

Table des matières

1. Connexion Bureau à distance (RDP)2
2. Capture de trames HTTP.....4

1. Connexion Bureau à distance (RDP)

```
Administrateur : Invite de commandes
TCP 172.17.2.3:62622 146.75.118.172:80 TIME_WAIT
TCP 172.17.2.3:62623 146.75.118.172:80 TIME_WAIT
TCP 172.17.2.3:62627 146.75.118.172:80 TIME_WAIT
TCP 172.17.2.3:62628 146.75.118.172:80 TIME_WAIT
TCP 172.17.2.3:62629 146.75.118.172:80 TIME_WAIT
TCP 172.17.2.3:62634 146.75.118.172:80 TIME_WAIT
TCP 172.17.2.3:62635 146.75.118.172:80 ESTABLISHED
TCP 172.17.2.3:62636 79.127.138.20:80 ESTABLISHED
TCP 172.17.2.3:62637 79.127.138.20:80 ESTABLISHED
TCP 172.17.2.3:62638 79.127.138.20:80 ESTABLISHED
TCP 172.17.2.3:62639 79.127.138.20:80 ESTABLISHED
TCP 172.17.2.3:62640 79.127.138.20:80 ESTABLISHED
TCP 172.17.2.3:62641 79.127.138.20:80 ESTABLISHED
TCP 172.17.2.3:62642 157.240.196.35:443 ESTABLISHED
TCP 172.17.2.3:62643 157.240.196.15:443 ESTABLISHED
TCP 172.17.2.3:62644 216.239.36.178:443 ESTABLISHED
TCP 172.17.2.3:62645 79.127.138.15:80 ESTABLISHED
TCP 172.17.2.3:62646 142.250.203.226:443 ESTABLISHED
TCP 172.17.2.3:62647 216.58.205.200:443 ESTABLISHED
TCP 172.17.2.3:62648 79.127.138.15:80 ESTABLISHED
TCP 172.17.2.3:62649 79.127.138.15:80 ESTABLISHED
TCP 172.17.2.3:62650 79.127.138.15:80 ESTABLISHED
TCP 172.17.2.3:62651 79.127.138.15:80 ESTABLISHED
TCP 172.17.2.3:62652 79.127.138.15:80 ESTABLISHED
TCP 172.17.2.3:62653 216.239.32.36:443 ESTABLISHED
```

```
C:\Windows\System32>ping 172.17.2.5

Envoi d'une requête 'Ping' 172.17.2.5 avec 32 octets de données :
Réponse de 172.17.2.5 : octets=32 temps=3 ms TTL=128
Réponse de 172.17.2.5 : octets=32 temps=2 ms TTL=128
Réponse de 172.17.2.5 : octets=32 temps=2 ms TTL=128
Réponse de 172.17.2.5 : octets=32 temps=2 ms TTL=128

Statistiques Ping pour 172.17.2.5:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 2ms, Maximum = 3ms, Moyenne = 2ms

C:\Windows\System32>
```

```
Administrateur : Invite de commandes
C:\Windows\System32>netstat -an

Connexions actives

Proto  Adresse locale      Adresse distante    État
TCP    0.0.0.0:80           0.0.0.0:0           LISTENING
TCP    0.0.0.0:135          0.0.0.0:0           LISTENING
TCP    0.0.0.0:445          0.0.0.0:0           LISTENING
TCP    0.0.0.0:903          0.0.0.0:0           LISTENING
TCP    0.0.0.0:913          0.0.0.0:0           LISTENING
TCP    0.0.0.0:2179         0.0.0.0:0           LISTENING
TCP    0.0.0.0:3306          0.0.0.0:0           LISTENING
TCP    0.0.0.0:3307          0.0.0.0:0           LISTENING
TCP    0.0.0.0:3389          0.0.0.0:0           LISTENING
TCP    0.0.0.0:5040          0.0.0.0:0           LISTENING
TCP    0.0.0.0:7680          0.0.0.0:0           LISTENING
TCP    0.0.0.0:49664          0.0.0.0:0           LISTENING
TCP    0.0.0.0:49665          0.0.0.0:0           LISTENING
TCP    0.0.0.0:49666          0.0.0.0:0           LISTENING
TCP    0.0.0.0:49667          0.0.0.0:0           LISTENING
TCP    0.0.0.0:49668          0.0.0.0:0           LISTENING
TCP    0.0.0.0:49669          0.0.0.0:0           LISTENING
TCP    0.0.0.0:49670          0.0.0.0:0           LISTENING
TCP    0.0.0.0:49671          0.0.0.0:0           LISTENING
TCP    127.0.0.1:19294        0.0.0.0:0           LISTENING
TCP    127.0.0.1:27017        0.0.0.0:0           LISTENING
TCP    127.0.0.1:39633        0.0.0.0:0           LISTENING
TCP    172.17.2.3:139         0.0.0.0:0           LISTENING
TCP    172.17.2.3:7680        172.17.2.8:59488    TIME_WAIT
TCP    172.17.2.3:7680        172.17.2.8:59491    TIME_WAIT
```

Quel est le port d'écoute du serveur Terminal Server ?

Le port d'écoute du serveur Terminal Server est 3389

Proto	Adresse locale	Adresse distante	État
TCP	0.0.0.0:80	0.0.0.0:0	LISTENING
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	0.0.0.0:903	0.0.0.0:0	LISTENING
TCP	0.0.0.0:913	0.0.0.0:0	LISTENING
TCP	0.0.0.0:2179	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3306	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3307	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3389	0.0.0.0:0	LISTENING
TCP	0.0.0.0:5040	0.0.0.0:0	LISTENING
TCP	0.0.0.0:7680	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49664	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49665	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49666	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49667	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49668	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49669	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49670	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49671	0.0.0.0:0	LISTENING
TCP	127.0.0.1:19294	0.0.0.0:0	LISTENING
TCP	127.0.0.1:27017	0.0.0.0:0	LISTENING
TCP	127.0.0.1:39633	0.0.0.0:0	LISTENING
TCP	172.17.2.3:139	0.0.0.0:0	LISTENING
TCP	172.17.2.3:3389	172.17.2.5:44498	ESTABLISHED
TCP	172.17.2.3:7680	172.17.2.8:59598	TIME_WAIT
TCP	172.17.2.3:7680	172.17.2.8:59599	TIME_WAIT
TCP	172.17.2.3:7680	172.17.2.8:59601	TIME_WAIT
TCP	172.17.2.3:7680	172.17.2.8:59602	TIME_WAIT

2. Capture de trames HTTP.

No.	http	Source	Destination	Protocol	Length	Info
55540	http2	146.75.118.133	172.17.2.3	HTTP	341	HTTP/1.1 200 OK (text/html)
55541	http3	172.17.2.3	146.75.118.133	OCSP	133	Request
55542	http	146.75.118.133	172.17.2.3	HTTP	193	GET /gsrsaovsslca2018.cr1 HTTP/1.1
55543	http	146.75.118.133	172.17.2.3	HTTP	341	HTTP/1.1 200 OK (text/html)
55544	http	146.75.118.133	172.17.2.3	HTTP	298	GET /rootr3/ME4wTDBKMEgwRjAJBgUrDgMCGGUABBTInGH%2FJbJW
55545	http	146.75.118.133	172.17.2.3	HTTP	341	HTTP/1.1 200 OK (text/html)
55546	http	146.75.118.133	172.17.2.3	HTTP	341	HTTP/1.1 200 OK (text/html)
55547	http	146.75.118.133	172.17.2.3	HTTP	341	HTTP/1.1 200 OK (text/html)
55548	http	146.75.118.133	172.17.2.3	HTTP	341	HTTP/1.1 200 OK (text/html)
55549	http	146.75.118.133	172.17.2.3	HTTP	341	HTTP/1.1 200 OK (text/html)
55550	http	146.75.118.133	172.17.2.3	HTTP	341	HTTP/1.1 200 OK (text/html)
55551	http	146.75.118.133	172.17.2.3	HTTP	341	HTTP/1.1 200 OK (text/html)
55552	http	146.75.118.133	172.17.2.3	HTTP	341	HTTP/1.1 200 OK (text/html)
55553	http	146.75.118.133	172.17.2.3	HTTP	341	HTTP/1.1 200 OK (text/html)
55554	http	146.75.118.133	172.17.2.3	HTTP	341	HTTP/1.1 200 OK (text/html)
55555	http	146.75.118.133	172.17.2.3	HTTP	341	HTTP/1.1 200 OK (text/html)
55556	http	146.75.118.133	172.17.2.3	HTTP	341	HTTP/1.1 200 OK (text/html)
55557	http	146.75.118.133	172.17.2.3	HTTP	341	HTTP/1.1 200 OK (text/html)
55558	http	146.75.118.133	172.17.2.3	HTTP	341	HTTP/1.1 200 OK (text/html)
55559	http	146.75.118.133	172.17.2.3	HTTP	341	HTTP/1.1 200 OK (text/html)
55560	http	146.75.118.133	172.17.2.3	HTTP	341	HTTP/1.1 200 OK (text/html)
55561	http	146.75.118.133	172.17.2.3	HTTP	341	HTTP/1.1 200 OK (text/html)
55562	http	146.75.118.133	172.17.2.3	HTTP	341	HTTP/1.1 200 OK (text/html)
55563	http	146.75.118.133	172.17.2.3	HTTP	341	HTTP/1.1 200 OK (text/html)
55564	http	146.75.118.133	172.17.2.3	HTTP	341	HTTP/1.1 200 OK (text/html)
55565	http	146.75.118.133	172.17.2.3	HTTP	341	HTTP/1.1 200 OK (text/html)
55566	http	146.75.118.133	172.17.2.3	HTTP	341	HTTP/1.1 200 OK (text/html)
55567	http	146.75.118.133	172.17.2.3	HTTP	341	HTTP/1.1 200 OK (text/html)
55568	http	146.75.118.133	172.17.2.3	HTTP	341	HTTP/1.1 200 OK (text/html)
55569	http	146.75.118.133	172.17.2.3	HTTP	341	HTTP/1.1 200 OK (text/html)
55570	http	146.75.118.133	172.17.2.3	HTTP	341	HTTP/1.1 200 OK (text/html)
55571	http	146.75.118.133	172.17.2.3	HTTP	341	HTTP/1.1 200 OK (text/html)
55572	http	146.75.118.133	172.17.2.3	HTTP	341	HTTP/1.1 200 OK (text/html)
55573	http	146.75.118.133	172.17.2.3	HTTP	341	HTTP/1.1 200 OK (text/html)
55574	http	146.75.118.133	172.17.2.3	HTTP	341	HTTP/1.1 200 OK (text/html)
55575	http	146.75.118.133	172.17.2.3	HTTP	341	HTTP/1.1 200 OK (text/html)
55576	http	146.75.118.133	172.17.2.3	HTTP	341	HTTP/1.1 200 OK (text/html)
55577	http	146.75.118.133	172.17.2.3	HTTP	341	HTTP/1.1 200 OK (text/html)
55578	http	146.75.118.133	172.17.2.3	HTTP	341	HTTP/1.1 200 OK (text/html)
55579	http	146.75.118.133	172.17.2.3	HTTP	341	HTTP/1.1 200 OK (text/html)
55580	http	146.75.118.133	172.17.2.3	HTTP	341	HTTP/1.1 200 OK (text/html)
55581	http	146.75.118.133	172.17.2.3	HTTP	341	HTTP/1.1 200 OK (text/html)
55582	http	146.75.118.133	172.17.2.3	HTTP	341	HTTP/1.1 200 OK (text/html)
55583	http	146.75.118.133	172.17.2.3	HTTP	341	HTTP/1.1 200 OK (text/html)
55584	http	146.75.118.133	172.17.2.3	HTTP	341	HTTP/1.1 200 OK (text/html)
55585	http	146.75.118.133	172.17.2.3	HTTP	341	HTTP/1.1 200 OK (text/html)
55586	http	146.75.118.133	172.17.2.3	HTTP	341	HTTP/1.1 200 OK (text/html)
55587	http	146.75.118.133	172.17.2.3	HTTP	341	HTTP/1.1 200 OK (text/html)
55588	http	146.75.118.133	172.17.2.3	HTTP	341	HTTP/1.1 200 OK (text/html)
55589	http	146.75.118.133	172.17.2.3	HTTP	341	HTTP/1.1 200 OK (text/html)
55590	http	146.75.118.133	172.17.2.3	HTTP	341	HTTP/1.1 200 OK (text/html)
55591	http	146.75.118.133	172.17.2.3	HTTP	341	HTTP/1.1 200 OK (text/html)
55592	http	146.75.118.133	172.17.2.3	HTTP	341	HTTP/1.1 200 OK (text/html)
55593	http	146.75.118.133	172.17.2.3	HTTP	341	HTTP/1.1 200 OK (text/html)
55594	http	146.75.118.133	172.17.2.3	HTTP	341	HTTP/1.1 200 OK (text/html)
55595	http	146.75.118.133	172.17.2.3	HTTP	341	HTTP/1.1 200 OK (text/html)
55596	http	146.75.118.133	172.17.2.3	HTTP	341	HTTP/1.1 200 OK (text/html)
55597	http	146.75.118.133	172.17.2.3	HTTP	341	HTTP/1.1 200 OK (text/html)
55598	http	146.75.118.133	172.17.2.3	HTTP	341	HTTP/1.1 200 OK (text/html)
55599	http	146.75.118.133	172.17.2.3	HTTP	341	HTTP/1.1 200 OK (text/html)
55600	http	146.75.118.133	172.17.2.3	HTTP	341	HTTP/1.1 200 OK (text/html)

```

> Frame 55484: 298 bytes on wire (2384 bits), 298 bytes captured (2384 bits) on interface 0
> Ethernet II, Src: Giga-Byt_2f:81:87 (74:56:3c:2f:81:87), Dst: Stc_00:0c:29:00:00:00
> Internet Protocol Version 4, Src: 172.17.2.3, Dst: 146.75.118.133
> Transmission Control Protocol, Src Port: 49829, Dst Port: 80, Seq: 474554, Len: 298
> Hypertext Transfer Protocol
0000 00 0d b4 2a a8 34 74 56 3c 2f 81 87 08 00 45 00 ...*4tV
0010 01 1c 58 1c 40 00 80 06 00 00 ac 11 02 03 92 4b ...X@...
0020 76 85 c2 a5 00 50 0c 77 e8 a1 63 ae 3a 38 50 18 v...Pw
0030 00 ff b7 f3 00 00 47 45 54 20 2f 72 6f 6f 74 72 .....GET
0040 33 2f 4d 45 34 77 54 44 42 4b 4d 45 67 77 52 6a B/ME4wTD
0050 41 4a 42 67 55 72 44 67 4d 43 47 67 55 41 42 42 AJBgUrDg
0060 54 31 6e 47 68 25 32 46 4a 42 6a 57 4b 6e 6b 50 TInGH%2F
0070 64 5a 49 7a 42 31 62 71 68 65 6c 48 42 77 51 55 dZI:B1bq
0080 6a 25 32 46 42 4c 66 36 67 75 52 53 53 75 54 56 j%2FBLf6
0090 44 36 59 35 71 4c 33 75 4c 64 47 37 77 43 44 51 D6YsQL3u
00a0 48 75 58 79 49 64 25 32 46 47 49 37 31 44 4d 36 HuXyId%2

```

No.	Time	Source	Destination	Protocol	Length	Info
59632	1017.377791	172.17.2.3	172.17.2.19	TCP	54	7680 → 50560 [FIN, ACK] Seq=124 Ack=124 Win=65280 Len=0
59633	1017.378898	172.17.2.19	172.17.2.3	TCP	60	50560 → 7680 [ACK] Seq=124 Ack=125 Win=65280 Len=0
59634	1017.378898	172.17.2.19	172.17.2.3	TCP	60	50560 → 7680 [FIN, ACK] Seq=124 Ack=125 Win=65280 Len=0
59635	1017.378921	172.17.2.3	172.17.2.19	TCP	54	7680 → 50560 [ACK] Seq=125 Ack=125 Win=65280 Len=0
59642	1018.152897	172.17.2.3	172.17.2.9	TCP	66	50060 → 7680 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256
59643	1018.154969	172.17.2.9	172.17.2.3	TCP	66	7680 → 50060 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256
59644	1018.155091	172.17.2.3	172.17.2.9	TCP	54	50060 → 7680 [ACK] Seq=1 Ack=1 Win=65280 Len=0
59645	1018.155244	172.17.2.3	172.17.2.9	TCP	129	50060 → 7680 [PSH, ACK] Seq=1 Ack=1 Win=65280 Len=75
59646	1018.156776	172.17.2.9	172.17.2.3	TCP	129	7680 → 50060 [PSH, ACK] Seq=1 Ack=76 Win=65280 Len=75
59647	1018.157012	172.17.2.3	172.17.2.9	TCP	108	50060 → 7680 [PSH, ACK] Seq=76 Ack=76 Win=65280 Len=54
59648	1018.158008	172.17.2.9	172.17.2.3	TCP	108	7680 → 50060 [PSH, ACK] Seq=76 Ack=130 Win=65280 Len=54
59649	1018.158008	172.17.2.9	172.17.2.3	TCP	60	7680 → 50060 [FIN, ACK] Seq=130 Ack=130 Win=65280 Len=0
59650	1018.158083	172.17.2.3	172.17.2.9	TCP	54	50060 → 7680 [ACK] Seq=130 Ack=131 Win=65280 Len=0
59651	1018.158288	172.17.2.3	172.17.2.9	TCP	54	50060 → 7680 [FIN, ACK] Seq=130 Ack=131 Win=65280 Len=0
59652	1018.159068	172.17.2.9	172.17.2.3	TCP	60	7680 → 50060 [ACK] Seq=131 Ack=131 Win=65280 Len=0
59687	1023.455881	172.17.2.3	98.66.133.184	TCP	66	50061 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256
59688	1023.460891	98.66.133.184	172.17.2.3	TCP	66	443 → 50061 [SYN, ACK] Seq=0 Ack=1 Win=17920 Len=0 MSS=1460 WS=256
59689	1023.460967	172.17.2.3	98.66.133.184	TCP	54	50061 → 443 [ACK] Seq=1 Ack=1 Win=65280 Len=0
59690	1023.461867	172.17.2.3	98.66.133.184	TLsv1.2	232	Client Hello
59691	1023.466785	98.66.133.184	172.17.2.3	TCP	60	443 → 50061 [ACK] Seq=1 Ack=179 Win=19456 Len=0
59692	1023.468903	98.66.133.184	172.17.2.3	TLsv1.2	1514	Server Hello
59693	1023.468903	98.66.133.184	172.17.2.3	TCP	1514	443 → 50061 [ACK] Seq=1461 Ack=179 Win=19456 Len=1460
59694	1023.468903	98.66.133.184	172.17.2.3	TLsv1.2	1230	Certificate
59695	1023.468957	172.17.2.3	98.66.133.184	TCP	54	50061 → 443 [ACK] Seq=179 Ack=4097 Win=65280 Len=0

```

> Frame 55484: 298 bytes on wire (2384 bits), 298 bytes captured (2384 bits) on interface 0
> Ethernet II, Src: Giga-Byt_2f:81:87 (74:56:3c:2f:81:87), Dst: Stc_00:0c:29:00:00:00
> Internet Protocol Version 4, Src: 172.17.2.3, Dst: 146.75.118.133
> Transmission Control Protocol, Src Port: 49829, Dst Port: 80, Seq: 474554, Len: 298
> Hypertext Transfer Protocol
0000 00 0d b4 2a a8 34 74 56 3c 2f 81 87 08 00 45 00 ...*4tV
0010 01 1c 58 1c 40 00 80 06 00 00 ac 11 02 03 92 4b ...X@...
0020 76 85 c2 a5 00 50 0c 77 e8 a1 63 ae 3a 38 50 18 v...Pw
0030 00 ff b7 f3 00 00 47 45 54 20 2f 72 6f 6f 74 72 .....GET
0040 33 2f 4d 45 34 77 54 44 42 4b 4d 45 67 77 52 6a B/ME4wTD
0050 41 4a 42 67 55 72 44 67 4d 43 47 67 55 41 42 42 AJBgUrDg
0060 54 31 6e 47 68 25 32 46 4a 42 6a 57 4b 6e 6b 50 TInGH%2F
0070 64 5a 49 7a 42 31 62 71 68 65 6c 48 42 77 51 55 dZI:B1bq
0080 6a 25 32 46 42 4c 66 36 67 75 52 53 53 75 54 56 j%2FBLf6
0090 44 36 59 35 71 4c 33 75 4c 64 47 37 77 43 44 51 D6YsQL3u
00a0 48 75 58 79 49 64 25 32 46 47 49 37 31 44 4d 36 HuXyId%2
00b0 68 56 63 25 33 44 20 48 54 54 50 2f 31 2e 31 0d hVc%3D
00c0 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 4b 65 65 ..Connect
00d0 70 2d 41 6c 69 76 65 0d 0a 41 63 63 65 70 74 3a p-Alive
00e0 20 2a 2f 2a 0d 0a 55 73 65 72 2d 41 67 65 6e 74 /*...Us
00f0 3a 20 4d 69 63 72 6f 73 6f 66 74 2d 43 72 79 70 : Micros
0100 74 6f 41 50 49 2f 31 30 2e 30 0d 0a 48 6f 73 74 toAPI/10
0110 3a 20 6f 63 73 70 32 2e 67 6c 6f 62 61 6c 73 69 : obsp2.
0120 67 6e 2e 63 6f 6d 0d 0a 0d 0a ..gn.com

```

```
C:\Users\msuiveng>nslookup www.http2demo.io
Serveur : roi.prince.local
Address: 172.17.254.1

Réponse ne faisant pas autorité :
Nom : 1906714720.rsc.cdn77.org
Addresses: 2a02:6ea0:dc00::30
           2a02:6ea0:dc00::32
           2a02:6ea0:dc00::31
           79.127.138.20
           79.127.138.17
           79.127.138.14
Aliases: www.http2demo.io
```

o.	Time	Source	Destination	Protocol	Length	Info
629	7.985508	172.17.2.2	79.127.138.14	HTTP	678	GET / HTTP/1.1
630	8.003715	79.127.138.14	172.17.2.2	HTTP	447	HTTP/1.1 304 Not Modified
633	8.018253	172.17.2.2	79.127.138.14	HTTP	577	GET /css/style.css HTTP/1.1
649	8.035184	79.127.138.14	172.17.2.2	HTTP	447	HTTP/1.1 304 Not Modified
650	8.035739	172.17.2.2	79.127.138.14	HTTP	581	GET /css/jsocials.css HTTP/1.1
657	8.039348	172.17.2.2	79.127.138.14	HTTP	592	GET /css/jsocials-theme-flat.css HTTP/1.1
658	8.039408	172.17.2.2	79.127.138.14	HTTP	585	GET /css/font-awesome.css HTTP/1.1
659	8.039468	172.17.2.2	79.127.138.14	HTTP	629	GET /img/refresh-icon.png HTTP/1.1
660	8.053655	79.127.138.14	172.17.2.2	HTTP	447	HTTP/1.1 304 Not Modified
661	8.054130	172.17.2.2	79.127.138.14	HTTP	626	GET /img/cdn77logo.png HTTP/1.1
664	8.056137	79.127.138.14	172.17.2.2	HTTP	423	HTTP/1.1 304 Not Modified
665	8.056137	79.127.138.14	172.17.2.2	HTTP	447	HTTP/1.1 304 Not Modified
666	8.056467	172.17.2.2	79.127.138.14	HTTP	630	GET /img/logo-10gbsio.png HTTP/1.1
667	8.056815	172.17.2.2	79.127.138.14	HTTP	569	GET /js/jsocials.min.js HTTP/1.1
670	8.057317	79.127.138.14	172.17.2.2	HTTP	448	HTTP/1.1 304 Not Modified
680	8.067287	172.17.2.2	79.127.138.14	HTTP	639	GET /img/http2-bg.png HTTP/1.1
684	8.071598	79.127.138.14	172.17.2.2	HTTP	421	HTTP/1.1 304 Not Modified
685	8.072648	79.127.138.14	172.17.2.2	HTTP	422	HTTP/1.1 304 Not Modified
686	8.073195	79.127.138.14	172.17.2.2	HTTP	448	HTTP/1.1 304 Not Modified
687	8.084601	79.127.138.14	172.17.2.2	HTTP	422	HTTP/1.1 304 Not Modified
692	8.087406	172.17.2.2	79.127.138.21	HTTP	599	GET /http2/html HTTP/1.1
770	8.104115	79.127.138.21	172.17.2.2	HTTP	443	HTTP/1.1 304 Not Modified
772	8.119538	172.17.2.2	79.127.138.21	HTTP	532	GET /http2/tiles_final/tile_0.png HTTP/1.1
810	8.136259	79.127.138.21	172.17.2.2	HTTP	419	HTTP/1.1 304 Not Modified
823	8.143373	172.17.2.2	79.127.138.21	HTTP	531	GET /http2/tiles_final/tile_1.png HTTP/1.1
824	8.143468	172.17.2.2	79.127.138.21	HTTP	531	GET /http2/tiles_final/tile_2.png HTTP/1.1

Frame 628: 678 bytes on wire (5424 bits), 678 bytes captured (5424 bits) on interface \Device\NPF_{A6A9C54A-A1CD-4F5E-A7DE-FE966EB45D} (Ethernet II, Src: Giga-Byt_2f:9b:ec (74:56:3c:2f:9b:ec), Dst: Stormsh_i_2a:a8:34 (00:0d:b4:2a:a8:34))

Internet Protocol Version 4, Src: 172.17.2.2, Dst: 79.127.138.14

Transmission Control Protocol, Src Port: 23965, Dst Port: 80, Seq: 1, Ack: 1, Len: 624

Hypertext Transfer Protocol

```

> GET / HTTP/1.1\r\n
Host: www.http2demo.io\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/139.0.0.0 Safari/537.36\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;q=0.9\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: fr-FR,fr;q=0.9,en-US;q=0.8,en;q=0.7\r\n
Cookie: _ga=GA1.2.1018825015.1760706537; _gid=GA1.2.1859830153.1760706537; _ga_RCV9W56Dj=GS2.2.1760706537$01$05t1760706537$J605
\r\n
[Full request URI: http://www.http2demo.io/]
[HTTP request 1/4]
[Response in frame: 630]
[Next request in frame: 633]

```

The screenshot displays a network capture in Wireshark. The top pane shows a list of captured packets, with packet 628 selected. The middle pane shows the details of this packet, identifying it as a Transmission Control Protocol (TCP) segment. The TCP header fields are expanded, showing a source port of 23965, a destination port of 80, and a sequence number of 625. The total length of the segment is 624 bytes. The bottom pane shows the raw hexadecimal and ASCII data of the packet, which is an HTTP GET request for the root path.

Quel est le nom du protocole transport utilisé par une trame HTTP ?

Le protocole de transport utilisé est le Transmission Control Protocol (TCP).

Quel est le nom du PDU encapsulant les données applicatives HTTP ?

L'unité de données de protocole (PDU) de la couche Transport qui encapsule les données applicatives (HTTP) est un Segment TCP (ou simplement Segment).

Quelle est la longueur de l'en-tête de transport ?

La longueur de l'en-tête de transport (TCP) est donc de 20 octets car "Header length: 20 bytes (5)"

Suiveng

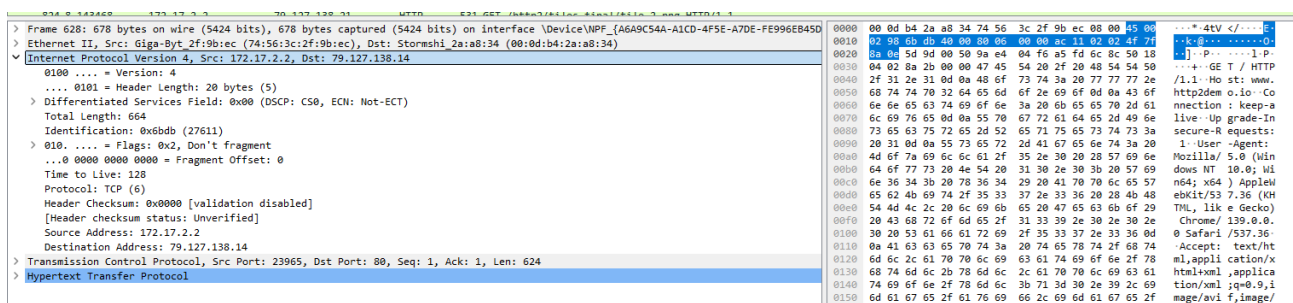
Mateo

TP 3 – Les Ports Logiciels

Quelles sont les valeurs décimale et hexadécimale correspondant aux ports source et destination ?

- La valeur décimale du port source est 23965 et sa valeur hexadécimale est 5d 9d
- La valeur décimale du port destination est 80 et sa valeur en hexadécimale est 00 50

Développez la section correspondant à l'en-tête Réseau :



Quelle est la longueur de l'en-tête de réseau ?

La longueur de l'en-tête de réseau : 20 octets (20 bytes).

Repérez le champ Protocole figurant dans l'en-tête Réseau. Quelle est la valeur présente ? Que signifie-t-elle ?

La valeur présente est TCP (6).

- Cela signifie que la charge utile de ce paquet IP est un segment TCP. Dans ce cas, ce segment TCP transporte lui-même les données de l'application (HTTP).

Quelles sont les valeurs décimales et hexadécimales des adresses IP source et destination ?

- La valeur décimale de l'IP source est 172.17.2.2 et sa valeur en hexadécimale est ac 11 02 02

```

Frame 628: 678 bytes on wire (5424 bits), 678 bytes captured (5424 bits) on interface \Device\NPF_{A6A9C54A-A1CD-4F5E-A7DE-FE996EB450}
Ethernet II, Src: Giga-Byt_2f:9b:ec (74:56:3c:2f:9b:ec), Dst: Stormshl_2a:a8:34 (00:0d:b4:2a:a8:34)
Internet Protocol Version 4, Src: 172.17.2.2, Dst: 79.127.138.14
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 664
  Identification: 0x6bdb (27611)
  > 010. .... = Flags: 0x2, Don't fragment
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 128
  Protocol: TCP (6)
  Header Checksum: 0x0000 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 172.17.2.2
  Destination Address: 79.127.138.14
  
```

- La valeur décimale de l'IP destination est 79.127.138.14 et sa valeur en hexadécimale est 4f 7f 8a 0e

```

Frame 628: 678 bytes on wire (5424 bits), 678 bytes captured (5424 bits) on interface \Device\NPF_{A6A9C54A-A1CD-4F5E-A7DE-FE996EB450}
Ethernet II, Src: Giga-Byt_2f:9b:ec (74:56:3c:2f:9b:ec), Dst: Stormshl_2a:a8:34 (00:0d:b4:2a:a8:34)
Internet Protocol Version 4, Src: 172.17.2.2, Dst: 79.127.138.14
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 664
  Identification: 0x6bdb (27611)
  010. .... = Flags: 0x2, Don't fragment
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 128
  Protocol: TCP (6)
  Header Checksum: 0x0000 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 172.17.2.2
  Destination Address: 79.127.138.14
  
```

- Développez la section correspondant à l'en-tête Ethernet :

```

Frame 628: 678 bytes on wire (5424 bits), 678 bytes captured (5424 bits) on interface \Device\NPF_{A6A9C54A-A1CD-4F5E-A7DE-FE996EB450}
Ethernet II, Src: Giga-Byt_2f:9b:ec (74:56:3c:2f:9b:ec), Dst: Stormshl_2a:a8:34 (00:0d:b4:2a:a8:34)
  Destination: Stormshl_2a:a8:34 (00:0d:b4:2a:a8:34)
  Source: Giga-Byt_2f:9b:ec (74:56:3c:2f:9b:ec)
  Type: IPv4 (0x0800)
  
```

- Repérez le champ EtherType. Quel est la valeur contenue ? Que signifie-t-elle ?

-Valeur contenue : IPv4 (0x0800).

- Signification : La valeur hexadécimale 0x0800 est l'identifiant pour le protocole Internet Protocol version 4 (IPv4). Cela signifie que la charge utile de cette trame Ethernet est un paquet IPv4.

- Quelles sont les valeurs des adresses MAC destination et source ?

Suiveng

Mateo

TP 3 – Les Ports Logiciels

- Adresse MAC Destination : 00:0b:0d:4a:2a:a4

- Adresse MAC Source : 74:56:3c:2f:9b:ec

- Repérez les trames associées à la mise en place de la connexion TCP entre le client et le serveur

32	0.953658	172.17.2.2	13.69.116.107	TCP	66	42436 → 443	[SYN]	Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
34	0.990524	13.69.116.107	172.17.2.2	TCP	66	443 → 42436	[SYN, ACK]	Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
35	0.990599	172.17.2.2	13.69.116.107	TCP	54	42436 → 443	[ACK]	Seq=1 Ack=1 Win=263424 Len=0

Les trames associées à la mise en place de la connexion TCP entre le client et le serveur sont donc SYN, SYN/ACK, ACK

No.	Time	Source	Destination	Protocol	Length	Info
32	0.953658	172.17.2.2	13.69.116.107	TCP	66	42436 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
34	0.990524	13.69.116.107	172.17.2.2	TCP	66	443 → 42436 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
35	0.990599	172.17.2.2	13.69.116.107	TCP	54	42436 → 443 [ACK] Seq=1 Ack=1 Win=263424 Len=0
36	0.991503	172.17.2.2	13.69.116.107	TLV1.2	266	Client Hello
38	1.032578	13.69.116.107	172.17.2.2	TCP	1514	443 → 42436 [ACK] Seq=1 Ack=213 Win=4194304 Len=1460 [TCP segment of a reassembled PDU]
39	1.032578	13.69.116.107	172.17.2.2	TCP	1514	443 → 42436 [ACK] Seq=1461 Ack=213 Win=4194304 Len=1460 [TCP segment of a reassembled PDU]
40	1.032681	172.17.2.2	13.69.116.107	TCP	54	42436 → 443 [ACK] Seq=213 Ack=2921 Win=263424 Len=0
41	1.032714	13.69.116.107	172.17.2.2	TLV1.2	1369	Server Hello, Certificate, Server Key Exchange, Server Hello Done
42	1.037429	172.17.2.2	13.69.116.107	TLV1.2	212	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
44	1.074937	13.69.116.107	172.17.2.2	TLV1.2	105	Change Cipher Spec, Encrypted Handshake Message
45	1.074937	13.69.116.107	172.17.2.2	TLV1.2	123	Application Data
46	1.074976	172.17.2.2	13.69.116.107	TCP	54	42436 → 443 [ACK] Seq=371 Ack=4356 Win=261888 Len=0
47	1.078901	172.17.2.2	13.69.116.107	TLV1.2	141	Application Data
48	1.078940	172.17.2.2	13.69.116.107	TLV1.2	957	Application Data
49	1.078980	172.17.2.2	13.69.116.107	TLV1.2	92	Application Data
50	1.079054	172.17.2.2	13.69.116.107	TLV1.2	947	Application Data
52	1.115155	13.69.116.107	172.17.2.2	TLV1.2	92	Application Data
53	1.115155	13.69.116.107	172.17.2.2	TCP	60	443 → 42436 [ACK] Seq=4394 Ack=1399 Win=4193024 Len=0
54	1.115155	13.69.116.107	172.17.2.2	TCP	60	443 → 42436 [ACK] Seq=4394 Ack=2292 Win=4194560 Len=0
55	1.115201	172.17.2.2	13.69.116.107	TCP	54	42436 → 443 [ACK] Seq=2292 Ack=4394 Win=263424 Len=0
57	1.151468	13.69.116.107	172.17.2.2	TLV1.2	339	Application Data
58	1.151498	172.17.2.2	13.69.116.107	TCP	54	42436 → 443 [ACK] Seq=2292 Ack=4679 Win=263168 Len=0
59	1.153450	172.17.2.2	13.69.116.107	TLV1.2	133	Application Data
60	1.153562	172.17.2.2	13.69.116.107	TLV1.2	2149	Application Data
62	1.190004	13.69.116.107	172.17.2.2	TCP	60	443 → 42436 [ACK] Seq=4679 Ack=3811 Win=4194560 Len=0
63	1.101430	13.69.116.107	172.17.2.2	TLV1.2	168	Application Data

```

> Frame 32: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{A6A9C54A-A1CD-4F5E-A7DE-FE996EB45D98},
> Ethernet II, Src: Stormsh1_2a:a8:34 (08:0d:b4:2a:a8:34), Dst: Stormsh1_2a:a8:34 (08:0d:b4:2a:a8:34)
> Internet Protocol Version 4, Src: 172.17.2.2, Dst: 13.69.116.107
  Transmission Control Protocol, Src Port: 42436, Dst Port: 443, Seq: 0, Len: 0
    Source Port: 42436
    Destination Port: 443
    [Stream index: 0]
    [Conversation completeness: Complete, WITH_DATA (63)]
    [TCP Segment Len: 0]
    Sequence Number: 0 (relative sequence number)
    Sequence Number (raw): 2751893935
    [Next Sequence Number: 1 (relative sequence number)]
    Acknowledgment Number: 0
    Acknowledgment Number (raw): 0
    1000 ... = Header Length: 32 bytes (8)
  Flags: 0x002 (SYN)
    Window: 64240
    [Calculated window size: 64240]
    Checksum: 0x2fea [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), SACK permiss
  [Timestamps]
  
```

```

0000 00 0d b4 2a a8 34 74 56 3c 2f 9b ec 08 00 45 00 ...*4tv </...E-
0010 00 34 aa 41 40 00 80 06 00 00 ac 11 02 02 0d 45 ...4A@.....E
0020 74 6b a5 c4 01 bb a4 06 91 af 00 00 00 00 00 tk.....
0030 fa f0 2f ea 00 00 02 04 05 b4 01 03 03 08 01 01 /.....
0040 04 02
  
```

No.	Time	Source	Destination	Protocol	Length	Info
32	0.953658	172.17.2.2	13.69.116.107	TCP	66	42436 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
34	0.990524	13.69.116.107	172.17.2.2	TCP	66	443 → 42436 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
35	0.990599	172.17.2.2	13.69.116.107	TCP	54	42436 → 443 [ACK] Seq=1 Ack=1 Win=263424 Len=0
36	0.991503	172.17.2.2	13.69.116.107	TLV1.2	266	Client Hello
38	1.032578	13.69.116.107	172.17.2.2	TCP	1514	443 → 42436 [ACK] Seq=1 Ack=213 Win=4194304 Len=1460 [TCP segment of a reassembled PDU]
39	1.032578	13.69.116.107	172.17.2.2	TCP	1514	443 → 42436 [ACK] Seq=1461 Ack=213 Win=4194304 Len=1460 [TCP segment of a reassembled PDU]
40	1.032681	172.17.2.2	13.69.116.107	TCP	54	42436 → 443 [ACK] Seq=213 Ack=2921 Win=263424 Len=0
41	1.032714	13.69.116.107	172.17.2.2	TLV1.2	1369	Server Hello, Certificate, Server Key Exchange, Server Hello Done
42	1.037429	172.17.2.2	13.69.116.107	TLV1.2	212	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
44	1.074937	13.69.116.107	172.17.2.2	TLV1.2	105	Change Cipher Spec, Encrypted Handshake Message
45	1.074937	13.69.116.107	172.17.2.2	TLV1.2	123	Application Data
46	1.074976	172.17.2.2	13.69.116.107	TCP	54	42436 → 443 [ACK] Seq=371 Ack=4356 Win=261888 Len=0
47	1.078901	172.17.2.2	13.69.116.107	TLV1.2	141	Application Data
48	1.078940	172.17.2.2	13.69.116.107	TLV1.2	957	Application Data
49	1.078980	172.17.2.2	13.69.116.107	TLV1.2	92	Application Data
50	1.079054	172.17.2.2	13.69.116.107	TLV1.2	947	Application Data
52	1.115155	13.69.116.107	172.17.2.2	TLV1.2	92	Application Data
53	1.115155	13.69.116.107	172.17.2.2	TCP	60	443 → 42436 [ACK] Seq=4394 Ack=1399 Win=4193024 Len=0
54	1.115155	13.69.116.107	172.17.2.2	TCP	60	443 → 42436 [ACK] Seq=4394 Ack=2292 Win=4194560 Len=0
55	1.115201	172.17.2.2	13.69.116.107	TCP	54	42436 → 443 [ACK] Seq=2292 Ack=4394 Win=263424 Len=0
57	1.151468	13.69.116.107	172.17.2.2	TLV1.2	339	Application Data
58	1.151498	172.17.2.2	13.69.116.107	TCP	54	42436 → 443 [ACK] Seq=2292 Ack=4679 Win=263168 Len=0
59	1.153450	172.17.2.2	13.69.116.107	TLV1.2	133	Application Data
60	1.153562	172.17.2.2	13.69.116.107	TLV1.2	2149	Application Data
62	1.190004	13.69.116.107	172.17.2.2	TCP	60	443 → 42436 [ACK] Seq=4679 Ack=3811 Win=4194560 Len=0
63	1.101430	13.69.116.107	172.17.2.2	TLV1.2	168	Application Data

```

> Frame 34: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{A6A9C54A-A1CD-4F5E-A7DE-FE996EB45D98},
> Ethernet II, Src: Stormsh1_2a:a8:34 (08:0d:b4:2a:a8:34), Dst: Giga-Byt_2f:9b:ec (74:56:3c:2f:9b:ec)
> Internet Protocol Version 4, Src: 13.69.116.107, Dst: 172.17.2.2
  Transmission Control Protocol, Src Port: 443, Dst Port: 42436, Seq: 0, Ack: 1, Len: 0
    Source Port: 443
    Destination Port: 42436
    [Stream index: 0]
    [Conversation completeness: Complete, WITH_DATA (63)]
    [TCP Segment Len: 0]
    Sequence Number: 0 (relative sequence number)
    Sequence Number (raw): 2893793993
    [Next Sequence Number: 1 (relative sequence number)]
    Acknowledgment Number: 1 (relative ack number)
    Acknowledgment Number (raw): 2751893936
    1000 ... = Header Length: 32 bytes (8)
  Flags: 0x012 (SYN, ACK)
    Window: 65535
    [Calculated window size: 65535]
    Checksum: 0xead4 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), SACK permit
  [Timestamps]
  [SEQ/ACK analysis]
    [This is an ACK to the segment in frame: 32]
    [The RTT to ACK the segment was: 0.036868000 seconds]
  
```

```

0000 74 56 3c 2f 9b ec 08 0d b4 2a a8 34 08 00 45 00 tv/.....*4-E-
0010 00 34 26 bb a0 00 0c 06 b8 a5 0d 45 74 0b ac 11 ...4&@l...E Etk...
0020 02 02 01 bb a5 c4 ac 7b ca c9 a4 06 91 b0 00 12 .....{.....
0030 ff ff ea d4 00 00 02 04 05 a0 01 03 03 08 01 01 /.....
0040 04 02
  
```

The screenshot displays a network traffic capture in Wireshark. The top pane shows a list of packets, with packet 35 (ACK) highlighted. The middle pane shows the packet details for the selected ACK, including source and destination ports, sequence numbers, and window size. The bottom pane shows the raw packet data in hexadecimal and ASCII.

- Que signifie le contenu de ce champ pour chacun des 3 segments TCP ? Quelle est la raison de la mise en place de ce mode connecté ?

- Segment SYN : Le client envoie une requête de synchronisation pour initier la connexion

- Segment SYN/ACK : le serveur accuse de réception du SYN du client(ACK) et envoie à son tour un SYN

-Segment ACK : Le client SYN du serveur, confirme donc la connexion

La raison de la mise en place de ce mode connecté :

Le protocole TCP utilise ce moyen de communication pour que les deux parties puissent échanger des données sans risque de perte.