query response 0x2055 Server failure A sirius.mwbsys.com
88	31.009622	192.168.137.1	192.168.137.235	DNS	173 Standard query response 0x2055 A sirius.mwbsys.com A 34.225.80.244 A 34.230.196.30 A 54.86.52.183 A 54.85...
89	32.625599	192.168.137.235	172.217.168.163	ICMP	106 Echo (ping) request id=0x0001, seq=5313568, ttl=5 (no response found!)
90	32.652263	192.168.100.1	192.168.137.235	ICMP	134 Time-to-live exceeded (Time to live exceeded in transit)
91	32.655605	192.168.137.235	172.217.168.163	ICMP	106 Echo (ping) request id=0x0001, seq=5413824, ttl=5 (no response found!)
92	32.669403	192.168.100.1	192.168.137.235	ICMP	134 Time-to-live exceeded (Time to live exceeded in transit)
93	32.672243	192.168.137.235	172.217.168.163	ICMP	106 Echo (ping) request id=0x0001, seq=5514080, ttl=5 (no response found!)
94	32.689261	192.168.100.1	192.168.137.235	ICMP	134 Time-to-live exceeded (Time to live exceeded in transit)
95	32.693169	192.168.137.235	192.168.137.1	DNS	86 Standard query 0x9158 PTR 1.100.168.192.in-addr.arpa
96	35.503123	fe80::122c:88f4:23ca:f02::fb	fe80::122c:88f4:23ca:f02::fb	NDNS	154 Standard query response 0x0000 AAAA, cache flush fe80::122c:88f4:23ca:f02::fb NSEC, cache flush DESKTOP-HGSEJ...
97	37.705215	192.168.137.235	192.168.137.1	DNS	86 Standard query 0x9158 PTR 1.100.168.192.in-addr.arpa
98	34.037619	192.168.137.1	192.168.137.235	DNS	141 Standard query response 0x9158 No such name PTR 1.100.168.192.in-addr.arpa SOA 168.192.IN-ADDR.ARPA
99	34.038666	192.168.137.235	192.168.100.1	NBNS	92 Name query NBSTAT <00><00><00><00><00><00><00><00><00><00><00><00><00><00><00><00><00><00>
100	34.038995	192.168.137.1	192.168.137.235	DNS	141 Standard query response 0x9158 No such name PTR 1.100.168.192.in-addr.arpa SOA 168.192.IN-ADDR.ARPA
101	34.087952	192.168.137.1	192.168.137.235	DNS	139 Standard query response 0xb2ee No such name PTR 1.253.31.172.in-addr.arpa SOA 31.172.IN-ADDR.ARPA
102	34.087952	192.168.137.1	192.168.137.235	DNS	139 Standard query response 0xb2ee No such name PTR 1.253.31.172.in-addr.arpa SOA 31.172.IN-ADDR.ARPA
103	34.255904	192.168.137.235	20.230.46.154	TCP	1420 60414 + 443 [ACK] Seq=1 Ack=1 Win=512 Len=1366 [TCP segment of a reassembled PDU]
104	34.255904	192.168.137.235	20.230.46.154	TLSv1.2	326 Application Data
105	34.460780	20.230.46.154	192.168.137.235	TCP	54 443 + 60414 [ACK] Seq=1 Ack=1639 Win=16386 Len=0
106	34.829011	192.168.137.235	23.223.102.98	TCP	54 60403 + 80 [FIN, ACK] Seq=1 Ack=1 Win=512 Len=0

Message UDP

1. L'adresse IP destination du premier paquet contenant le message UDP : 192.168.43.1 , et les valeurs des champs sont avec Protocol Type et Time to Live :

```
✓ Internet Protocol Version 4, Src: 192.168.43.105, Dst: 192.168.43.1
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 57
  Identification: 0xfec5 (65221)
  > 000. .... = Flags: 0x0
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 128
  Protocol: UDP (17)
  Header Checksum: 0x6433 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.43.105
  Destination Address: 192.168.43.1
```

2. L'adresse IP relevée : 192.168.43.1 est différent à celle de la réponse DNS :
192.168.43.105
3. Combien d'octets de données sont présents dans ce message de requête ?

```
✓ Internet Protocol Version 4, Src: 192.168.43.1, Dst: 192.168.43.105
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 167
  Identification: 0x4e58 (20056)
  > 010. .... = Flags: 0x2, Don't fragment
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 64
  Protocol: UDP (17)
```

Partie Pratique 2 : HTTP

Trame Ethernet , paquet IP et datagramme UD

1. Les adresses MAC & IP du client :

```
> Frame 16: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface \Device\NPF_{BCE582C6-A5CD-4...}
> Ethernet II, Src: Intel_a6:60:17 (64:80:99:a6:60:17), Dst: TPLink_47:8a:f2 (c0:06:c3:47:8a:f2)
▼ Internet Protocol Version 4, Src: 192.168.0.187, Dst: 192.168.0.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 61
    Identification: 0xeed3 (61139)
    > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0xc9cf [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.0.187
    Destination Address: 192.168.0.1
> User Datagram Protocol, Src Port: 49732, Dst Port: 53
> Domain Name System (query)
```

2. Le contenu du champ type de la trame ethernet :

```
▼ Ethernet II, Src: Intel_a6:60:17 (64:80:99:a6:60:17), Dst: TPLink_47:8a:f2 (c0:06:c3:47:8a:f2)
> Destination: TPLink_47:8a:f2 (c0:06:c3:47:8a:f2)
> Source: Intel_a6:60:17 (64:80:99:a6:60:17)
Type: IPv4 (0x0800)
```

3. Les adresses MAC & IP du destination :

```
> Frame 16: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface \Device\NPF_{BCE582C6-A5CD-4...}
> Ethernet II, Src: Intel_a6:60:17 (64:80:99:a6:60:17), Dst: TPLink_47:8a:f2 (c0:06:c3:47:8a:f2)
▼ Internet Protocol Version 4, Src: 192.168.0.187, Dst: 192.168.0.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 61
    Identification: 0xeed3 (61139)
    > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0xc9cf [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.0.187
    Destination Address: 192.168.0.1
> User Datagram Protocol, Src Port: 49732, Dst Port: 53
> Domain Name System (query)
```

4. Les machines correspondent ces adresses :

```
▼ Ethernet II, Src: Intel_a6:60:17 (64:80:99:a6:60:17), Dst: TPLink_47:8a:f2 (c0:06:c3:47:8a:f2)
  > Destination: TPLink_47:8a:f2 (c0:06:c3:47:8a:f2)
  > Source: Intel_a6:60:17 (64:80:99:a6:60:17)
  Type: IPv4 (0x0800)
```

5. La taille de l'en-tête & longueur total du paquet :

```
> Frame 16: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface \Device\NPF_{BCE582C6-A5CD-4...}
> Ethernet II, Src: Intel_a6:60:17 (64:80:99:a6:60:17), Dst: TPLink_47:8a:f2 (c0:06:c3:47:8a:f2)
▼ Internet Protocol Version 4, Src: 192.168.0.187, Dst: 192.168.0.1
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 61
  Identification: 0xeed3 (61139)
  > 000. .... = Flags: 0x0
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 128
  Protocol: UDP (17)
  Header Checksum: 0xc9cf [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.0.187
  Destination Address: 192.168.0.1
  > User Datagram Protocol, Src Port: 49732, Dst Port: 53
  > Domain Name System (query)
```

6. Type de protocole & numéro du type de protocole :

```
> Frame 16: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface \Device\NPF_{BCE582C6-A5CD-4...}
> Ethernet II, Src: Intel_a6:60:17 (64:80:99:a6:60:17), Dst: TPLink_47:8a:f2 (c0:06:c3:47:8a:f2)
▼ Internet Protocol Version 4, Src: 192.168.0.187, Dst: 192.168.0.1
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 61
  Identification: 0xeed3 (61139)
  > 000. .... = Flags: 0x0
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 128
  Protocol: UDP (17)
  Header Checksum: 0xc9cf [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.0.187
  Destination Address: 192.168.0.1
  > User Datagram Protocol, Src Port: 49732, Dst Port: 53
  > Domain Name System (query)
```

7. Les numéros ports du client/serveur , particularités & le protocole :

```
▼ User Datagram Protocol, Src Port: 49732, Dst Port: 53
  Source Port: 49732
  Destination Port: 53
  Length: 41
  Checksum: 0x4ce5 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 0]
  > [Timestamps]
  UDP payload (33 bytes)
```

8. Longueur de l'en-tête UDP :

```
▼ User Datagram Protocol, Src Port: 49732, Dst Port: 53
  Source Port: 49732
  Destination Port: 53
  Length: 41
  Checksum: 0x4ce5 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 0]
  > [Timestamps]
  UDP payload (33 bytes)
```

Les deux valeurs sont différentes

Services DNS

1. Le champ qu'indique que le message est une requête ou une réponse :

```
▼ Domain Name System (query)
  Transaction ID: 0x2fa7
  > Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  > Queries
  [Response In: 17]
```

2. Les informations transposées dans le corps de la requête & le type et la classe de la requête :

```
> Frame 16: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface \Device\NPF_{BCE582C6-A5CD-46D6-B494-7B88622491BA},
> Ethernet II, Src: Intel_a6:60:17 (64:00:99:a6:60:17), Dst: TPLink_47:8a:f2 (c8:06:c3:47:8a:f2)
> Internet Protocol Version 4, Src: 192.168.0.187, Dst: 192.168.0.1
> User Datagram Protocol, Src Port: 49732, Dst Port: 53
▼ Domain Name System (query)
  Transaction ID: 0x2fa7
  > Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  > Queries
  > www.youtube.com: type A, class IN
  [Response In: 17]
```

3. L'identification de transaction de la requête :

```
▼ Domain Name System (query)
  Transaction ID: 0x2fa7
  > Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  > Queries
  > www.youtube.com: type A, class IN
  [Response In: 17]
```

4. Les adresses MAC | Ethernet & IP du paquet :

1. Adresse Source : **192.168.0.1**
2. Adresse Destination : **192.168.0.187**

16 2.118211	192.168.0.187	192.168.0.1	DNS	75 Standard query 0x2fa7 A www.youtube.com
17 2.144625	192.168.0.1	192.168.0.187	DNS	285 Standard query response 0x2fa7 A www.youtube.co

5. Taille du paquet IP du message UDP :

✚ Paquet IP :

```
Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.187
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 271
    Identification: 0xd427 (54311)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 63
    Protocol: UDP (17)
    Header Checksum: 0xe4a9 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.0.1
    Destination Address: 192.168.0.187
```

✚ Message UDP :

```
User Datagram Protocol, Src Port: 53, Dst Port: 49732
  Source Port: 53
  Destination Port: 49732
  Length: 251
  Checksum: 0x7e1b [unverified]
  [Checksum Status: Unverified]
  [Stream index: 0]
  > [Timestamps]
  UDP payload (243 bytes)
```

6. L'identification de transaction de la réponse :

```
Domain Name System (response)
  Transaction ID: 0x2fa7
  > Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 12
  Authority RRs: 0
  Additional RRs: 0
  > Queries
    > www.youtube.com: type A, class IN
  > Answers
    [Request In: 16]
    [Time: 0.026414000 seconds]
```

Requête HTTP GET

1. Numéro du séquence & acquittement de l'en-tête TCP :

```
▼ Transmission Control Protocol, Src Port: 55664, Dst Port: 80, Seq: 1, Ack: 1, Len: 449
  Source Port: 55664
  Destination Port: 80
  [Stream index: 3]
  > [Conversation completeness: Incomplete, DATA (15)]
  [TCP Segment Len: 449]
  Sequence Number: 1 (relative sequence number)
  Sequence Number (raw): 1039237113
  [Next Sequence Number: 450 (relative sequence number)]
  Acknowledgment Number: 1 (relative ack number)
  Acknowledgment number (raw): 3455888063
  0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
  Window: 259
  [Calculated window size: 66304]
  [Window size scaling factor: 256]
  Checksum: 0x4c83 [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  > [Timestamps]
  > [SEQ/ACK analysis]
```

2. Les indicateurs d'état actif dans l'en-tête TCP :

```
▼ Transmission Control Protocol, Src Port: 55664, Dst Port: 80, Seq: 1, Ack: 1, Len: 449
  Source Port: 55664
  Destination Port: 80
  [Stream index: 3]
  ▼ [Conversation completeness: Incomplete, DATA (15)]
    ..0. .... = RST: Absent
    ...0 .... = FIN: Absent
    .... 1... = Data: Present
    .... .1.. = ACK: Present
    .... ..1. = SYN-ACK: Present
    .... ...1 = SYN: Present
  [Completeness Flags: ..DASS]
```

- ❖ Aucune réinitialisation de connexion (RST) ou demande de fermeture (FIN) n'est présente.
- ❖ Le segment contient des données et un numéro d'acquittement valide (ACK).
- ❖ Il s'agit d'une réponse SYN-ACK dans le processus d'établissement de connexion.

3. La longueur de l'en-tête & la charge du message TCP :

```
Transmission Control Protocol, Src Port: 55664, Dst Port: 80, Seq: 1, Ack: 1, Len: 449
  Source Port: 55664
  Destination Port: 80
  [Stream index: 3]
  > [Conversation completeness: Incomplete, DATA (15)]
  [TCP Segment Len: 449]
  Sequence Number: 1 (relative sequence number)
  Sequence Number (raw): 1039237113
  [Next Sequence Number: 450 (relative sequence number)]
  Acknowledgment Number: 1 (relative ack number)
  Acknowledgment number (raw): 3455888063
  0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
  Window: 259
  [Calculated window size: 66304]
  [Window size scaling factor: 256]
  Checksum: 0x4c83 [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  > [Timestamps]
  > [SEQ/ACK analysis]
  TCP payload (449 bytes)
```

Réponse HTTP

1. Temps écoulé entre la capture du message GET & message de réponse :

80	2.383723	192.168.0.187	142.250.184.3	OCSP	504 Request
84	2.465910	142.250.184.3	192.168.0.187	OCSP	755 Response

2. Le serveur répond par un segment TCP ACK :

```
Transmission Control Protocol, Src Port: 80, Dst Port: 55664, Seq: 1, Ack: 450, Len: 701
  Source Port: 80
  Destination Port: 55664
  [Stream index: 3]
  > [Conversation completeness: Incomplete, DATA (15)]
  ..0. .... = RST: Absent
  ...0 .... = FIN: Absent
  .... 1... = Data: Present
  .... .1.. = ACK: Present
  .... ..1. = SYN-ACK: Present
  .... ...1 = SYN: Present
  [Completeness Flags: ..DASS]
  [TCP Segment Len: 701]
```

3. Le numéro de séquence émis par le serveur http :

Sequence Number: 1 (relative sequence number)

4. La longueur de la charge dans l'en-tête TCP :

0101 = Header Length: 20 bytes (5)

5. Les indicateurs d'état actifs de l'en-tête TCP :

```
...0. .... = RST: Absent
...0 .... = FIN: Absent
.... 1... = Data: Present
.... .1.. = ACK: Present
.... ..1. = SYN-ACK: Present
.... ...1 = SYN: Present
```

- ❖ Le drapeau DATA indique la présence de données dans le segment TCP.
- ❖ ACK signifie que le segment contient un numéro d'acquittement valide.
- ❖ SYN-ACK indique une réponse au processus d'établissement de connexion TCP.
- ❖ SYN signifie qu'une demande de connexion a été initiée.

6. Le prochain numéro de séquence est **2**.