جامعة مولاي إسماعيل
UNIVERSITÉ MOULAY ISMAÏL

المدرسة العليا للأساتذة
ÉCOLE NORMALE SUPÉRIEURE

Livrable

Le protocole SSH sous Linux

Préparé par :

- Herraf Nadia
- Soussan Jawad

Encadré par :

Pr. Mehdi Moukhafi

C’est Quoi Telnet ?

- Le protocole Telnet (Teletype Network) a été inventé en 1969 pour se connecter à des ordinateurs distants et accéder à leurs ressources.

Les étapes pour installer telnet :

- On utilise la commande suivante pour installer les dépendances de dnf pour ne pas trouver aucun problème dans l’installation :

```
[nadiaherraf@fedora ~]$ sudo dnf install dnf-plugins-core -y
Fedora 36 openh264 (From Cisco) - x86_64                        1.2 kB/s | 989  B     00:00
Fedora 36 - x86_64 - Updates                                     34 kB/s |  41 kB     00:01
Fedora 36 - x86_64 - Updates                                    475 kB/s | 4.1 MB     00:08
Fedora Modular 36 - x86_64 - Updates                             37 kB/s |  46 kB     00:01
Le paquet dnf-plugins-core-4.1.0-1.fc36.noarch est déjà installé.
Dépendances résolues.
Rien à faire.
Terminé !
```


- On install Telnet par la commande :

```
sudo dnf install telnet telnet-server -y
```

```
[nadiaherraf@fedora ~]$ sudo dnf install telnet telnet-server
Dernière vérification de l’expiration des métadonnées effectuée il y a 0:06:21 le ven. 09 déc. 2022 15:44:12.
Dépendances résolues.
================================================================================
 Paquet                 Architecture          Version                 Dépôt    Taille
================================================================================
Installation:
 telnet                 x86_64                1:0.17-86.fc36          fedora   64 k
 telnet-server          x86_64                1:0.17-86.fc36          fedora   38 k

Résumé de la transaction
================================================================================
Installer  2 Paquets

Taille totale des téléchargements : 102 k
Taille des paquets installés : 180 k
Voulez-vous continuer ? [o/N] :
```


- On tape sur oui pour continuer :

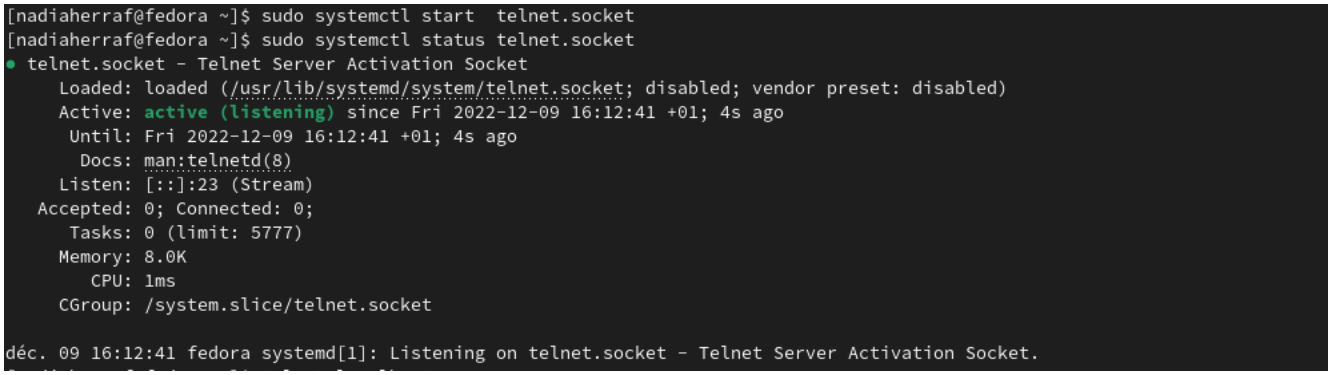
```
Voulez-vous continuer ? [o/N] : o
Téléchargement des paquets :
(1/2): telnet-server-0.17-86.fc36.x86_64.rpm                    23 kB/s |  38 kB     00:01
(2/2): telnet-0.17-86.fc36.x86_64.rpm                           36 kB/s |  64 kB     00:01
--------------------------------------------------------------------------------
Total                                                           26 kB/s | 102 kB     00:03
Test de la transaction
La vérification de la transaction a réussi.
Lancement de la transaction de test
Transaction de test réussie.
Exécution de la transaction
  Préparation          :                                                        1/1
  Installation         : telnet-server-1:0.17-86.fc36.x86_64                    1/2
  Exécution du scriptlet: telnet-server-1:0.17-86.fc36.x86_64                   1/2
  Installation         : telnet-1:0.17-86.fc36.x86_64                           2/2
  Exécution du scriptlet: telnet-1:0.17-86.fc36.x86_64                          2/2
  Vérification de      : telnet-1:0.17-86.fc36.x86_64                           1/2
  Vérification de      : telnet-server-1:0.17-86.fc36.x86_64                    2/2

Installé:
  telnet-1:0.17-86.fc36.x86_64                  telnet-server-1:0.17-86.fc36.x86_64

Terminé !
```

- Pour vérifier l'activation du Telnet on utilise la commande suivante :

```
sudo systemctl status telnet.socket
```

- S'il est inactif, on utilise la commande suivante pour l'activer :

```
sudo systemctl start telnet.socket
```



Firewall :

- On utilise la commande suivante pour ajouter une nouvelle zone dédiée pour Telnet :

```
sudo firewall-cmd --permanent --new-zone=telnet
```

- Pour spécifier les adresse IP autorisée à accéder au serveur Telnet on utilise cette commande :

```
sudo firewall-cmd --permanent --zone=telnet --add-source=1.2.3.4
```

- Une fois vous avez fini d'ajouter les adresse IP , cette commande permet d'ouvrir le port du Telnet par défaut il s'agit du port TCP23 :

```
sudo firewall-cmd --permanent --zone=telnet --add-port=23/tcp
```

- Après avoir exécuter ces commandes, on charge le firewall pour mettre en œuvre les nouvelles règles par la commande :

```
sudo firewall-cmd –reload
```

C'est quoi SSH ?

- SSH, ou Secure Shell, a été inventé par Tatu Ylönen en 1995, il est un protocole d'administration à distance qui permet aux utilisateurs de contrôler et de modifier leurs serveurs distants.
- Le service a été créé en tant que remplacement sécurisé pour le Telnet non chiffré, et utilise des techniques cryptographiques pour s'assurer que toutes les communications vers et depuis le serveur distant se produisent de manière chiffrée.

Installation de SSH :

- Mettez à jour votre système d'exploitation Fedora pour vous assurer que tous les packages existants sont à jour par la commande:

```
sudo dnf upgrade --refresh -y
```

- On install Telnet par la commande :

```
sudo dnf install openssh-server
```

```
================================================================================
 Package              Architecture  Version              Repository      Size
================================================================================
Installing:
 openssh-server       x86_64        8.7p1-3.fc35         updates        451 k

Transaction Summary
================================================================================
Install  1 Package

Total download size: 451 k
Installed size: 1.0 M
Is this ok [y/N]:
```

- Une fois installé, par défaut, cela devrait être activé, mais pour les utilisateurs qui ont déjà SSH sur leur système, vous devrez exécuter la commande enable car, par défaut, pour des raisons de sécurité, il est désactivé sur les nouvelles installations :

```
sudo systemctl enable sshd –now
```

- Pour vérifier l'activation du SSH on utilise la commande suivante :

```
Suso systemctl status sshd
```

- S'il n'est pas actif on utilise la commande suivante :

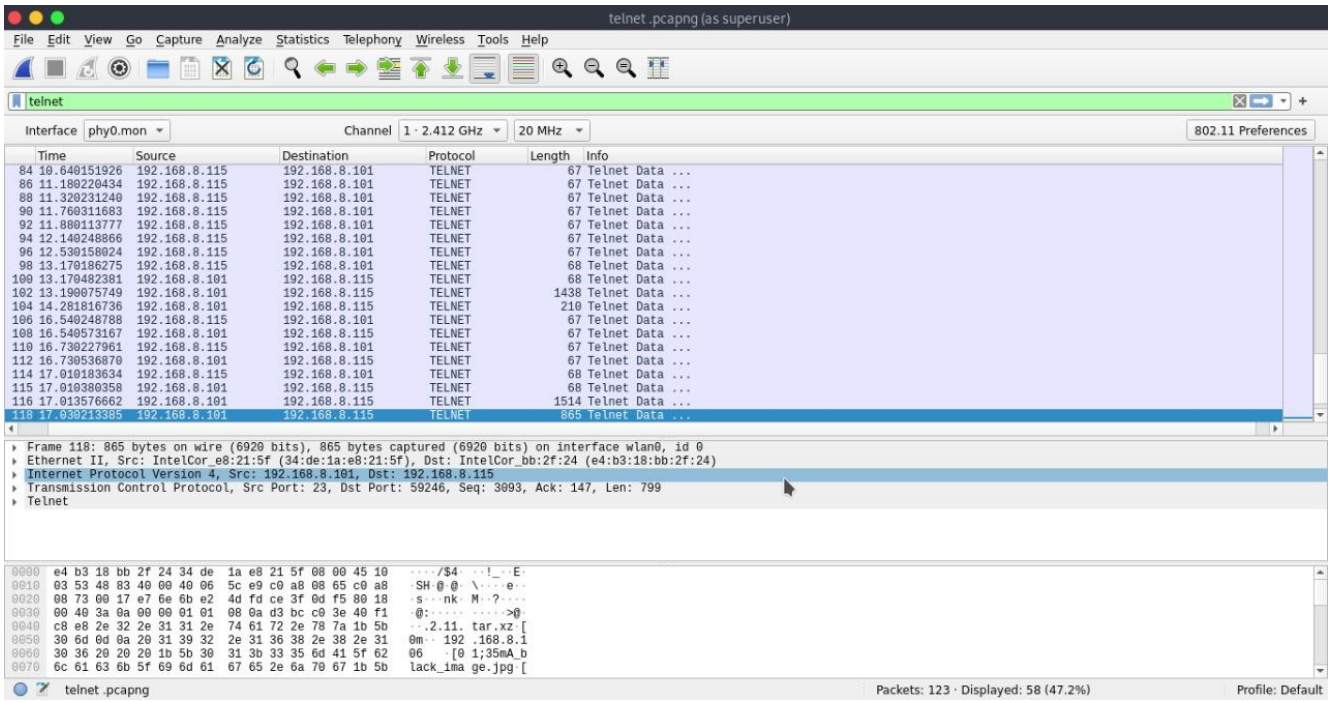
```
Suso systemctl start sshd
```

```
[nadiaherraf@fedora ~]$ systemctl status sshd
● sshd.service - OpenSSH server daemon
     Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; vendor preset: disabled)
     Active: active (running) since Tue 2022-12-13 15:30:24 +01; 4h 48min ago
       Docs: man:sshd(8)
             man:sshd_config(5)
   Main PID: 707 (sshd)
      Tasks: 1 (limit: 5777)
     Memory: 2.6M
        CPU: 40ms
     CGroup: /system.slice/sshd.service
             └─707 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

déc. 13 15:30:23 fedora systemd[1]: Starting sshd.service - OpenSSH server daemon...
déc. 13 15:30:24 fedora sshd[707]: Server listening on 0.0.0.0 port 22.
déc. 13 15:30:24 fedora sshd[707]: Server listening on :: port 22.
déc. 13 15:30:24 fedora systemd[1]: Started sshd.service - OpenSSH server daemon.
```


Wireshark :

- **Wireshark est** un outil de capture et d'analyse de paquets. Il capture le trafic du réseau local et stocke les données ainsi obtenues pour permettre leur analyse hors ligne. On l'installe avec la commande suivante :
  `sudo dnf install wireshark-devel -y`
- Interface graphique de wireshark est la suivante :

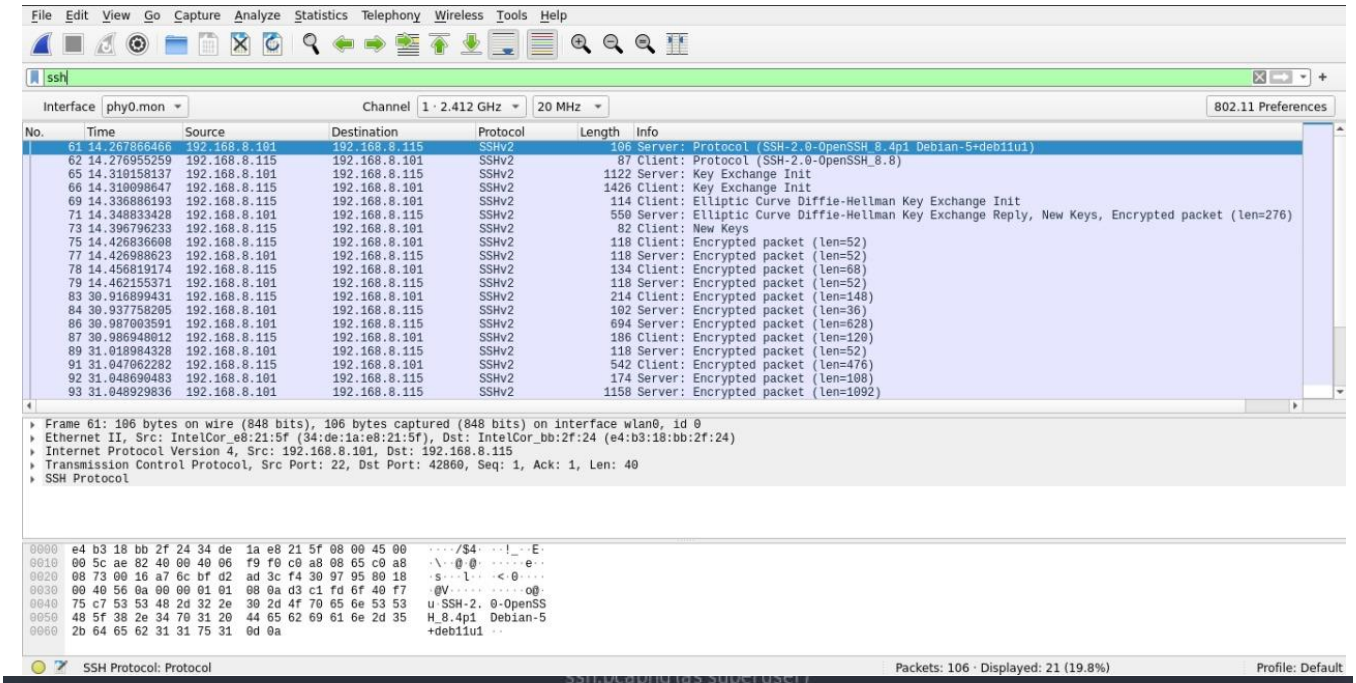
- Lorsque on transfère les information le protocole Telnet , wireshark peut capturer les données clairement :

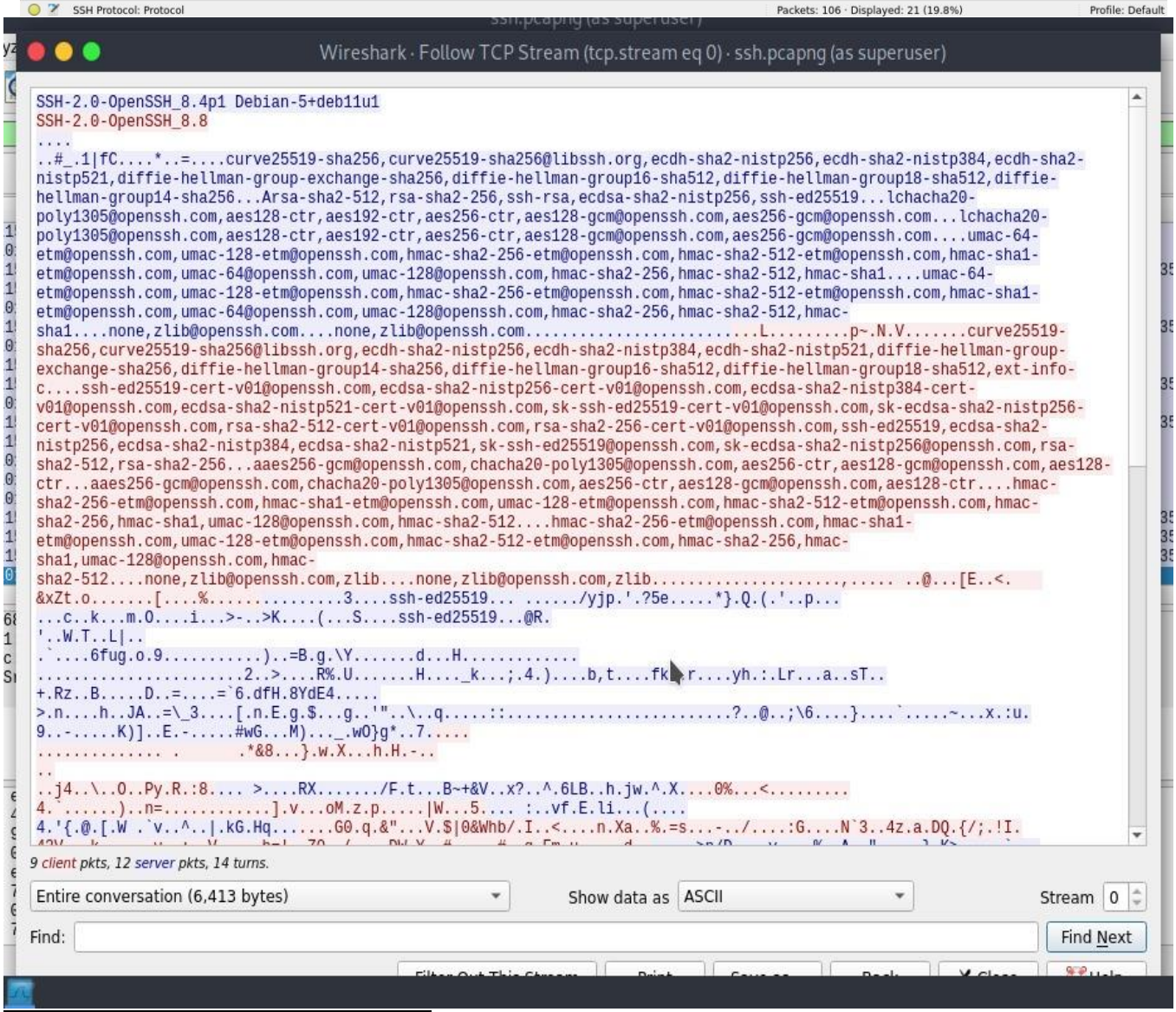


- Les informations sont non cryptées on peut les lires facilement :

```
.......... ..!.."..'.....#..... ..#..'........!.."..... .....#.....'..............&.... .38400,38400....#.fedora:
0....'..DISPLAY.fedora:0......XTERM-256COLOR..........Parrot OS 4.11
jawadsoussan-80lt login: ...jjaawwaaddssooouussssaann
.
Password: [redacted]61
.
/etc/update-motd.d/10-uname: 2: source: not found
-e
 ____                  _     ____
|  _ \ __ _ _ __ _ __ ___ | |_ / ___|  ___  ___
| |_) / _` | '__| '__/ _ \| __| \___ \ / _ \/ __|
|  __/ (_| | |  | | | (_) | |_   ___) |  __/ (__
|_|   \__,_|_|  |_|  \___/ \__| |____/ \___|\___|
```

- Par contre lorsque on utilise le protocole SSH pour transférer nos informations, on ne peut jamais savoir les informations transférés car les information sont cryptées :


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ssh
Interface phy0.mon
Channel 1 · 2.412 GHz
20 MHz
802.11 Preferences
No. Time Source Destination Protocol Length Info
61 14.267866466 192.168.8.101 192.168.8.115 SSHv2 106 Server: Protocol (SSH-2.0-OpenSSH_8.4p1 Debian-5+deb11u1)
62 14.276955259 192.168.8.115 192.168.8.101 SSHv2 87 Client: Protocol (SSH-2.0-OpenSSH_8.8)
65 14.310158137 192.168.8.101 192.168.8.115 SSHv2 1122 Server: Key Exchange Init
66 14.310098647 192.168.8.115 192.168.8.101 SSHv2 1426 Client: Key Exchange Init
69 14.336886193 192.168.8.115 192.168.8.101 SSHv2 114 Client: Elliptic Curve Diffie-Hellman Key Exchange Init
71 14.348833428 192.168.8.101 192.168.8.115 SSHv2 550 Server: Elliptic Curve Diffie-Hellman Key Exchange Reply, New Keys, Encrypted packet (len=276)
73 14.396796233 192.168.8.115 192.168.8.101 SSHv2 82 Client: New Keys
75 14.426836608 192.168.8.115 192.168.8.101 SSHv2 118 Client: Encrypted packet (len=52)
77 14.426988623 192.168.8.101 192.168.8.115 SSHv2 118 Server: Encrypted packet (len=52)
78 14.456819174 192.168.8.115 192.168.8.101 SSHv2 134 Client: Encrypted packet (len=68)
79 14.462155371 192.168.8.101 192.168.8.115 SSHv2 118 Server: Encrypted packet (len=52)
83 30.916899431 192.168.8.115 192.168.8.101 SSHv2 214 Client: Encrypted packet (len=148)
84 30.937758205 192.168.8.101 192.168.8.115 SSHv2 102 Server: Encrypted packet (len=36)
86 30.987003591 192.168.8.101 192.168.8.115 SSHv2 694 Server: Encrypted packet (len=628)
87 30.986948012 192.168.8.115 192.168.8.101 SSHv2 186 Client: Encrypted packet (len=120)
89 31.018984328 192.168.8.101 192.168.8.115 SSHv2 118 Server: Encrypted packet (len=52)
91 31.047062282 192.168.8.115 192.168.8.101 SSHv2 542 Client: Encrypted packet (len=476)
92 31.048690483 192.168.8.101 192.168.8.115 SSHv2 174 Server: Encrypted packet (len=108)
93 31.048929836 192.168.8.101 192.168.8.115 SSHv2 1158 Server: Encrypted packet (len=1092)
Frame 61: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface wlan0, id 0
Ethernet II, Src: IntelCor_e8:21:5f (34:de:1a:e8:21:5f), Dst: IntelCor_bb:2f:24 (e4:b3:18:bb:2f:24)
Internet Protocol Version 4, Src: 192.168.8.101, Dst: 192.168.8.115
Transmission Control Protocol, Src Port: 22, Dst Port: 42860, Seq: 1, Ack: 1, Len: 40
SSH Protocol
0000 e4 b3 18 bb 2f 24 34 de 1a e8 21 5f 08 00 45 00 ····/$4· ··!_··E·
0010 00 5c ae 82 40 00 40 06 f9 f0 c0 a8 08 65 c0 a8 ·\··@·@· ·····e··
0020 08 73 00 16 a7 6c bf d2 ad 3c f4 30 97 95 80 18 ·s···l·· ·<·0····
0030 00 40 56 0a 00 00 01 01 08 0a d3 c1 fd 6f 40 f7 ·@V····· ·····o@·
0040 75 c7 53 53 48 2d 32 2e 30 2d 4f 70 65 6e 53 53 u·SSH-2. 0-OpenSS
0050 48 5f 38 2e 34 70 31 20 44 65 62 69 61 6e 2d 35 H_8.4p1 Debian-5
0060 2b 64 65 62 31 31 75 31 0d 0a +deb11u1 ··
SSH Protocol: Protocol
Packets: 106 · Displayed: 21 (19.8%)
Profile: Default


Wireshark · Follow TCP Stream (tcp.stream eq 0) · ssh.pcapng (as superuser)
SSH-2.0-OpenSSH_8.4p1 Debian-5+deb11u1
SSH-2.0-OpenSSH_8.8
....
..#_.1|fC....*..=....curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,diffie-hellman-group14-sha256...Arsa-sha2-512,rsa-sha2-256,ssh-rsa,ecdsa-sha2-nistp256,ssh-ed25519...lchacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com...lchacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com....umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@openssh.com,umac-128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha1....umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@openssh.com,umac-128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha1....none,zlib@openssh.com....none,zlib@openssh.com.....L.....p~.N.V.....curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group14-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,ext-info-c....ssh-ed25519-cert-v01@openssh.com,ecdsa-sha2-nistp256-cert-v01@openssh.com,ecdsa-sha2-nistp384-cert-v01@openssh.com,ecdsa-sha2-nistp521-cert-v01@openssh.com,sk-ssh-ed25519-cert-v01@openssh.com,sk-ecdsa-sha2-nistp256-cert-v01@openssh.com,rsa-sha2-512-cert-v01@openssh.com,rsa-sha2-256-cert-v01@openssh.com,ssh-ed25519,ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521,sk-ssh-ed25519@openssh.com,sk-ecdsa-sha2-nistp256@openssh.com,rsa-sha2-512,rsa-sha2-256...aaes256-gcm@openssh.com,chacha20-poly1305@openssh.com,aes256-ctr,aes128-gcm@openssh.com,aes128-ctr...aaes256-gcm@openssh.com,chacha20-poly1305@openssh.com,aes256-ctr,aes128-gcm@openssh.com,aes128-ctr....hmac-sha2-256-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha2-256,hmac-sha1,umac-128@openssh.com,hmac-sha2-512....hmac-sha2-256-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha2-256,hmac-sha1,umac-128@openssh.com,hmac-sha2-512....none,zlib@openssh.com,zlib....none,zlib@openssh.com,zlib.....,..... ..@...[E..<.
&xZt.o.....[....%.....3....ssh-ed25519... ...../yjp.'.?5e.....*}.Q.(.'..p...
...c..k...m.O....i...>-..>K....(...S....ssh-ed25519...@R.
'..W.T..L|..
.`....6fug.o.9.....)..=B.g.\Y.....d...H.....
.....2..>....R%.U.....H...._k...;.4.)....b,t....fk.r....yh.:.Lr...a..sT..
+.Rz..B.....D..=....=`6.dfH.8YdE4.....
>.n....h..JA..=_3....[.n.E.g.$...g..'"..\..q.....::.....?..@..;\6....}....`.....~...x.:u.
9..-.....K)]..E.-.....#wG...M)..._.wO}g*..7....
....*&8...}.w.X...h.H.-..
..
..j4..\..O..Py.R.:8.... >....RX...../F.t...B~+&V..x?..^.6LB..h.jw.^.X....0%...<.....
4.`.....)..n=.....].v...oM.z.p.....|W...5.... :..vf.E.li...(....
4.'{.@.[.W .`v..^..|.kG.Hq.....G0.q.&"...V.$|0&Whb/.I..<....n.Xa..%.=s...-../....:G....N`3..4z.a.DQ.{/;.!I.
9 client pkts, 12 server pkts, 14 turns.
Entire conversation (6,413 bytes)
Show data as ASCII
Stream 0
Find:
Find Next

Les sources :

- https://www.linuxcapable.com/install-enable-connect-to-ssh-on-fedora-linux-35/
- https://www.linuxcapable.com/how-to-install-telnet-on-fedora-36-linux/
- https://waytolearnx.com/2017/12/difference-entre-ssh1-et-ssh2.html
- https://www.youtube.com/watch?v=iCb5r37I8iU