

## sommaire

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

## PARTI 1 -Connexion Bureau à distance (RDP)

Mon adresse :172.17.2.9

```

Suffixe DNS propre à la connexion. . . : prince.local
Description. . . . . : Realtek PCIe GbE Family Controller
Adresse physique . . . . . : 74-56-3C-2F-82-CE
DHCP activé. . . . . : Oui
Configuration automatique activée. . . : Oui
Adresse IPv6 de liaison locale. . . . . : fe80::425f:a7ba:d519:b2c%8(préféré)
Adresse IPv4. . . . . : 172.17.2.9(préféré)
Masque de sous-réseau. . . . . : 255.255.0.0
Bail obtenu. . . . . : mercredi 1 octobre 2025 09:55:57
Bail expirant. . . . . : mercredi 1 octobre 2025 10:25:49

```

adresse voisin : 172.17.2.13

- ping de la station du voisin

```

C:\Users\rcorreia>ping 172.17.2.13

Envoi d'une requête 'Ping' 172.17.2.13 avec 32 octets de données :
Réponse de 172.17.2.13 : octets=32 temps=2 ms TTL=128
Réponse de 172.17.2.13 : octets=32 temps=2 ms TTL=128
Réponse de 172.17.2.13 : octets=32 temps=2 ms TTL=128
Réponse de 172.17.2.13 : octets=32 temps=2 ms TTL=128

Statistiques Ping pour 172.17.2.13:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 2ms, Maximum = 2ms, Moyenne = 2ms

```

Activation du Bureau à distance





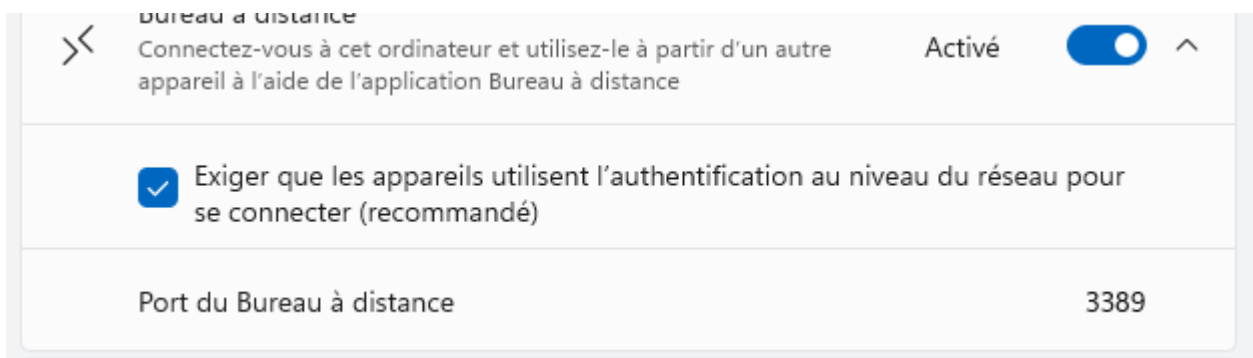
- Saisissez la commande netstat -an depuis l'invite de commandes de votre station Windows

```
C:\Users\rcorreia>netstat -an

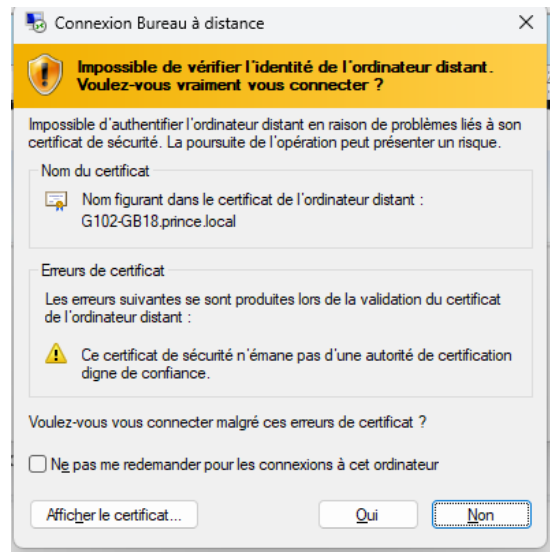
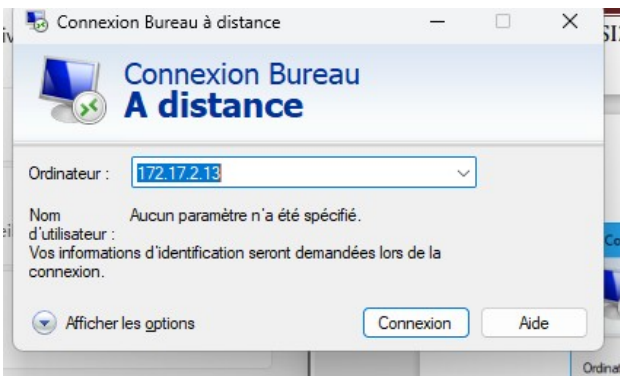
Connexions actives

Proto  Adresse locale      Adresse distante    État
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    0.0.0.0:902          0.0.0.0:0           LISTENING
TCP    0.0.0.0:912          0.0.0.0:0           LISTENING
TCP    0.0.0.0:2179        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    0.0.0.0:49664        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    127.0.0.1:27017      0.0.0.0:0           LISTENING
TCP    172.17.2.9:139       0.0.0.0:0           LISTENING
TCP    172.17.2.9:50430     172.17.254.5:445    ESTABLISHED
TCP    172.17.2.9:58078     172.17.254.5:445    ESTABLISHED
TCP    172.17.2.9:58321     95.100.133.19:443   TIME_WAIT
TCP    172.17.2.9:58324     95.100.133.19:443   TIME_WAIT
TCP    172.17.2.9:58327     95.100.133.19:443   TIME_WAIT
```

Quel est le port d'écoute du serveur Terminal Server ? Le TCP 0.0.0.0.3389



connection au bureau a distance

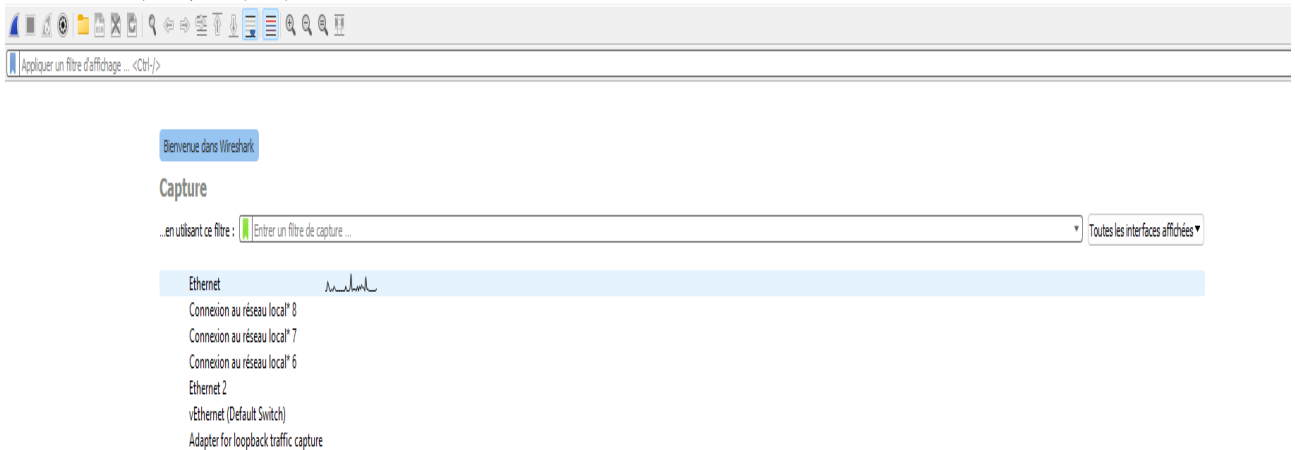


PROTO	Adresse locale	Adresse distante	Etat
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	0.0.0.0:2179	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3389	0.0.0.0:0	LISTENING
TCP	0.0.0.0:5040	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49664	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49665	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49666	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49671	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49672	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49673	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49722	0.0.0.0:0	LISTENING
TCP	0.0.0.0:65046	0.0.0.0:0	LISTENING
TCP	127.0.0.1:27017	0.0.0.0:0	LISTENING
TCP	172.17.2.13:139	0.0.0.0:0	LISTENING
TCP	172.17.2.13:3389	172.17.2.9:58586	ESTABLISHED
TCP	172.17.2.13:64649	172.17.254.5:445	ESTABLISHED
TCP	172.17.2.13:65227	40.126.31.71:443	TIME_WAIT
TCP	172.17.2.13:65228	40.126.31.71:443	TIME_WAIT

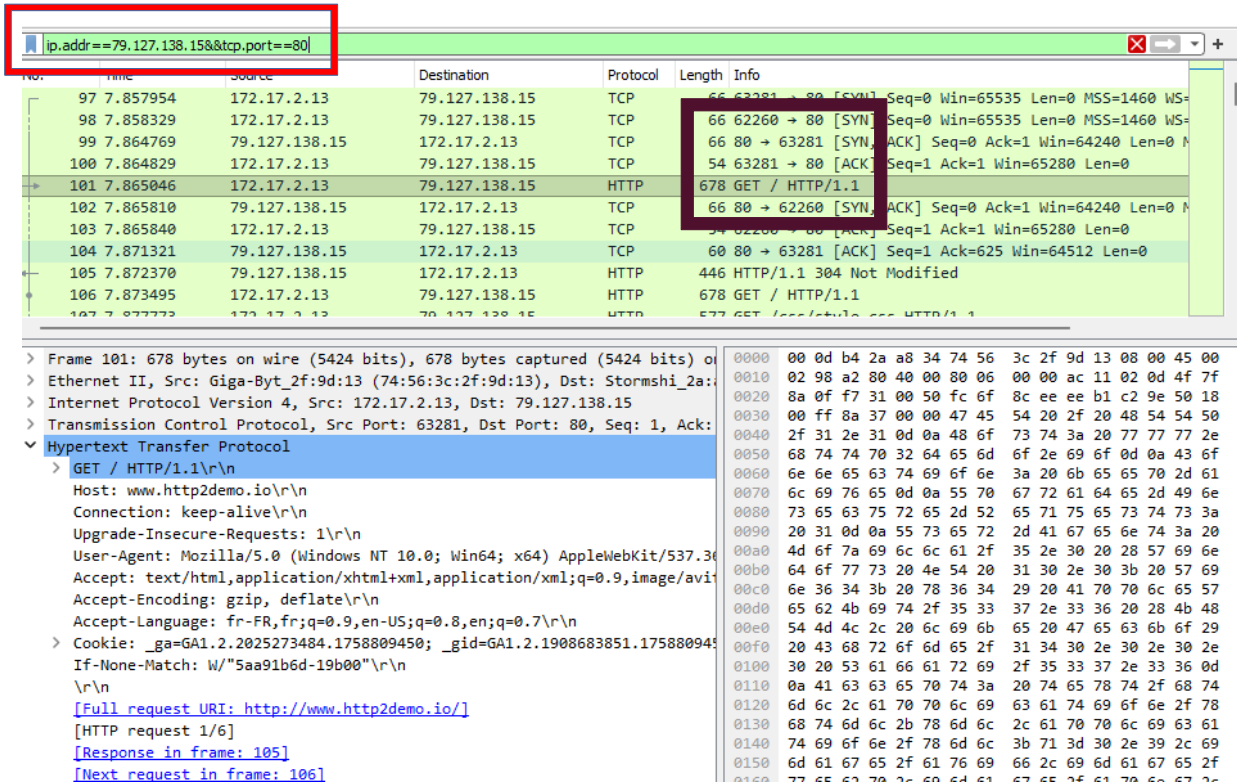
la session a etait arreter

## 2. Capture de trames HTTP

Wireshark lancé en mode admin



ont est aller sur l'adresse [HTTP/2 technology demo](http://www.http2demo.io)



```

C:\Users\rcorreia>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::32
           2a02:6ea0:dc00::31
           2a02:6ea0:dc00::30
           79.127.138.14
           79.127.138.20
           79.127.138.18
Aliases: www.http2demo.io
    
```

trame http reperé

100	7.864829	172.17.2.13	79.127.138.15	TCP	64 63261 → 80 [ACK]	Seq=1 Ack=1 Win=65280 Len=0
101	7.865046	172.17.2.13	79.127.138.15	HTTP	678 GET / HTTP/1.1	
102	7.865810	79.127.138.15	172.17.2.13	TCP	66 80 → 63260 [ACK]	Seq=0 Ack=1 Win=64240 Len=0 M
103	7.865840	172.17.2.13	79.127.138.15	TCP	54 62260 → 80 [ACK]	Seq=1 Ack=1 Win=65280 Len=0
104	7.871321	79.127.138.15	172.17.2.13	TCP	60 80 → 63281 [ACK]	Seq=1 Ack=625 Win=64512 Len=0

```

> Frame 101: 678 bytes on wire (5424 bits), 678 bytes captured (5424 bits) on
> Ethernet II, Src: Giga-Byt 2f:9d:13:74:56:3c, Dst: Stormsh 2a:02:6e:
> Internet Protocol Version 4, Src: 172.17.2.13, Dst: 79.127.138.15
> Transmission Control Protocol, Src Port: 63281, Dst Port: 80, Seq: 1, Ack:
< 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
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avi
    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=GA1.2.2025273484.1758809450; _gid=GA1.2.1908683851.17588094
    If-None-Match: W/"5aa91b6d-19b00"\r\n
    \r\n
    [Full request URI: http://www.http2demo.io/]
    [HTTP request 1/6]
    [Response in frame: 105]
    [Next request in frame: 106]
    
```

**en-tête transport developpe**

Frame 101: 678 bytes on wire (5424 bits), 678 bytes captured (5424 bits) on  
 Ethernet II, Src: Giga-Byt\_2f:9d:13 (74:56:3c:2f:9d:13), Dst: Stormsh...  
 Internet Protocol Version 4, Src: 172.17.2.13, Dst: 79.127.138.15  
 Transmission Control Protocol, Src Port: 63281, Dst Port: 80, Seq: 1, Ac  
 Source Port: 63281  
 Destination Port: 80  
 [Stream index: 1]  
 [Conversation completeness: Incomplete, DATA (15)]  
 [TCP Segment Len: 624]  
 Sequence Number: 1 (relative sequence number)  
 Sequence Number (raw): 4235169006  
 [Next Sequence Number: 625 (relative sequence number)]  
 Acknowledgment Number: 1 (relative ack number)  
 Acknowledgment number (raw): 4004627102  
 0101 .... = Header Length: 20 bytes (5)  
 Flags: 0x018 (PSH, ACK)  
 Window: 255  
 [Calculated window size: 65280]  
 [Window size scaling factor: 256]  
 Checksum: 0x8a37 [unverified]  
 [Checksum Status: Unverified]  
 Urgent Pointer: 0  
 Timestamps

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

Le nom du protocole ce'st transmission Control Protocol ou TCP

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

Le pdu de TCP c'est le segment

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

Elle est de 20 bytes

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

Port source : 80 / 00 50

port destination: 63281 / f7 31

Source Port: 63281  
 Destination Port: 80

Developpez l'en-tete reseau

Frame 101: 678 bytes on wire (5424 bits), 678 bytes captured (5424 bits) on  
 Ethernet II, Src: Giga-Byt\_2f:9d:13 (74:56:3c:2f:9d:13), Dst: Stormsh...  
 Internet Protocol Version 4, Src: 172.17.2.13, Dst: 79.127.138.15  
 0100 .... = Version: 4  
 .... 0101 = Header Length: 20 bytes (5)  
 Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
 Total Length: 664  
 Identification: 0xa280 (41600)  
 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: 172.17.2.13  
 Destination Address: 79.127.138.15  
 Transmission Control Protocol, Src Port: 63281, Dst Port: 80, Seq: 1, Ac

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

20 bytes

Repérez le champ Protocole figurant dans l'en-tête Réseau. Quelle est la valeur présente ?

6

Que signifie-t-elle ?

Elle signifie que ont a un TCP , ont peut aussi avoir 1 1 qui veut dire UDP

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

IP source : 172,17,2,13 / hexa : ac 11 02 0d

IP destination : 79,127,138,15 / hexa : 4f 7f 8a 0f

```
Source Address: 172.17.2.13
Destination Address: 79.127.138.15
```

en-tete Ethernet developé

```
> Frame 101: 678 bytes on wire (5424 bits) - 678 bytes captured (5424 bits) on 0
Ethernet II, Src: Giga-Byt_2f:9d:13 (74:56:3c:2f:9d:13), Dst: Stormshi_2a:a8:34 (00:0d:b4:2a:a8:34)
  > Destination: Stormshi_2a:a8:34 (00:0d:b4:2a:a8:34)
  > Source: Giga-Byt_2f:9d:13 (74:56:3c:2f:9d:13)
  Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 172.17.2.13, Dst: 79.127.138.15
Transmission Control Protocol, Src Port: 80, Dst Port: 63281, Seq: 1, ACK: 1
Hypertext Transfer Protocol
```

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

0X800 ,elle signifie que cest un IPv4, si ont avais 0x806 ont aurais eu une trame ARP

Quelles sont les valeurs des adresses MAC destination et source ?

Mac source : 74:56:3c:2f:9d:13

mac Destination : 00:0d:b4:2a:a8:34

```
> Destination: Stormshi_2a:a8:34 (00:0d:b4:2a:a8:34)
> Source: Giga-Byt_2f:9d:13 (74:56:3c:2f:9d:13)
```

ont repere les trame de connexion tcp

```
Ethernet II, Src: Stormshi_2a:a8:34 (00:0d:b4:2a:a8:34), Dst: Giga-Byt_2f:9d:13 (74:56:3c:2f:9d:13)
  > Destination: Giga-Byt_2f:9d:13 (74:56:3c:2f:9d:13)
  > Source: Stormshi_2a:a8:34 (00:0d:b4:2a:a8:34)
  Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 79.127.138.15, Dst: 172.17.2.13
Transmission Control Protocol, Src Port: 80, Dst Port: 63281, Seq: 1, ACK: 1
  Source Port: 80
  Destination Port: 63281
  [Stream index: 1]
  [Conversation completeness: Incomplete, DATA (15)]
  [TCP Segment Len: 0]
  Sequence Number: 0 (relative sequence number)
  Sequence Number (raw): 4004627101
  [Next Sequence Number: 1 (relative sequence number)]
  Acknowledgment Number: 1 (relative ack number)
  Acknowledgment number (raw): 4235169006
  1000 ... = Header Length: 32 bytes (8)
  > Flags: 0x012 (SYN, ACK)
  Window: 64240
  [Calculated window size: 64240]
  Checksum: 0xba31 [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  > Options: (12 bytes), Maximum segment size, No-Operation (NO)
  > [Timestamps]
```

122	7.889236	172.17.2.13	79.127.138.15	HTTP	577	GET /css/style.css HTTP/1.1
-----	----------	-------------	---------------	------	-----	-----------------------------

```

Ethernet II, Src: Giga-Byt_2f:9d:13 (74:56:3c:2f:9d:13), Dst:
> Destination: Stormsh_i_2a:a8:34 (00:0d:b4:2a:a8:34)
> Source: Giga-Byt_2f:9d:13 (74:56:3c:2f:9d:13)
  Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 172.17.2.13, Dst: 79.127.138
Transmission Control Protocol, Src Port: 63281, Dst Port: 80,
  Source Port: 63281
  Destination Port: 80
  [Stream index: 1]
  [Conversation completeness: Incomplete, DATA (15)]
  [TCP Segment Len: 0]
  Sequence Number: 1 (relative sequence number)
  Sequence Number (raw): 4235169006
  [Next Sequence Number: 1 (relative sequence number)]
  Acknowledgment Number: 1 (relative ack number)
  Acknowledgment number (raw): 4004627102
  0101 ... = Header Length: 20 bytes (5)
> [Flags: 0x010 (ACK)]
  Window: 255
  [Calculated window size: 65280]
  [Window size scaling factor: 256]
  Checksum: 0x87c7 [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
> [Timestamps]
  ...

```

que signifie le contenu de ce champ pour chacun des 3 segment tcp ?  
c'est la poigné a 3 vois

sa etabli un un transport plus fiable en assurant les garanties RIS

Le serveur reçoit le segment SYN et répond par un segment SYN/ACK. Il faut comprendre ce message comme étant la superposition de deux messages : « j'accepte d'ouvrir une liaison de toi vers moi » (ACK) et « je souhaite moi aussi établir une liaison vers toi » (SYN). Le client reçoit le segment SYN/ACK et répond par un segment ACK

sa etabli un un transport plus fiable en assurant les garanties RIS.