

La sécurité des protocoles /Cryptographie



Les protocoles

Les protocoles doivent offrir un **échange sécurisé** et un **chiffrement des données**. On entend par échange sécurisé, une communication qui comprend : - la garantie de **Confidentialité** (l'information n'est pas accessible par un tiers autre que le destinataire) ; - l'**Authenticité** (l'expéditeur est sûr de l'identité du destinataire et inversement) ; - l'**Intégrité** (l'information n'est pas modifiée lors de la communication).

Par la suite le chiffrement des données s'effectue via des **algorithmes**. En effet ces derniers transforment l'information à l'aide de ce qu'on appelle **clefs de cryptage**, où sans ces clefs, une fois cryptée l'information devient ainsi illisible. Il existe ainsi divers types de chiffrement, le **symétrique** et l'**asymétrique**. Le symétrique impose un échange de clef (il est donc impossible d'avoir une communication qui passe en clair sur internet), où au contraire l'asymétrique lui, est efficace si l'on est sûr de l'authenticité des pairs.

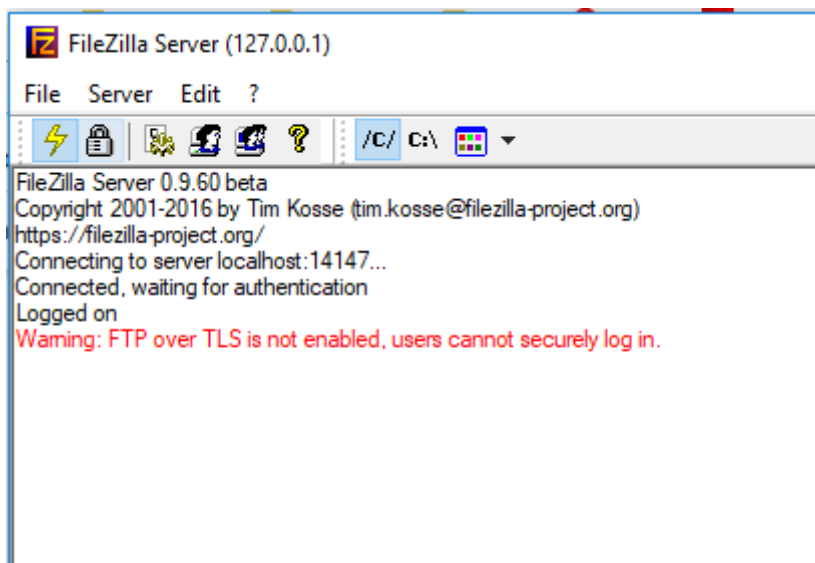
Il existe une grande variété de protocoles tels que l'HTTPS ou bien le TLS. Où par exemple l'HTTP étant un protocole d'échange web sur un réseau (internet & intranet).

L'importance de crypter

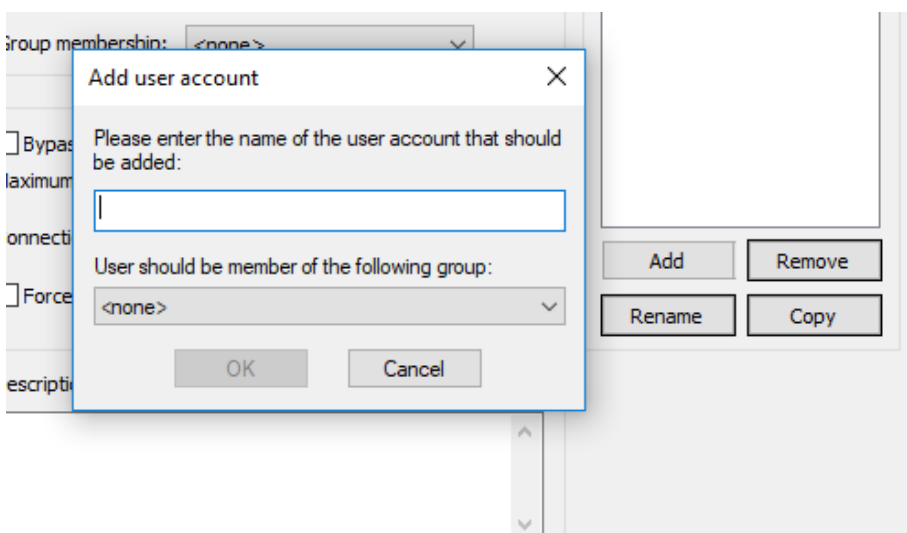
En effet, sans ces protocoles, les données lors de communication peuvent donc être interprétées par un tiers. Voici donc ci-dessous un exemple, d'une des manières où sans protocoles les données sont détournées. (De la création du serveur au piratage des données)

“Man in the Middle”
Server-Pirate-Client

Etape 1 : Ouverture du FTP serveur



Etape 2 : Création du compte



Etape 3 : Adressage du mot de passe

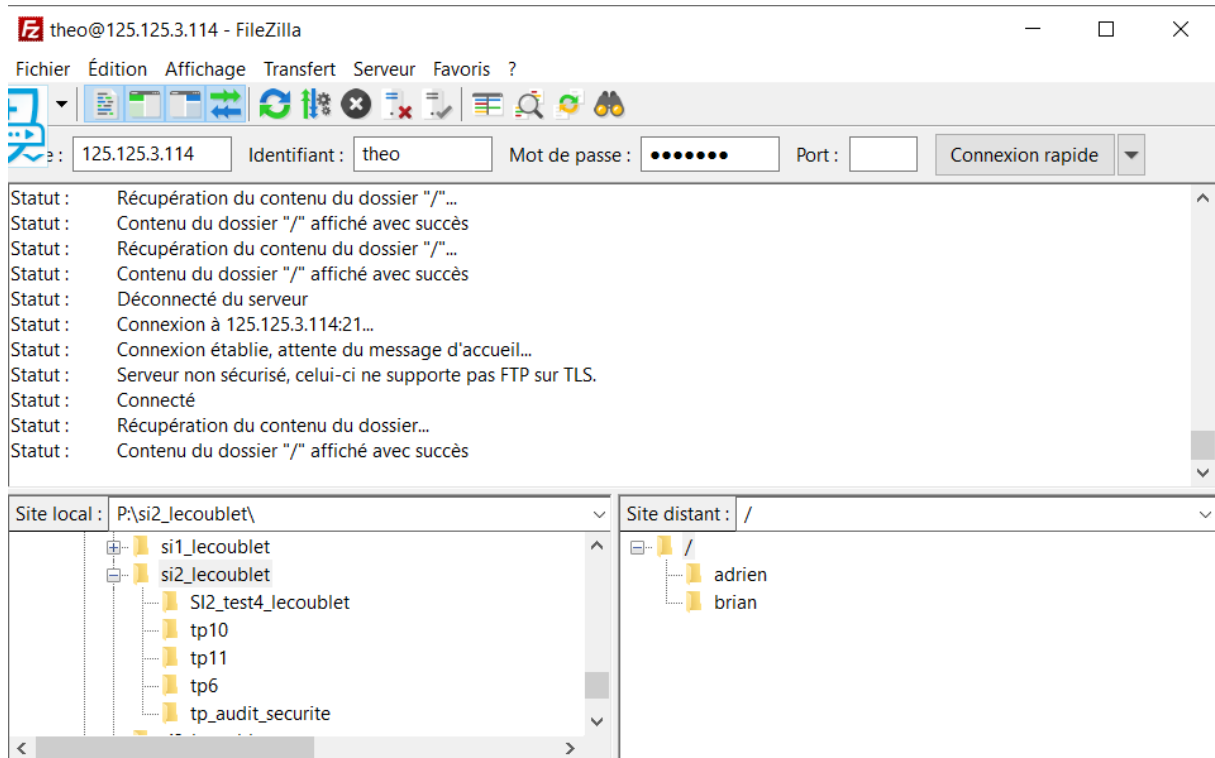
The screenshot shows the 'Users' dialog box with the 'Account settings' tab selected. On the left, a 'Page:' sidebar lists 'General', 'Shared folders', 'Speed Limits', and 'IP Filter'. The 'Account settings' section includes: 'Enable account' (checked), 'Password:' (a text box with 10 dots), 'Group membership:' (a dropdown menu showing '<none>'), 'Bypass userlimit of server' (unchecked), 'Maximum connection count:' (a text box with '0'), 'Connection limit per IP:' (a text box with '0'), and 'Force TLS for user login' (unchecked). Below this is a 'Description' text area with the placeholder text 'You can enter some comments about the user'. On the right, a 'Users' list contains the name 'theo'. At the bottom left are 'OK' and 'Cancel' buttons. At the bottom right are 'Add', 'Remove', 'Rename', and 'Copy' buttons.

Etape 4 : Don des droits d'accès aux fichiers/dossiers à l'utilisateur

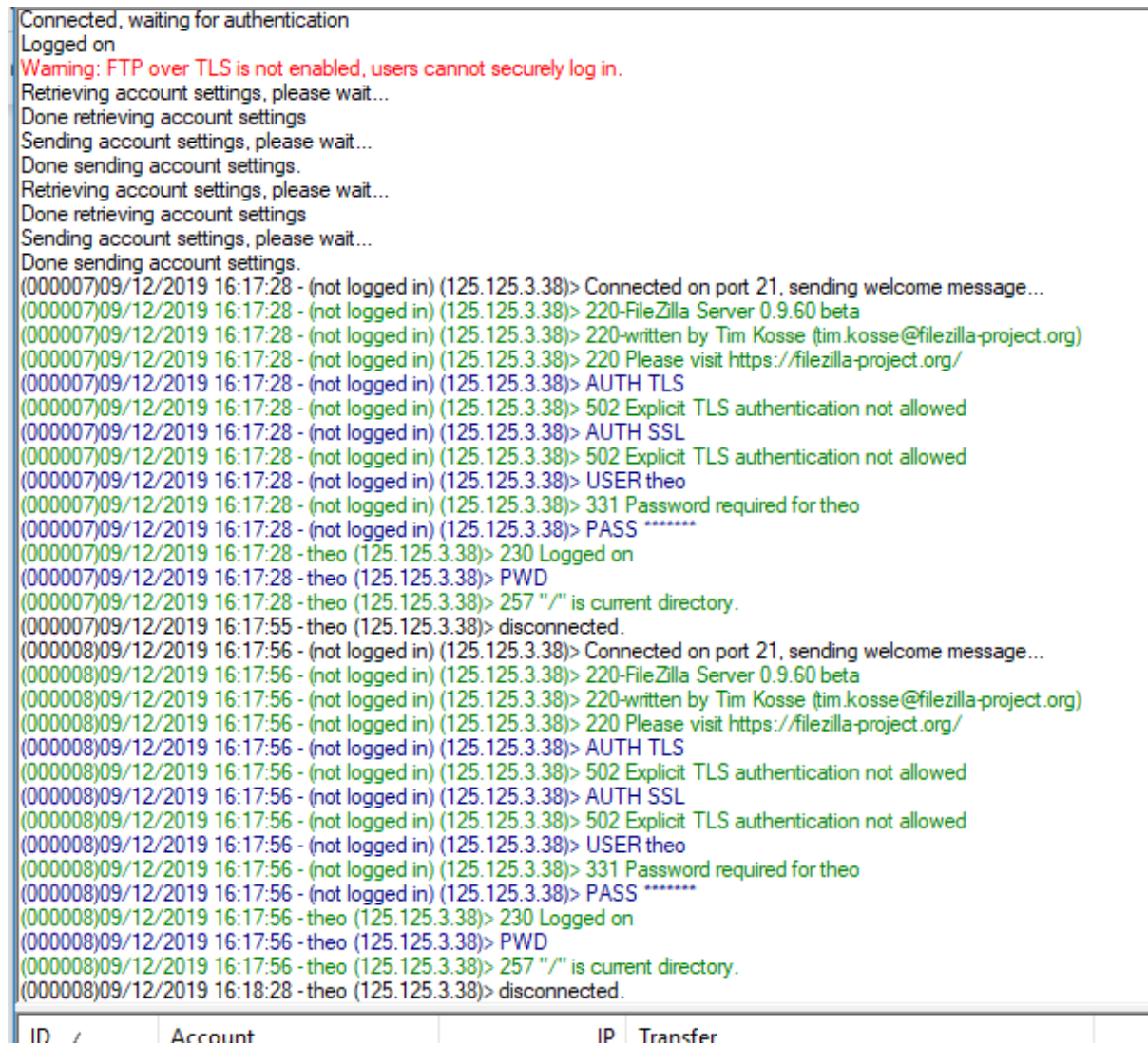
The screenshot shows the 'Users' dialog box with the 'Shared folders' tab selected. On the left, the 'Page:' sidebar lists 'General', 'Shared folders', 'Speed Limits', and 'IP Filter'. The 'Shared folders' section is divided into 'Directories' and 'Aliases' tabs. The 'Directories' list contains 'H C:\Users\ecomte...'. Below this list are 'Add', 'Remove', 'Rename', and 'Set as home dir' buttons. To the right, there are two sections of checkboxes: 'Files' (Read, Write, Delete, Append) and 'Directories' (Create, Delete, List, + Subdirs). On the right side of the dialog, the 'Users' list contains the name 'theo'. At the bottom left are 'OK' and 'Cancel' buttons. At the bottom right are 'Add', 'Remove', 'Rename', and 'Copy' buttons. Below the 'Shared folders' list, there is explanatory text: 'A directory alias will also appear at the specified location. Aliases must contain the full virtual path. Separate multiple aliases for one directory with the pipe character (|) If using aliases, please avoid cyclic directory structures, it will only confuse FTP clients.'

Etape 5 : Connexion entre le Client et le Serveur

Vue client :



Vue serveur :



Etape 6 : Connexion du pirate en parallèle de l'Etape 5 / Interception du pirate

Le pirate s'est connecté au réseau :

No.	Time	Source	Destination	Protocol	Length	Info
20	30.51609	254.247.173	239.255.255.250	SSCP	216	M-SEARCH * HTTP/1.1
21	31.51609	254.247.173	239.255.255.250	SSCP	216	M-SEARCH * HTTP/1.1
26	32.00000	169.254.247.173	169.254.255.255	Browse	220	Become Backup Browser
27	32.00000	169.254.247.173	169.254.255.250	Browse	216	M-SEARCH * HTTP/1.1
28	33.11609	254.125.55	169.254.255.255	Browse	220	Become Backup Browser
29	34.00000	169.254.247.173	169.254.255.250	Browse	216	M-SEARCH * HTTP/1.1
30	36.00000	169.254.247.173	169.254.255.250	Browse	216	M-SEARCH * HTTP/1.1
31	36.50000	169.254.247.173	169.254.255.250	Browse	216	M-SEARCH * HTTP/1.1
32	36.50000	169.254.247.173	169.254.255.250	Browse	216	M-SEARCH * HTTP/1.1
33	38.00000	169.254.247.173	169.254.255.250	Browse	216	M-SEARCH * HTTP/1.1
34	38.60000	169.254.247.173	169.254.255.250	Browse	216	M-SEARCH * HTTP/1.1
35	40.00000	169.254.247.173	169.254.255.250	Browse	216	M-SEARCH * HTTP/1.1
36	42.10000	169.254.247.173	169.254.255.250	Browse	216	M-SEARCH * HTTP/1.1
37	44.10000	169.254.247.173	169.254.255.250	Browse	216	M-SEARCH * HTTP/1.1
38	46.10000	169.254.247.173	169.254.255.250	Browse	216	M-SEARCH * HTTP/1.1
39	48.10000	169.254.247.173	169.254.255.250	Browse	216	M-SEARCH * HTTP/1.1
40	48.70000	169.254.247.173	169.254.255.250	Browse	216	M-SEARCH * HTTP/1.1
41	50.10000	169.254.247.173	169.254.255.250	Browse	216	M-SEARCH * HTTP/1.1
42	52.10000	169.254.247.173	169.254.255.250	Browse	216	M-SEARCH * HTTP/1.1
43	52.20000	169.254.247.173	169.254.255.250	Browse	216	M-SEARCH * HTTP/1.1
44	54.10000	169.254.247.173	169.254.255.250	Browse	216	M-SEARCH * HTTP/1.1
45	56.10000	169.254.247.173	169.254.255.250	Browse	216	M-SEARCH * HTTP/1.1
46	58.10000	169.254.247.173	169.254.255.250	Browse	216	M-SEARCH * HTTP/1.1
47	58.70000	169.254.247.173	169.254.255.250	Browse	216	M-SEARCH * HTTP/1.1
48	59.10000	169.254.247.173	169.254.255.250	Browse	216	M-SEARCH * HTTP/1.1
49	61.41609	254.247.173	169.254.255.250	UDP	82	55872 → 1047 Len=40
50	62.10000	169.254.247.173	169.254.255.250	Browse	216	M-SEARCH * HTTP/1.1
51	64.10000	169.254.247.173	169.254.255.250	Browse	216	M-SEARCH * HTTP/1.1
52	66.10000	169.254.247.173	169.254.255.250	Browse	216	M-SEARCH * HTTP/1.1
53	66.50000	169.254.247.173	169.254.255.250	Browse	216	M-SEARCH * HTTP/1.1
54	66.50000	169.254.247.173	169.254.255.250	Browse	216	M-SEARCH * HTTP/1.1
55	68.10000	169.254.247.173	169.254.255.250	Browse	216	M-SEARCH * HTTP/1.1
56	68.70000	169.254.247.173	169.254.255.250	Browse	216	M-SEARCH * HTTP/1.1
57	70.10000	169.254.247.173	169.254.255.250	Browse	216	M-SEARCH * HTTP/1.1
58	72.10000	169.254.247.173	169.254.255.250	Browse	216	M-SEARCH * HTTP/1.1
59	74.10000	169.254.247.173	169.254.255.250	Browse	216	M-SEARCH * HTTP/1.1
60	76.10000	169.254.247.173	169.254.255.250	Browse	216	M-SEARCH * HTTP/1.1
61	76.50000	169.254.247.173	169.254.255.250	Browse	216	M-SEARCH * HTTP/1.1
62	78.10000	169.254.247.173	169.254.255.250	Browse	216	M-SEARCH * HTTP/1.1
63	78.70000	169.254.247.173	169.254.255.250	Browse	216	M-SEARCH * HTTP/1.1
64	80.10000	169.254.247.173	169.254.255.250	Browse	216	M-SEARCH * HTTP/1.1
65	82.10000	169.254.247.173	169.254.255.250	Browse	216	M-SEARCH * HTTP/1.1

Il intercepte les paquets durant la connexion du client au serveur :

No.	Time	Source	Destination	Protocol	Length	Info
660	220.11609	254.247.173	169.254.255.250	NBNS	110	Registration NB HP06-24-200
661	226.11609	254.247.173	169.254.255.250	NBNS	110	Registration NB HP06-24-200
662	226.11609	254.247.173	169.254.255.250	NBNS	110	Registration NB D0MAD3-000
663	227.11609	254.125.55	169.254.255.250	TCP	68	55908 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
664	227.11609	254.125.55	169.254.255.250	TCP	68	[TCP Out-of-Order] 21 ← 55908 [SYN, ACK] Seq=0 Ack=1 Wm=65333 Len=0 MSS=1460 WS=256 SACK_PERM=1
665	227.11609	254.125.55	169.254.255.250	TCP	68	55908 → 21 [ACK] Seq=0 Ack=1 Wm=65333 Len=0 MSS=1460 WS=256 SACK_PERM=1
666	227.11609	254.125.55	169.254.255.250	TCP	68	[TCP Dup ACK 667] 21 ← 55908 [PSH, ACK] Seq=0 Ack=1 Wm=65333 Len=0 MSS=1460 WS=256 SACK_PERM=1
667	227.11609	254.125.55	169.254.255.250	FTP	197	Response: 220 21@211a Server 0.0.60 beta
668	227.11609	254.125.55	169.254.255.250	TCP	68	[TCP Retransmission] 21 ← 55908 [PSH, ACK] Seq=0 Ack=1 Wm=65333 Len=0 MSS=1460 WS=256 SACK_PERM=1
669	227.11609	254.125.55	169.254.255.250	FTP	64	Request: AUTH TLS
670	227.11609	254.125.55	169.254.255.250	TCP	68	[TCP Retransmission] 21 ← 55908 [PSH, ACK] Seq=0 Ack=1 Wm=65333 Len=0 MSS=1460 WS=256 SACK_PERM=1
671	227.11609	254.125.55	169.254.255.250	FTP	64	Request: AUTH TLS
672	227.11609	254.125.55	169.254.255.250	TCP	68	[TCP Retransmission] 21 ← 55908 [PSH, ACK] Seq=0 Ack=1 Wm=65333 Len=0 MSS=1460 WS=256 SACK_PERM=1
673	227.11609	254.125.55	169.254.255.250	FTP	64	Request: AUTH TLS
674	227.11609	254.125.55	169.254.255.250	TCP	68	[TCP Retransmission] 21 ← 55908 [PSH, ACK] Seq=0 Ack=1 Wm=65333 Len=0 MSS=1460 WS=256 SACK_PERM=1
675	227.11609	254.125.55	169.254.255.250	FTP	64	Request: AUTH TLS
676	227.11609	254.125.55	169.254.255.250	TCP	68	[TCP Retransmission] 21 ← 55908 [PSH, ACK] Seq=0 Ack=1 Wm=65333 Len=0 MSS=1460 WS=256 SACK_PERM=1
677	227.11609	254.125.55	169.254.255.250	FTP	89	Response: 302 Explicit TLS authentication not allowed
678	227.11609	254.125.55	169.254.255.250	TCP	68	[TCP Retransmission] 21 ← 55908 [PSH, ACK] Seq=0 Ack=1 Wm=65333 Len=0 MSS=1460 WS=256 SACK_PERM=1
679	227.11609	254.125.55	169.254.255.250	TCP	68	55908 → 21 [ACK] Seq=0 Ack=234 Wm=65333 Len=0 MSS=1460 WS=256 SACK_PERM=1
680	227.11609	254.125.55	169.254.255.250	TCP	68	[TCP Dup ACK 679] 21 ← 55908 [PSH, ACK] Seq=0 Ack=234 Wm=65333 Len=0 MSS=1460 WS=256 SACK_PERM=1
681	227.11609	254.125.55	169.254.255.250	TCP	68	[TCP Dup ACK 679] 21 ← 55908 [PSH, ACK] Seq=0 Ack=234 Wm=65333 Len=0 MSS=1460 WS=256 SACK_PERM=1
682	227.11609	254.125.55	169.254.255.250	TCP	68	[TCP Dup ACK 679] 21 ← 55908 [PSH, ACK] Seq=0 Ack=234 Wm=65333 Len=0 MSS=1460 WS=256 SACK_PERM=1
683	227.11609	254.125.55	169.254.255.250	TCP	68	[TCP Dup ACK 679] 21 ← 55908 [PSH, ACK] Seq=0 Ack=234 Wm=65333 Len=0 MSS=1460 WS=256 SACK_PERM=1
684	227.11609	254.125.55	169.254.255.250	TCP	68	[TCP Dup ACK 679] 21 ← 55908 [PSH, ACK] Seq=0 Ack=234 Wm=65333 Len=0 MSS=1460 WS=256 SACK_PERM=1
685	227.11609	254.125.55	169.254.255.250	TCP	68	[TCP Dup ACK 679] 21 ← 55908 [PSH, ACK] Seq=0 Ack=234 Wm=65333 Len=0 MSS=1460 WS=256 SACK_PERM=1
686	227.11609	254.125.55	169.254.255.250	TCP	68	[TCP Dup ACK 679] 21 ← 55908 [PSH, ACK] Seq=0 Ack=234 Wm=65333 Len=0 MSS=1460 WS=256 SACK_PERM=1
687	228.41609	254.247.173	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
688	228.41609	254.247.173	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
689	228.41609	254.247.173	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
690	228.41609	254.247.173	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
691	228.41609	254.247.173	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
692	228.41609	254.247.173	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
693	228.41609	254.247.173	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
694	228.41609	254.247.173	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
695	228.41609	254.247.173	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
696	228.41609	254.247.173	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
697	228.41609	254.247.173	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
698	228.41609	254.247.173	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
699	228.41609	254.247.173	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
700	228.41609	254.247.173	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
701	228.41609	254.247.173	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1

Plus précisément ceci :

169.254.247.173	FTP	65 Request: USER theo
169.254.247.173	TCP	65 [TCP Retransmission] 55908 → 21 [PSH, ACK] Seq=21 A
169.254.247.173	FTP	68 [TCP ACKed unseen segment] Request: PASS theo123

Ainsi il a sa disposition les informations suivante sous cette forme :

```
220-Filezilla server 0.9.60 beta
220-written by Tim Kosse (tim.kosse@filezilla-project.org)
220 Please visit https://filezilla-project.org/
AUTH TLS
502 Explicit TLS authentication not allowed
AUTH SSL
502 Explicit TLS authentication not allowed
USER theo
PASS theo123
331 Password required for theo
230 Logged on
SYST
FEAT
215 UNIX emulated by Filezilla
211-Features:
  MDTM
  REST STREAM
  SIZE
  MLST type*;size*;modify*;
  MLSD
  UTF8
  CLNT
  MFMT
  EPSV
  EPRT
211 End
PWD
TYPE I
257 "/" is current directory.
200 Type set to I
PASV
```

Entire conversation (768 bytes)

Find Save As Print ASCII EBCDIC Hex Dump C Arrays Raw

Help Filter Out This Stream Close