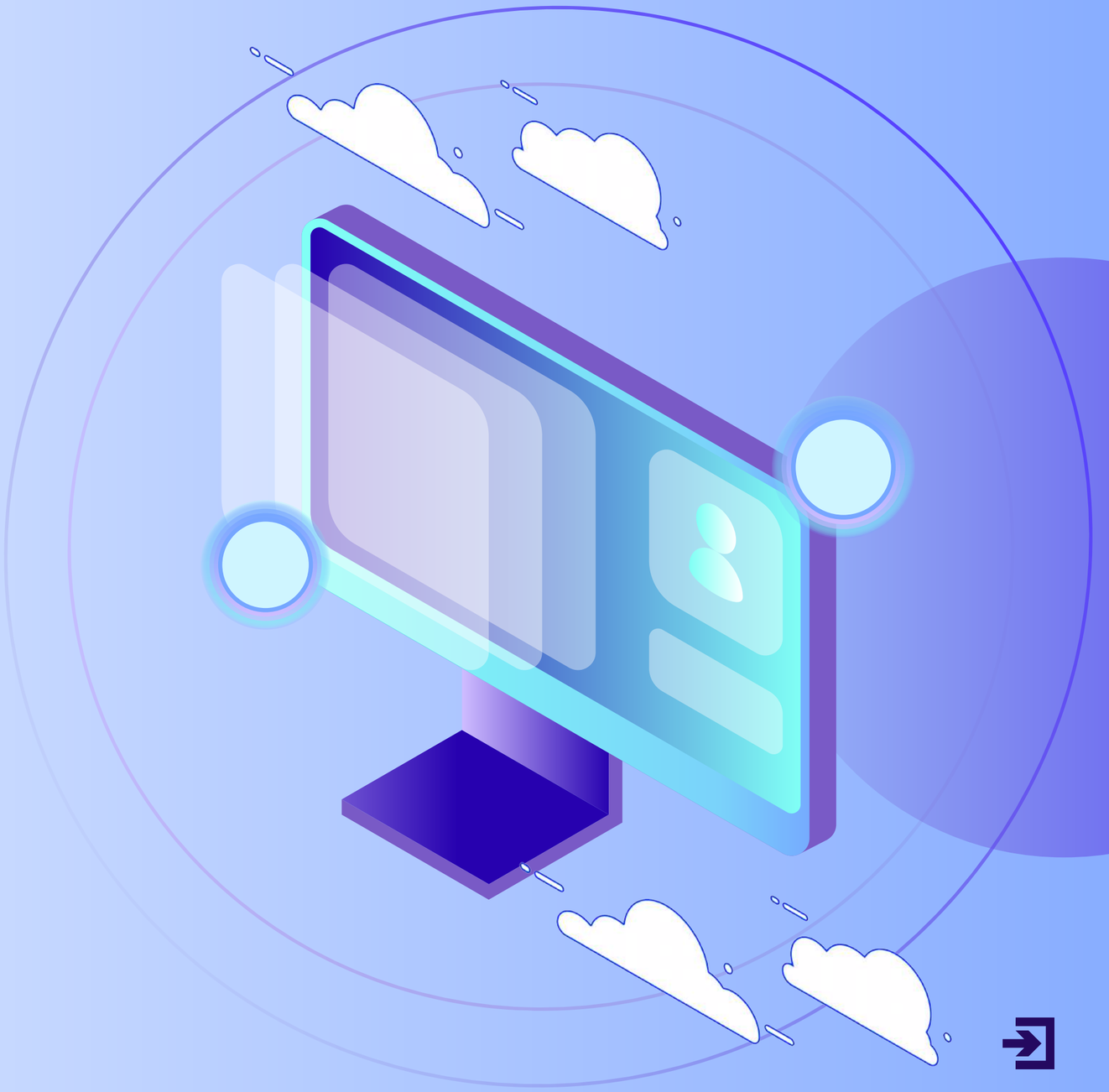
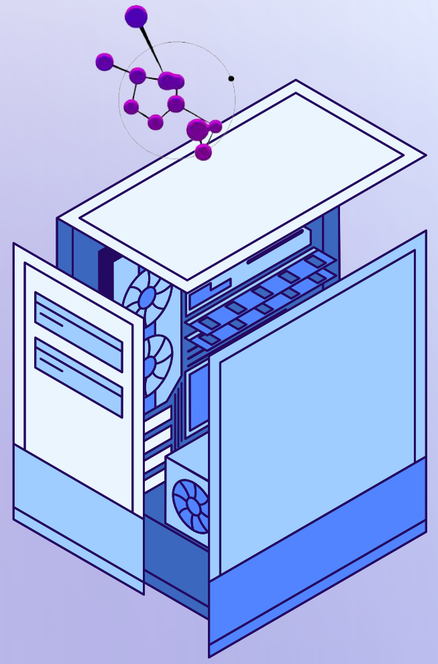
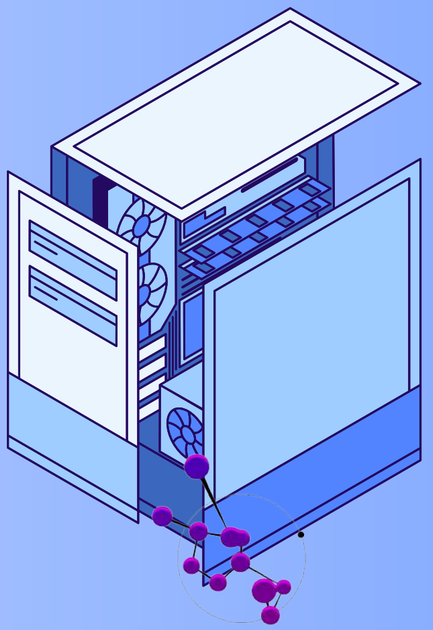
L'ÉVOLUTION DES PROTOCOLES DE CONNEXION A DISTANCE



SOMMAIRE





I/La naissance des protocoles de communication

II/Les protocoles les plus utilisées et leurs évolutions

III/Conclusion

I/

LA NAISSANCE DES PROTOCOLES DE COMMUNICATIONS

1. Code Morse

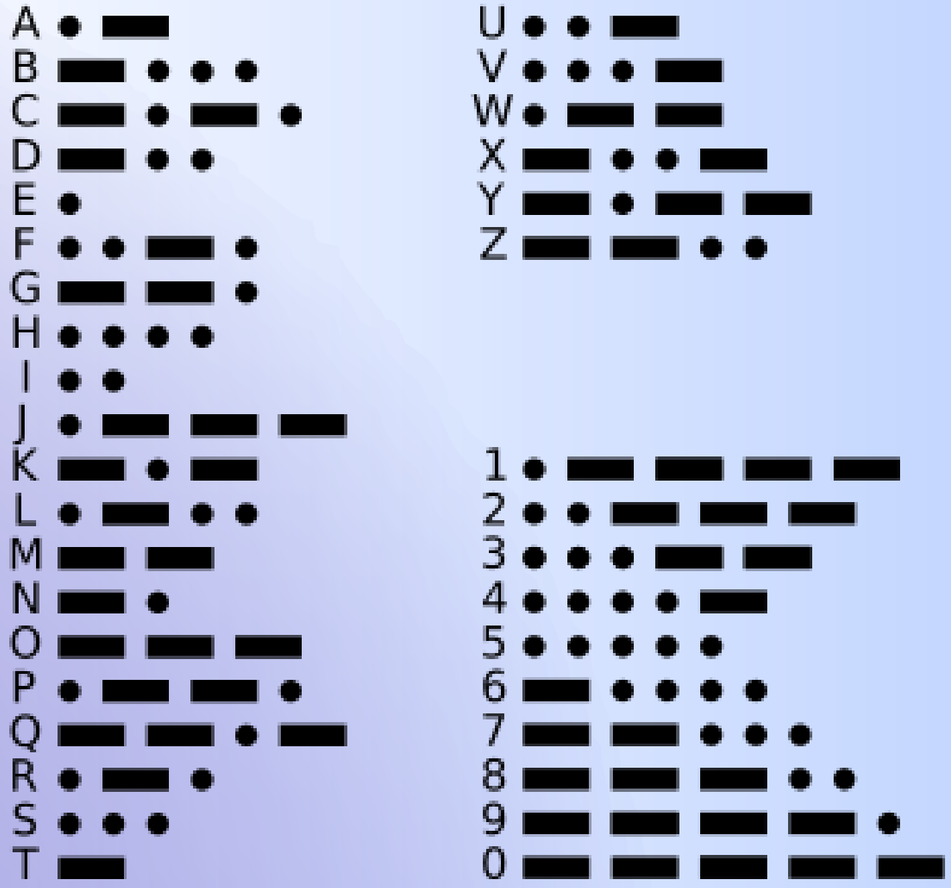
2. ARPANET Network Control Protocol (NCP)

3. TCP/IP

1. CODE MORSE

Code morse international

1. Un tiret est égal à trois points.
2. L'espacement entre deux éléments d'une même lettre est égal à un point.
3. L'espacement entre deux lettres est égal à trois points.
4. L'espacement entre deux mots est égal à sept points.

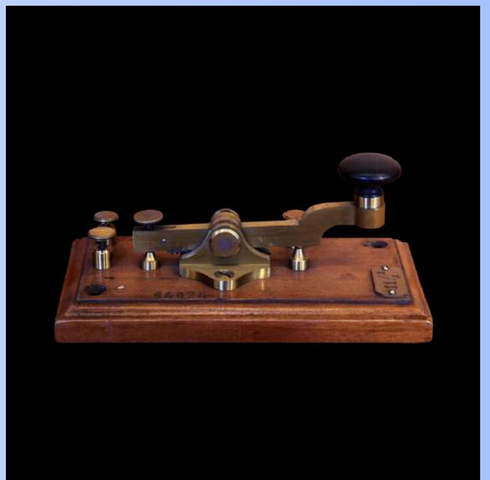


1838

Créer par Samuel Morse et Alfred Vail

Utilisation militaire

Manipulateur morse



Signal radio

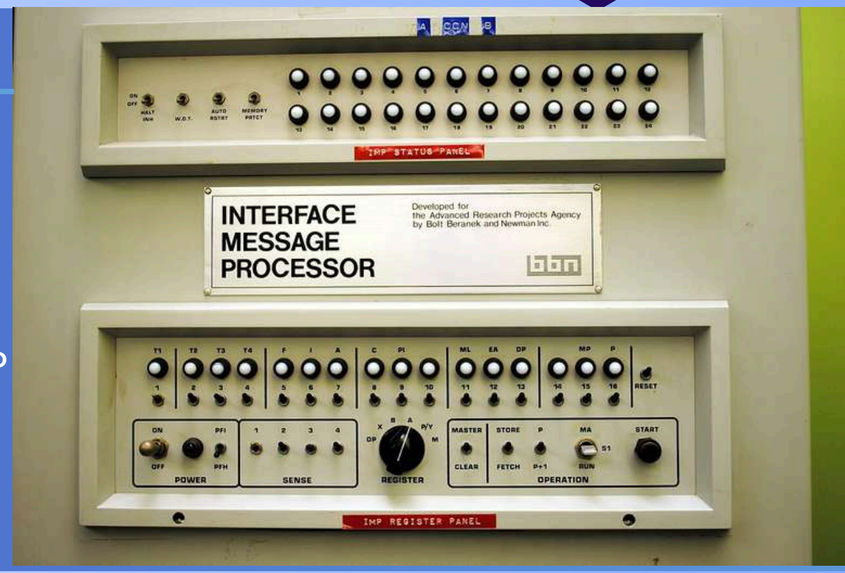
2. ARPANET NETWORK CONTROL PROTOCOL

ARPANET (Advanced Research Projects Agency Network)

Premier protocole informatique

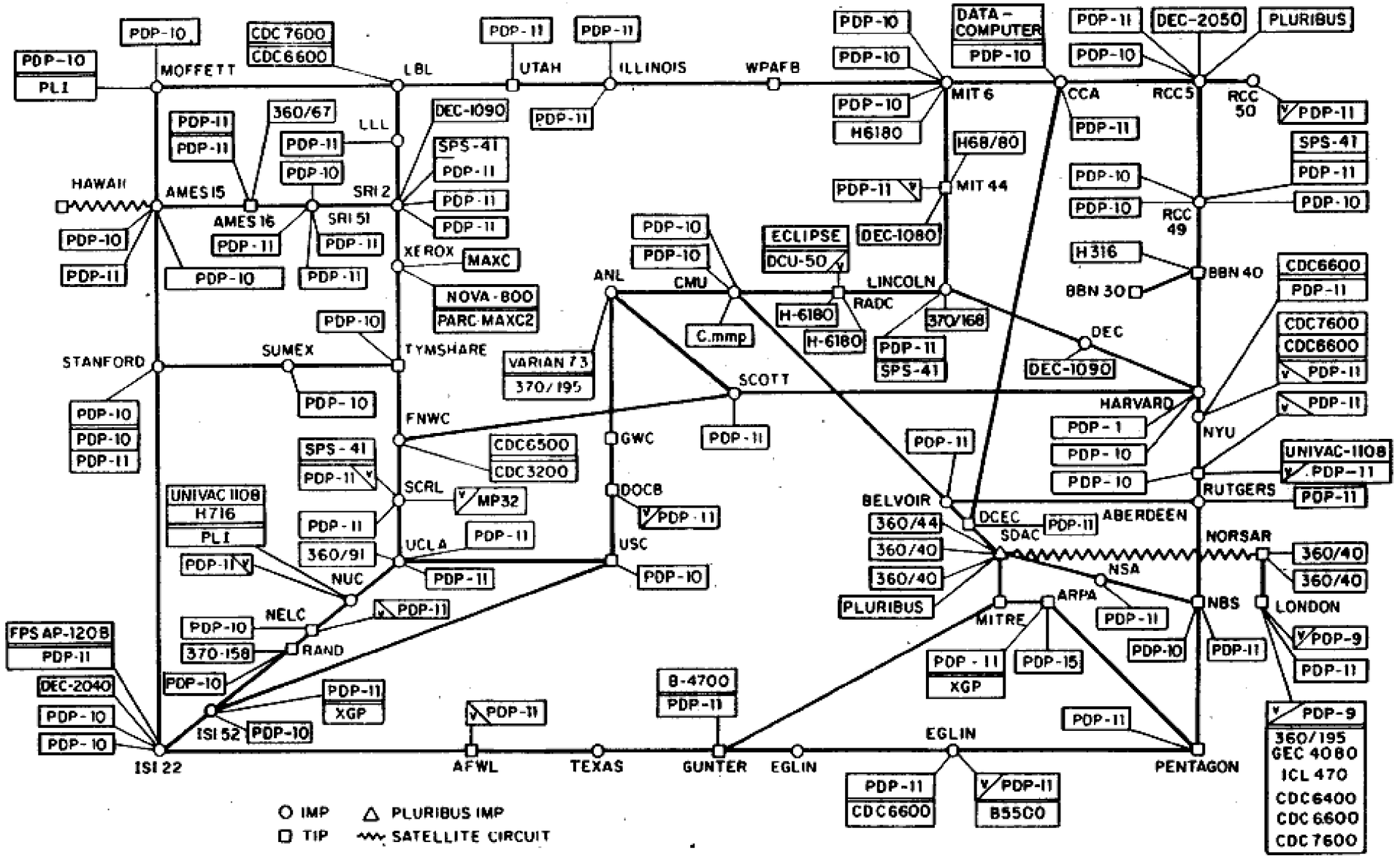
Commutation de paquets

Protocole NCP ancêtre de TCP/IP



Routeur IMP

ARPANET LOGICAL MAP, MARCH 1977



(PLEASE NOTE THAT WHILE THIS MAP SHOWS THE HOST POPULATION OF THE NETWORK ACCORDING TO THE BEST INFORMATION OBTAINABLE, NO CLAIM CAN BE MADE FOR ITS ACCURACY)

NAMES SHOWN ARE IMP NAMES, NOT (NECESSARILY) HOST NAMES

3. TCP/IP

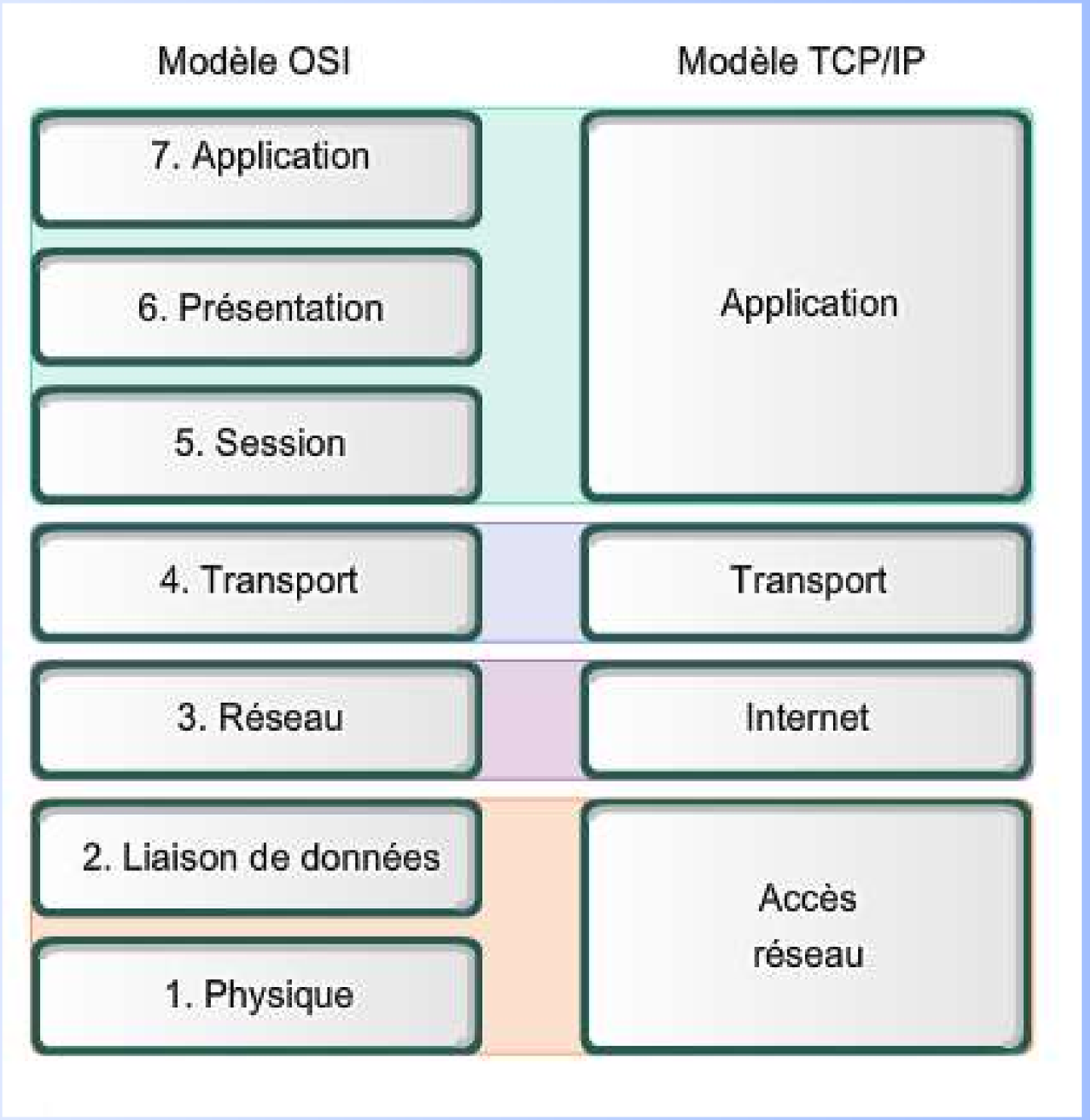
1983 --> Remplace NCP

Réutilisation des fragmentations des données

Contrôle le flux et les erreurs

Communication LAN, WAN...

Toujours utilisé aujourd'hui


Modèle OSI
Modèle TCP/IP
7. Application
6. Présentation
5. Session
Application
4. Transport
Transport
3. Réseau
Internet
2. Liaison de données
1. Physique
Accès
réseau

II/LES PROTOCOLES LES PLUS UTILISÉES ET LEURS ÉVOLUTIONS

1. **Telnet --> SSH**
2. **FTP --> SFTP ou FTPS**
3. **HTTP --> HTTPS**

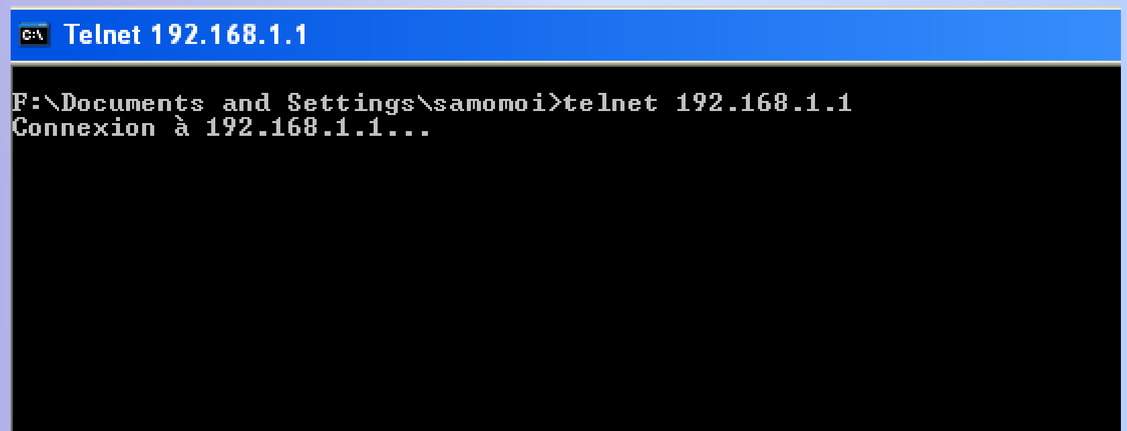
Liceria Tech

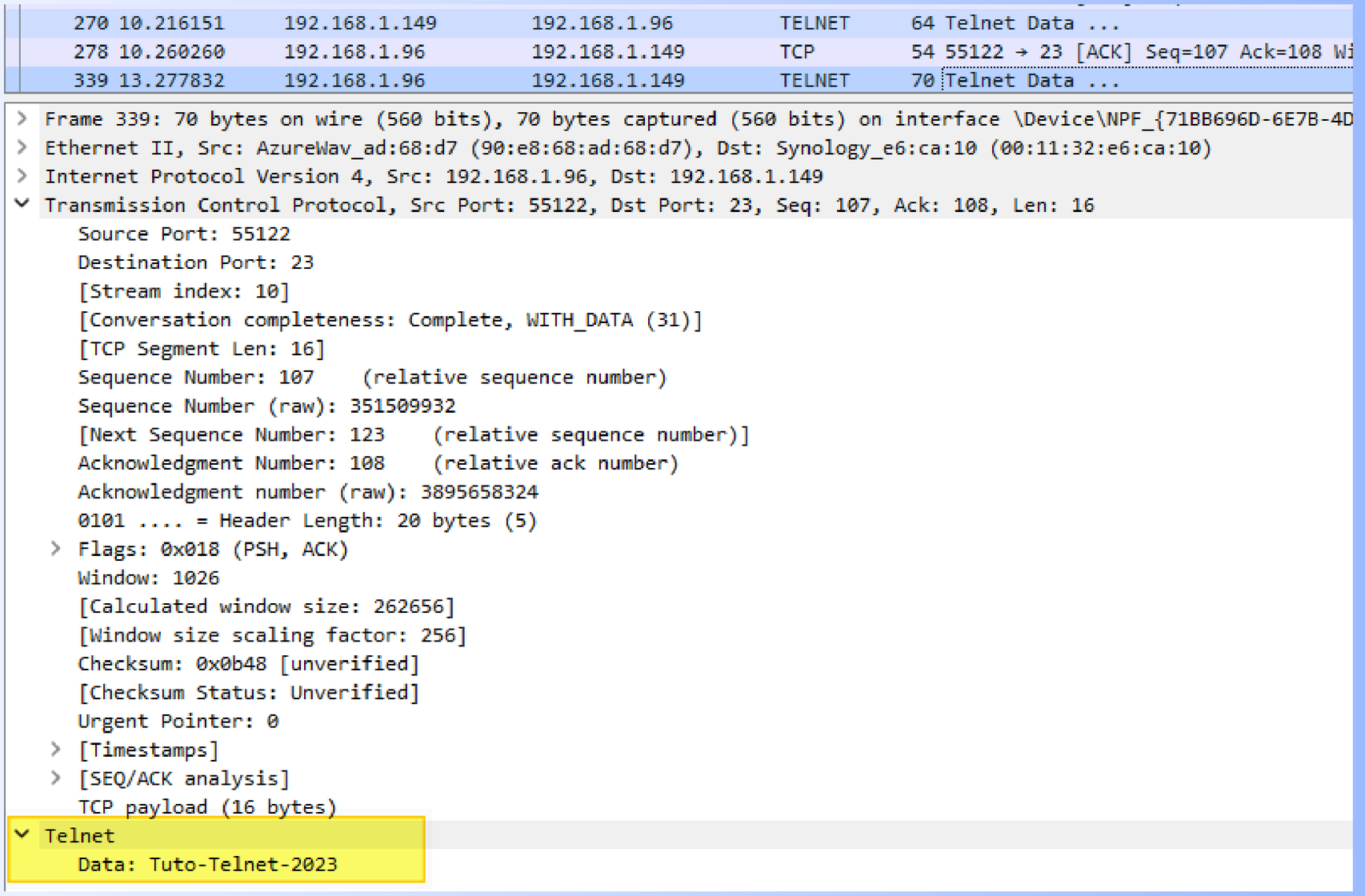
1.TELNET

Un des premiers protocoles pour accéder a distance à un ordinateur (1960) Port 23

Pas sécurisé

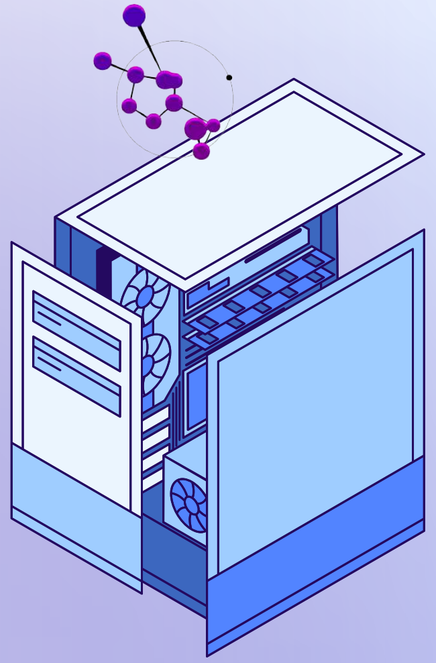
Très simple a utiliser

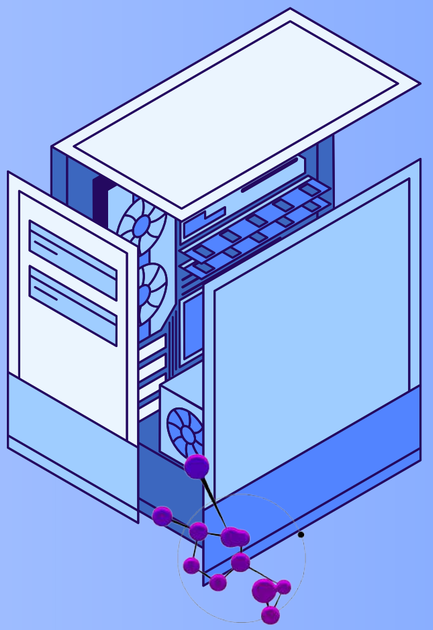



270 10.216151 192.168.1.149 192.168.1.96 TELNET 64 Telnet Data ...
278 10.260260 192.168.1.96 192.168.1.149 TCP 54 55122 → 23 [ACK] Seq=107 Ack=108 Wi
339 13.277832 192.168.1.96 192.168.1.149 TELNET 70 Telnet Data ...
Frame 339: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{71BB696D-6E7B-4D
Ethernet II, Src: AzureWav_ad:68:d7 (90:e8:68:ad:68:d7), Dst: Synology_e6:ca:10 (00:11:32:e6:ca:10)
Internet Protocol Version 4, Src: 192.168.1.96, Dst: 192.168.1.149
Transmission Control Protocol, Src Port: 55122, Dst Port: 23, Seq: 107, Ack: 108, Len: 16
Source Port: 55122
Destination Port: 23
[Stream index: 10]
[Conversation completeness: Complete, WITH_DATA (31)]
[TCP Segment Len: 16]
Sequence Number: 107 (relative sequence number)
Sequence Number (raw): 351509932
[Next Sequence Number: 123 (relative sequence number)]
Acknowledgment Number: 108 (relative ack number)
Acknowledgment number (raw): 3895658324
0101 .... = Header Length: 20 bytes (5)
Flags: 0x018 (PSH, ACK)
Window: 1026
[Calculated window size: 262656]
[Window size scaling factor: 256]
Checksum: 0x0b48 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
[Timestamps]
[SEQ/ACK analysis]
TCP payload (16 bytes)
Telnet
Data: Tuto-Telnet-2023

Liceria Tech

SSH





Sorti bien après Telnet (1995)

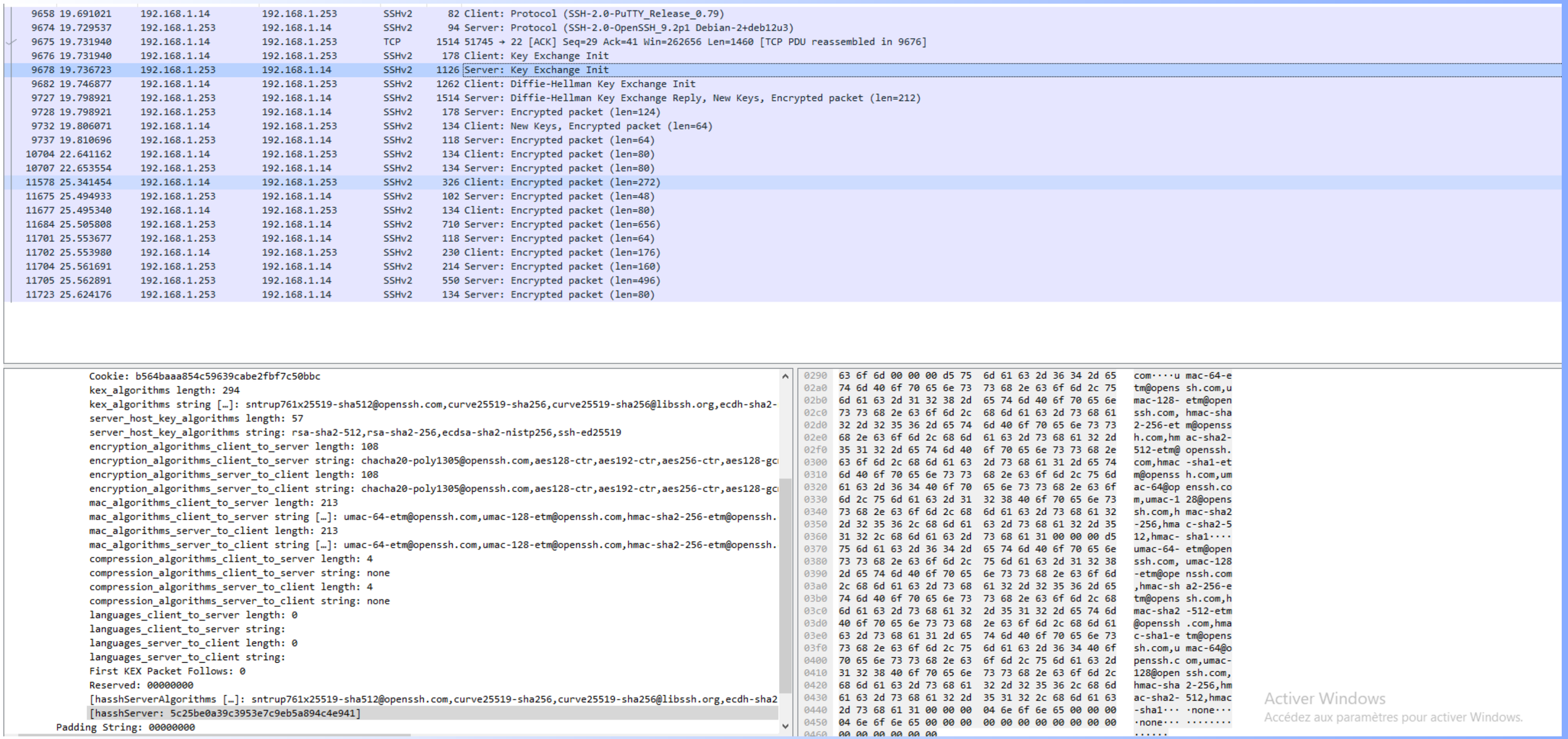
Port par défaut : 22

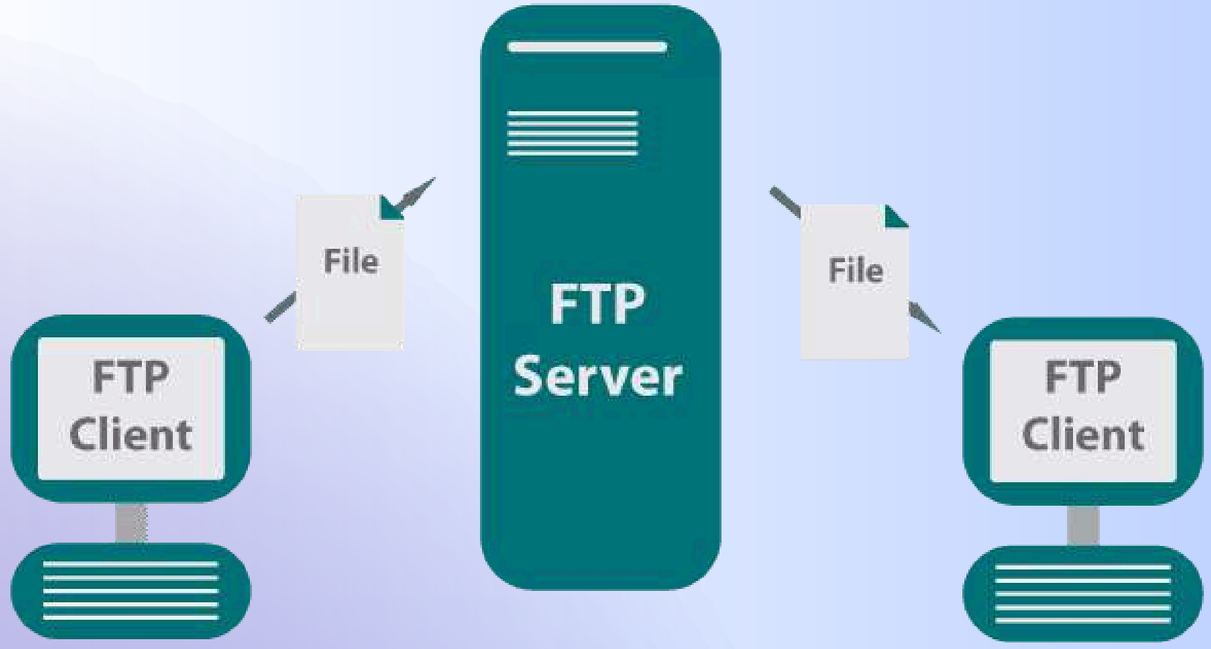
Chiffrée

/etc/ssh/sshd_config

```
C:\WINDOWS\system32>ssh 192.168.1.253
alexis@192.168.1.253's password:

C:\WINDOWS\system32>ssh -p 22 alexis@192.168.1.253
alexis@192.168.1.253's password:
```


9658 19.691021 192.168.1.14 192.168.1.253 SSHv2 82 Client: Protocol (SSH-2.0-PuTTY_Release_0.79)
9674 19.729537 192.168.1.253 192.168.1.14 SSHv2 94 Server: Protocol (SSH-2.0-OpenSSH_9.2p1 Debian-2+deb12u3)
9675 19.731940 192.168.1.14 192.168.1.253 TCP 1514 51745 → 22 [ACK] Seq=29 Ack=41 Win=262656 Len=1460 [TCP PDU reassembled in 9676]
9676 19.731940 192.168.1.14 192.168.1.253 SSHv2 178 Client: Key Exchange Init
9678 19.736723 192.168.1.253 192.168.1.14 SSHv2 1126 Server: Key Exchange Init
9682 19.746877 192.168.1.14 192.168.1.253 SSHv2 1262 Client: Diffie-Hellman Key Exchange Init
9727 19.798921 192.168.1.253 192.168.1.14 SSHv2 1514 Server: Diffie-Hellman Key Exchange Reply, New Keys, Encrypted packet (len=212)
9728 19.798921 192.168.1.253 192.168.1.14 SSHv2 178 Server: Encrypted packet (len=124)
9732 19.806071 192.168.1.14 192.168.1.253 SSHv2 134 Client: New Keys, Encrypted packet (len=64)
9737 19.810696 192.168.1.253 192.168.1.14 SSHv2 118 Server: Encrypted packet (len=64)
10704 22.641162 192.168.1.14 192.168.1.253 SSHv2 134 Client: Encrypted packet (len=80)
10707 22.653554 192.168.1.253 192.168.1.14 SSHv2 134 Server: Encrypted packet (len=80)
11578 25.341454 192.168.1.14 192.168.1.253 SSHv2 326 Client: Encrypted packet (len=272)
11675 25.494933 192.168.1.253 192.168.1.14 SSHv2 102 Server: Encrypted packet (len=48)
11677 25.495340 192.168.1.14 192.168.1.253 SSHv2 134 Client: Encrypted packet (len=80)
11684 25.505808 192.168.1.253 192.168.1.14 SSHv2 710 Server: Encrypted packet (len=656)
11701 25.553677 192.168.1.253 192.168.1.14 SSHv2 118 Server: Encrypted packet (len=64)
11702 25.553980 192.168.1.14 192.168.1.253 SSHv2 230 Client: Encrypted packet (len=176)
11704 25.561691 192.168.1.253 192.168.1.14 SSHv2 214 Server: Encrypted packet (len=160)
11705 25.562891 192.168.1.253 192.168.1.14 SSHv2 550 Server: Encrypted packet (len=496)
11723 25.624176 192.168.1.253 192.168.1.14 SSHv2 134 Server: Encrypted packet (len=80)
Cookie: b564baaa854c59639cabe2fbf7c50bbc
kex_algorithms length: 294
kex_algorithms string […]: sntrup761x25519-sha512@openssh.com,curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-
server_host_key_algorithms length: 57
server_host_key_algorithms string: rsa-sha2-512,rsa-sha2-256,ecdsa-sha2-nistp256,ssh-ed25519
encryption_algorithms_client_to_server length: 108
encryption_algorithms_client_to_server string: chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gc
encryption_algorithms_server_to_client length: 108
encryption_algorithms_server_to_client string: chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gc
mac_algorithms_client_to_server length: 213
mac_algorithms_client_to_server string […]: umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.
mac_algorithms_server_to_client length: 213
mac_algorithms_server_to_client string […]: umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.
compression_algorithms_client_to_server length: 4
compression_algorithms_client_to_server string: none
compression_algorithms_server_to_client length: 4
compression_algorithms_server_to_client string: none
languages_client_to_server length: 0
languages_client_to_server string:
languages_server_to_client length: 0
languages_server_to_client string:
First KEX Packet Follows: 0
Reserved: 00000000
[hasshServerAlgorithms […]: sntrup761x25519-sha512@openssh.com,curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2
[hasshServer: 5c25be0a39c3953e7c9eb5a894c4e941]
Padding String: 00000000
0290 63 6f 6d 00 00 00 d5 75 6d 61 63 2d 36 34 2d 65 com····u mac-64-e
02a0 74 6d 40 6f 70 65 6e 73 73 68 2e 63 6f 6d 2c 75 tm@opens sh.com,u
02b0 6d 61 63 2d 31 32 38 2d 65 74 6d 40 6f 70 65 6e mac-128- etm@open
02c0 73 73 68 2e 63 6f 6d 2c 68 6d 61 63 2d 73 68 61 ssh.com, hmac-sha
02d0 32 2d 32 35 36 2d 65 74 6d 40 6f 70 65 6e 73 73 2-256-et m@openss
02e0 68 2e 63 6f 6d 2c 68 6d 61 63 2d 73 68 61 32 2d h.com,hm ac-sha2-
02f0 35 31 32 2d 65 74 6d 40 6f 70 65 6e 73 73 68 2e 512-etm@ openssh.
0300 63 6f 6d 2c 68 6d 61 63 2d 73 68 61 31 2d 65 74 com,hmac -sha1-et
0310 6d 40 6f 70 65 6e 73 73 68 2e 63 6f 6d 2c 75 6d m@openss h.com,um
0320 61 63 2d 36 34 40 6f 70 65 6e 73 73 68 2e 63 6f ac-64@op enssh.co
0330 6d 2c 75 6d 61 63 2d 31 32 38 40 6f 70 65 6e 73 m,umac-1 28@opens
0340 73 68 2e 63 6f 6d 2c 68 6d 61 63 2d 73 68 61 32 sh.com,h mac-sha2
0350 2d 32 35 36 2c 68 6d 61 63 2d 73 68 61 32 2d 35 -256,hma c-sha2-5
0360 31 32 2c 68 6d 61 63 2d 73 68 61 31 00 00 00 d5 12,hmac- sha1····
0370 75 6d 61 63 2d 36 34 2d 65 74 6d 40 6f 70 65 6e umac-64- etm@open
0380 73 73 68 2e 63 6f 6d 2c 75 6d 61 63 2d 31 32 38 ssh.com, umac-128
0390 2d 65 74 6d 40 6f 70 65 6e 73 73 68 2e 63 6f 6d -etm@ope nssh.com
03a0 2c 68 6d 61 63 2d 73 68 61 32 2d 32 35 36 2d 65 ,hmac-sh a2-256-e
03b0 74 6d 40 6f 70 65 6e 73 73 68 2e 63 6f 6d 2c 68 tm@opens sh.com,h
03c0 6d 61 63 2d 73 68 61 32 2d 35 31 32 2d 65 74 6d mac-sha2 -512-etm
03d0 40 6f 70 65 6e 73 73 68 2e 63 6f 6d 2c 68 6d 61 @openssh .com,hma
03e0 63 2d 73 68 61 31 2d 65 74 6d 40 6f 70 65 6e 73 c-sha1-e tm@opens
03f0 73 68 2e 63 6f 6d 2c 75 6d 61 63 2d 36 34 40 6f sh.com,u mac-64@o
0400 70 65 6e 73 73 68 2e 63 6f 6d 2c 75 6d 61 63 2d penssh.c om,umac-
0410 31 32 38 40 6f 70 65 6e 73 73 68 2e 63 6f 6d 2c 128@open ssh.com,
0420 68 6d 61 63 2d 73 68 61 32 2d 32 35 36 2c 68 6d hmac-sha 2-256,hm
0430 61 63 2d 73 68 61 32 2d 35 31 32 2c 68 6d 61 63 ac-sha2- 512,hmac
0440 2d 73 68 61 31 00 00 00 04 6e 6f 6e 65 00 00 00 -sha1··· ·none···
0450 04 6e 6f 6e 65 00 00 00 00 00 00 00 00 00 00 00 ·none··· ········
0460 00 00 00 00 00 00 ··· ·····
Activer Windows
Accédez aux paramètres pour activer Windows.
Encrypted Packet […]: 2416d74a996839664b84e84a4251e0889720c842a372b6485ddf1cb8c1b164ddce18c538bbd59b3b599161af625a09ccd272918bfa6f864d2f4e09661b1153f0ba4957c9c40342217ed41d93236cbb8fe97

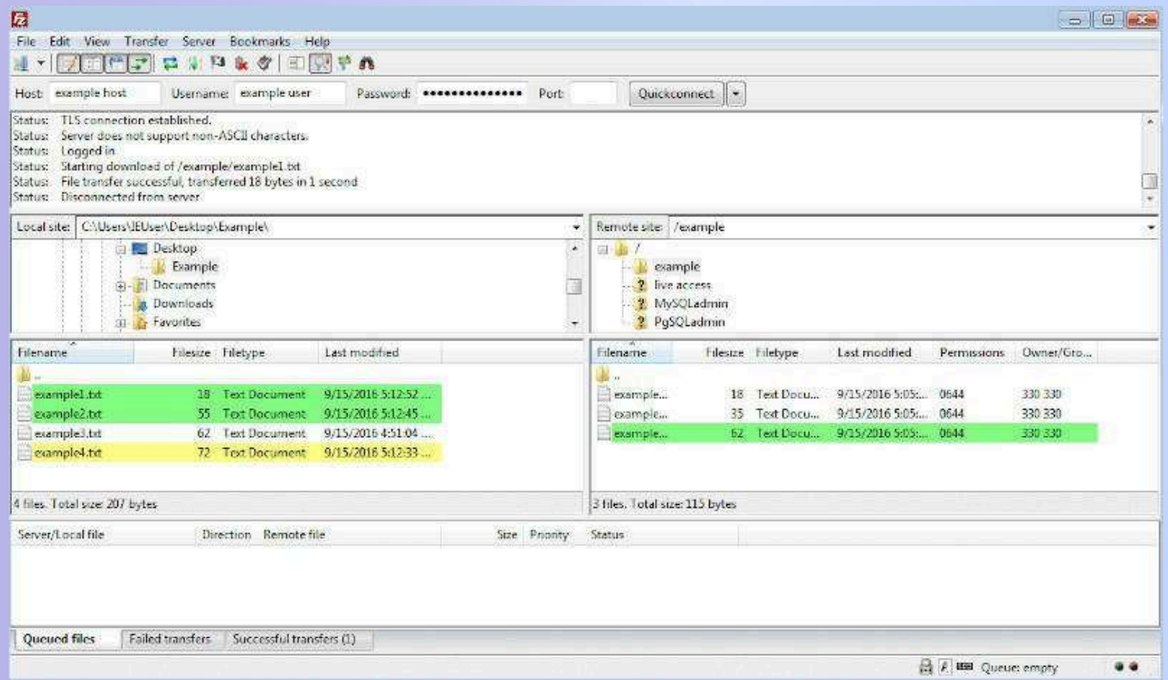


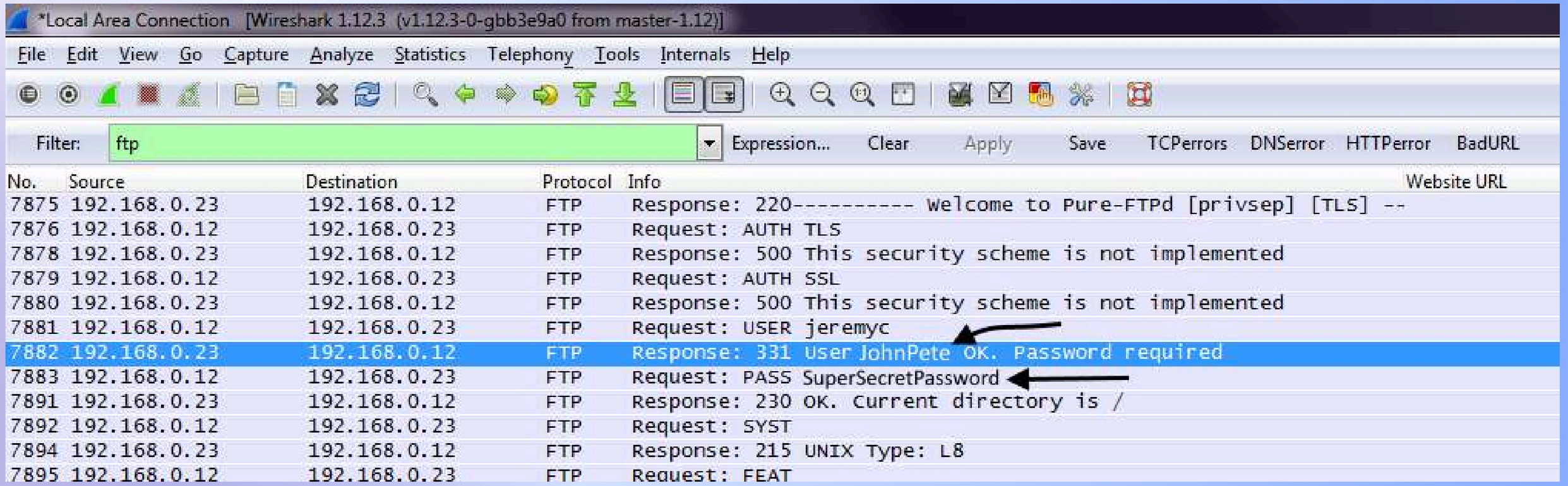
2. FTP

Logiciel : Filezilla, WinSCP, Cyberduck...

Mode actif : Client --> Serveur

Mode passif : Client initialise les commandes --> Serveur qui écoute sur un port dynamique




*Local Area Connection [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: ftp
Expression... Clear Apply Save TCPerrors DNSerror HTTPerror BadURL
No. Source Destination Protocol Info Website URL
7875 192.168.0.23 192.168.0.12 FTP Response: 220---------- Welcome to Pure-FTPd [privsep] [TLS] --
7876 192.168.0.12 192.168.0.23 FTP Request: AUTH TLS
7878 192.168.0.23 192.168.0.12 FTP Response: 500 This security scheme is not implemented
7879 192.168.0.12 192.168.0.23 FTP Request: AUTH SSL
7880 192.168.0.23 192.168.0.12 FTP Response: 500 This security scheme is not implemented
7881 192.168.0.12 192.168.0.23 FTP Request: USER jeremyc
7882 192.168.0.23 192.168.0.12 FTP Response: 331 User JohnPete OK. Password required
7883 192.168.0.12 192.168.0.23 FTP Request: PASS SuperSecretPassword
7891 192.168.0.23 192.168.0.12 FTP Response: 230 OK. Current directory is /
7892 192.168.0.12 192.168.0.23 FTP Request: SYST
7894 192.168.0.23 192.168.0.12 FTP Response: 215 UNIX Type: L8
7895 192.168.0.12 192.168.0.23 FTP Request: FEAT

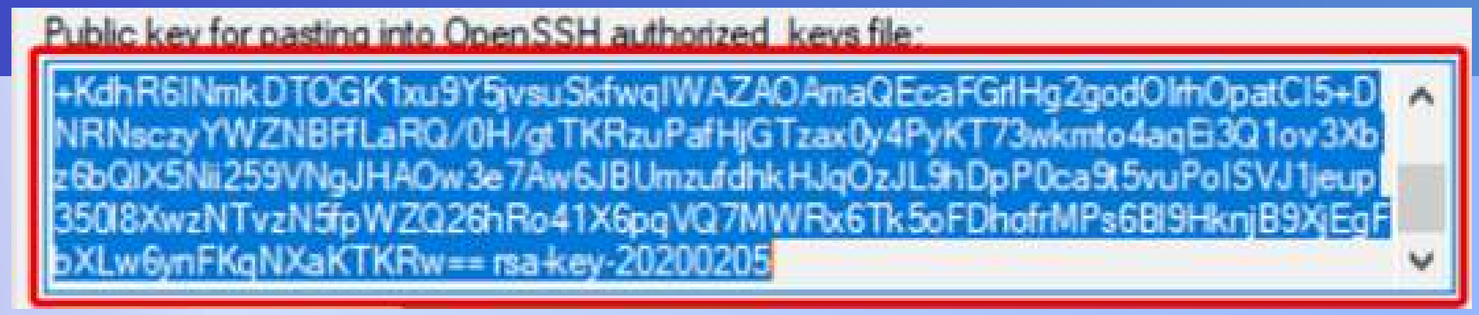
SFTP/FTPS

Evolution du FTP

FTPS --> SSL (port 21)
SFTP --> SSH (port 22)

Chiffrement des données

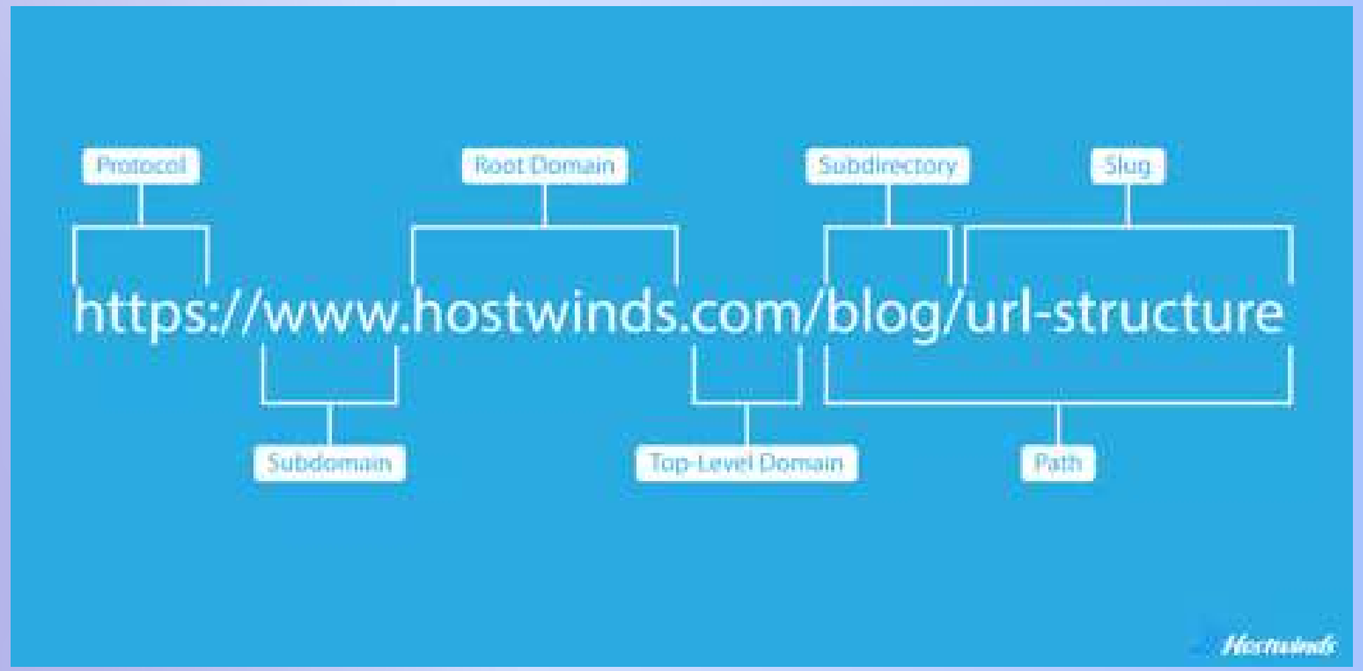
SFTP meilleur que FTPS ?

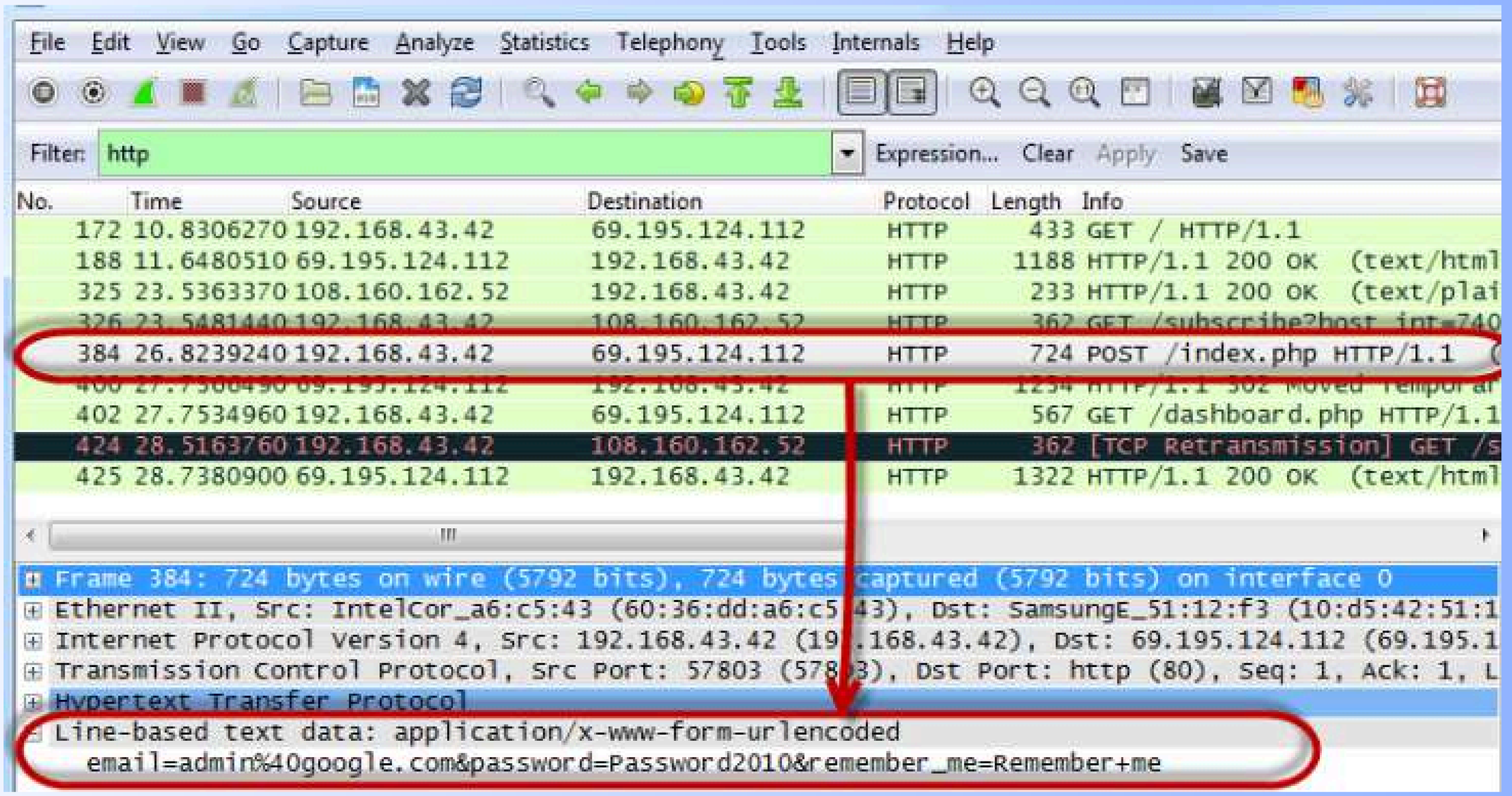


3. HTTP

HTTP (Hypertext Transfer Protocol)

GET
POST
PUT
DELETE

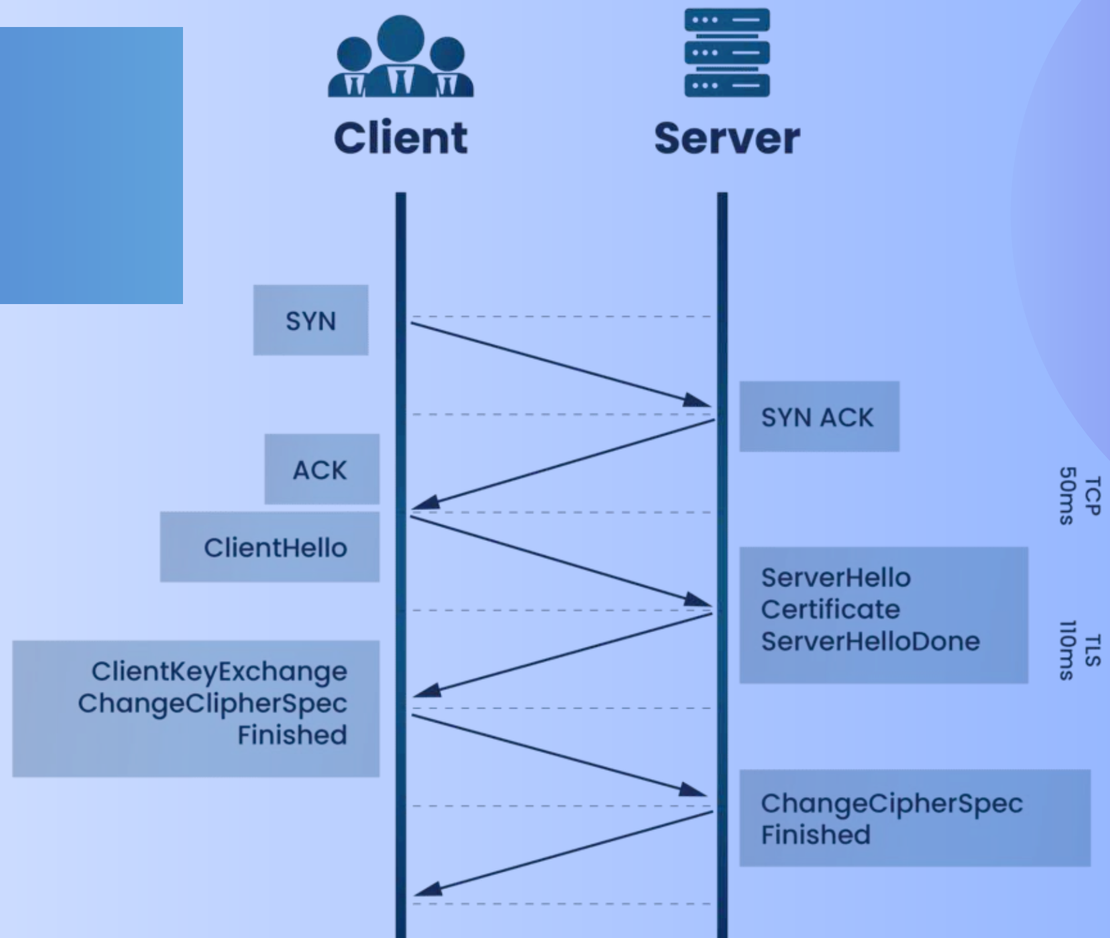



File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: http
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
172 10.8306270 192.168.43.42 69.195.124.112 HTTP 433 GET / HTTP/1.1
188 11.6480510 69.195.124.112 192.168.43.42 HTTP 1188 HTTP/1.1 200 OK (text/html
325 23.5363370 108.160.162.52 192.168.43.42 HTTP 233 HTTP/1.1 200 OK (text/plai
384 26.8239240 192.168.43.42 69.195.124.112 HTTP 724 POST /index.php HTTP/1.1
402 27.7534960 192.168.43.42 69.195.124.112 HTTP 567 GET /dashboard.php HTTP/1.1
424 28.5163760 192.168.43.42 108.160.162.52 HTTP 362 [TCP Retransmission] GET /s
425 28.7380900 69.195.124.112 192.168.43.42 HTTP 1322 HTTP/1.1 200 OK (text/html
Frame 384: 724 bytes on wire (5792 bits), 724 bytes captured (5792 bits) on interface 0
Ethernet II, Src: IntelCor_a6:c5:43 (60:36:dd:a6:c5:43), Dst: SamsungE_51:12:f3 (10:d5:42:51:1
Internet Protocol Version 4, Src: 192.168.43.42 (192.168.43.42), Dst: 69.195.124.112 (69.195.1
Transmission Control Protocol, Src Port: 57803 (57803), Dst Port: http (80), Seq: 1, Ack: 1, L
Hypertext Transfer Protocol
Line-based text data: application/x-www-form-urlencoded
email=admin%40google.com&password=Password2010&remember_me=Remember+me

HTTPS

Version amélioré de HTTP --> Plus sécurisé

SSL/TLS



CONCLUSION