SSH használata Linuxon

Linux alapok

Varga Tibi 2020

SSH - Secure Shell

- A Secure Shell (röviden: SSH) egy szabványcsalád, és egyben egy protokoll is, amelyet a kliens és a szerver közötti biztonságos kapcsolatra használnak.
- Ha a szerveren engedélyezve van a belépés a felhasználónknak, és a kliensgépen telepítve van egy SSH kliens program is, akkor parancssoros felületen keresztül beléphetünk távoltól egy szerveren parancssoros módban.
- Támogatja a tunnelinget, azaz X11 grafikus ablak is kapcsolható (ha távoligépen engedélyezett és alkalmazható)
- Az SSH fájlok biztonságos átvitelére is használható a kapcsolódó SFTP (Secure FTP) és SCP (Secure Copy) protokollok segítségéve

SSH Szerver

- A távoli gépen rendelkezni kell egy SSH szerver alkalmazásnak amihez kapcsolódunk.
- Az SSH szerver alapértelmezés szerint nincs telepítve a legtöbb asztali Linux rendszeren, de könnyen telepíthető a szokásos módon.
- Az SSH telepítéséhez és engedélyezéséhez debian alapú rendszere:

```
$ sodo apt install openssh-server
```

- A telepítés befejezése után az SSH szolgáltatás automatikusan elindul. SSH-kiszolgáló állapotának ellenőrzése:

```
$ sudo systemctl status ssh
```

- Amennyiben tűzfal aktív engedélyezzük a az SSH-t:

```
$ sudo ufw allow ssh
```

Az SSH letiltása és engedélyezése

- Ha valamilyen okból meg szeretné tiltani az SSH-t az akkor egyszerűen leállíthatja az SSH szolgáltatást:

```
$ sudo systemctl stop ssh
```

Az újraindítás :

```
$ sudo systemctl start ssh
```

- Az SSH szolgáltatás letiltásához az indításhoz a rendszer indításakor:

```
$ sudo systemctl disable ssh
```

- Az újbóli engedélyezéshez írja be:

```
$ sudo systemctl enable ssh
```

SSH / OpenSSH / Konfigurálás

- Az OpenSSH szervert konfigurálnia kell az **sshd_config** fájl szerkesztésével ami az **/etc /ssh** könyvtárban található.

- Az **sshd**_config az OpenSSH szerver konfigurációs fájlja
- Az ssh_config az OpenSSH kliens konfigurációs fájlja . Ügyelj arra, hogy ne kevered össze.

Néhány módosíthatóbeállítás az *sshd _config* fájlban :

- Módosítsa a Port direktívát a következőre az OpenSSH beállításához a 2222-es TCP port figyelésére az alapértelmezett 22-es TCP port helyett:

  Port 2222

- Ahhoz, hogy az sshd engedélyezze a nyilvános kulcs alapú bejelentkezést, vegye fel vagy módosítsa a következő sort az /etc/ssh/sshd_config fájlba:

  PubkeyAuthentication yes

ha pedig már tartalmazza, ellenőrizd, hogy a sor nincs megjegyzésben (nincs előtte #).

- Mivel sok SSH szerverrel rendelkező ember gyenge jelszavakat használ, sok online támadó SSH szervert keres, majd véletlenszerűen találgatni kezdi a jelszavakat. A támadó több ezer jelszót próbálhat ki egy óra alatt, ezért zélszerő letiltani a jelszó alapu bejelentkezést:

  PasswordAuthentication no

SSH kulcs

- Az SSH lehetővé teszi a hitelesítést két gazdagép között jelszó nélkül kulcsok segitségével.
- Egy nyilvános és egy titkos kulcsot kell elképzelni, melyek gyakorlatilag kódolt szövegek. A titkos kulcsot titokban kell tartani valahol a saját kliensgépünkön, ahol más nem fér hozzá. A nyilvános kulcsot pedig egy távoli szerverre kell eljuttatni, ahova majd be szeretnénk lépni jelszó nélkül.
- Ennek a kettőnek a segítségével a kliens és a szerver biztonságosan meg tudja beszélni egymással, hogy a felhasználó beléphet-e. Az erre felhasználható publikus kulcsokat a szerveren a felhasználóhoz tartozó "AuthorizedKeysFile" beállításnak megfelelő fájlban találhatjuk.

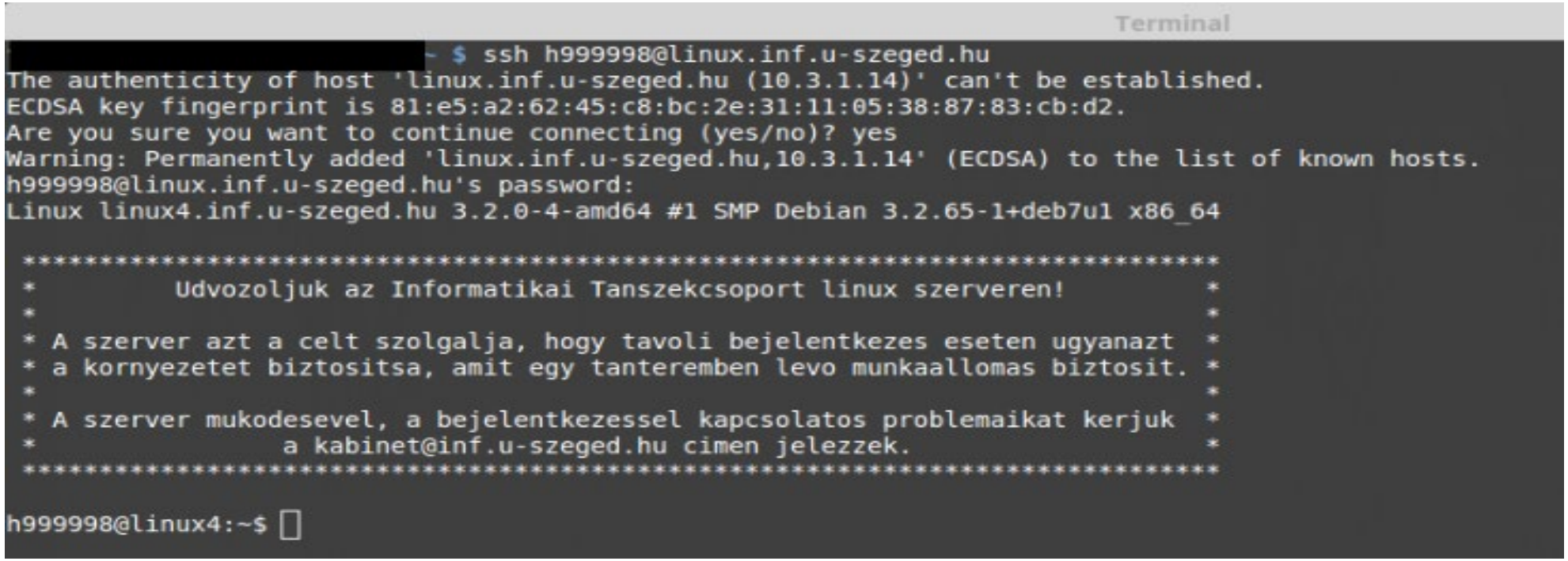
Csatlakozás SSH-hoz hálózaton

- LAN-on keresztüli csatlakozáshoz az Linux géphez csak a következő parancsot kell megadni:

```
$ ssh username@ip_address
$ ssh username@domain_name
```

vagy

Jelszavas bejelentkezés esetén jelszó begépeléskor nem jelenik meg

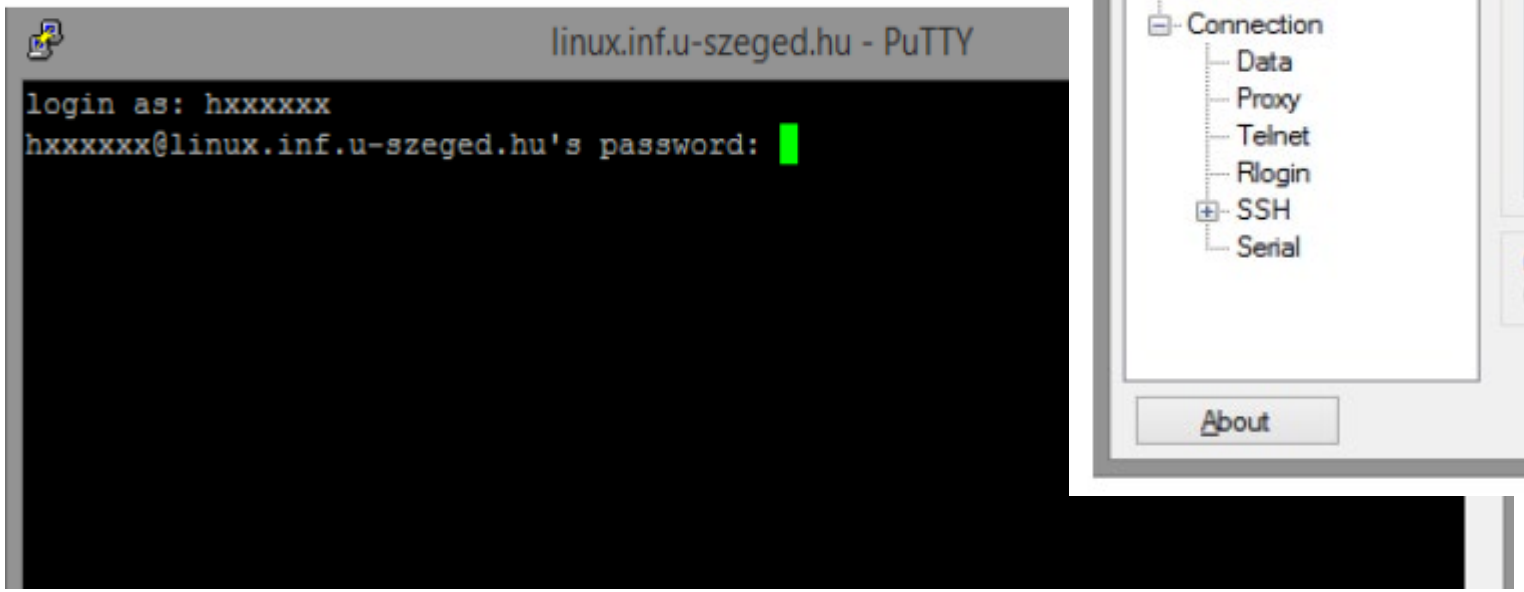


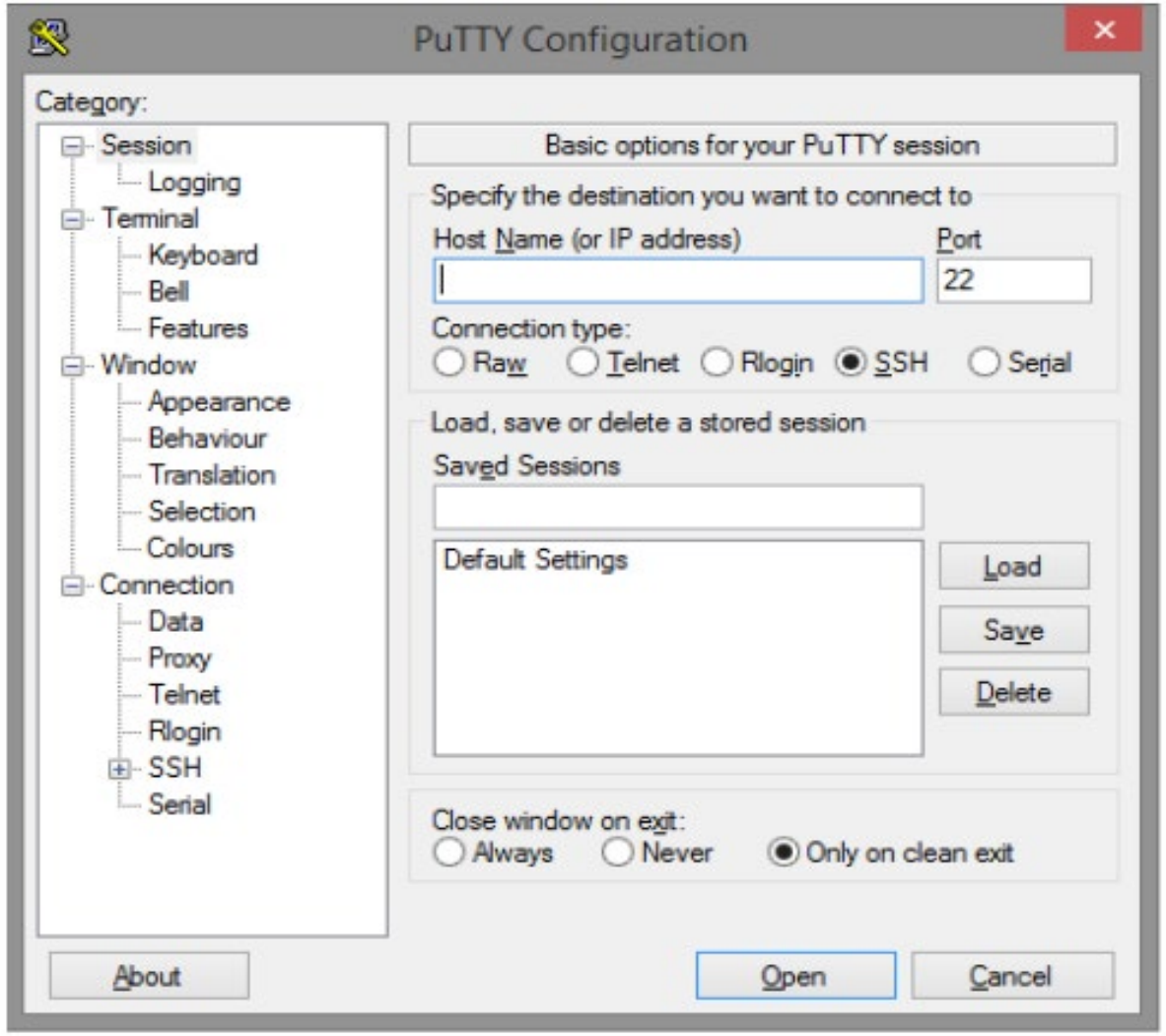
SSH Windows-on (kliens oldal)

- Windows SSH kliens ***putty***

A putty használata:

- ***Host Name or IP adresse***
- ***Port 22***

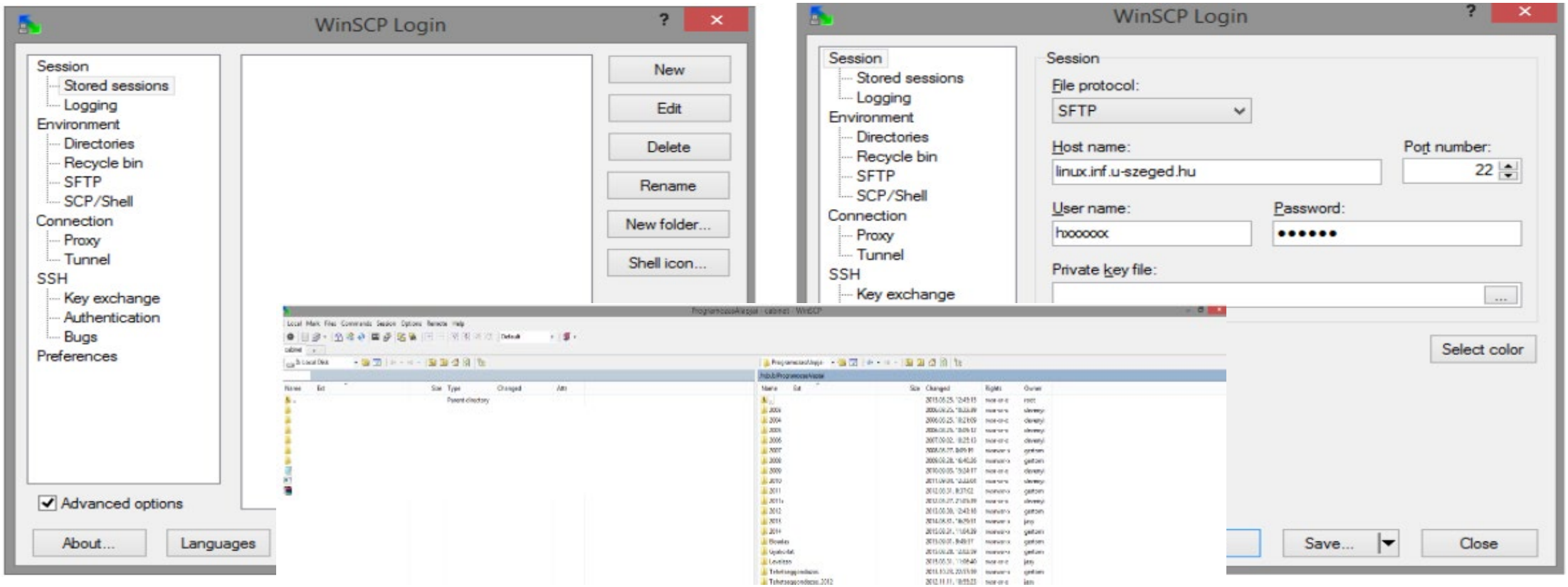




Fájl átvitel

- SFTP (secure file transfer protocol) Windows alatt WinSCP használatával:

Fájlok távoli átviteléhez valamilyen SFTP-t támogató kliens szükséges. Ilyenek például a WinSCP vagy FileZilla programok.



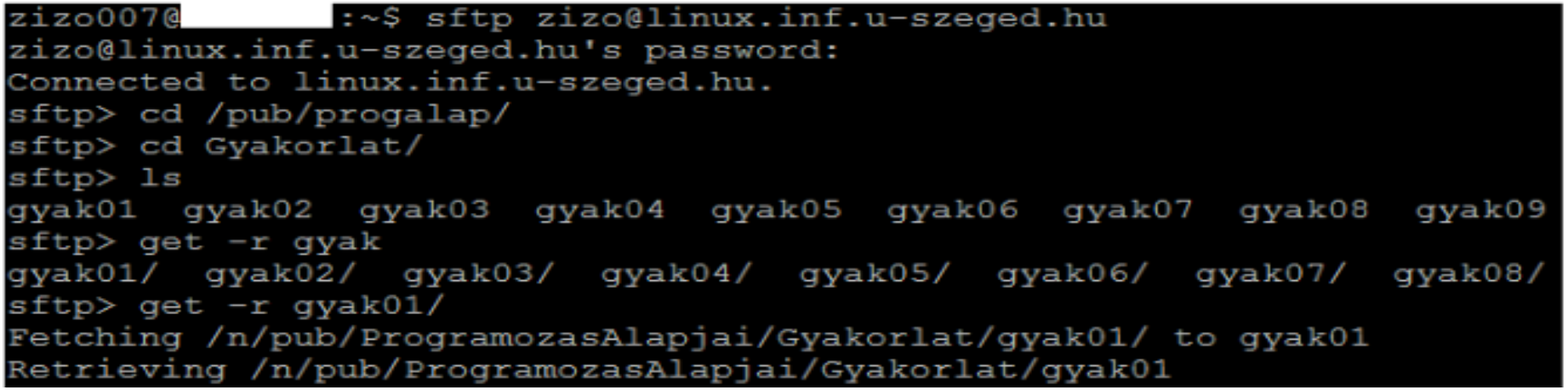
SFTP (secure file transfer protocol) Linux alatt terminálból

Nyiss egy terminált majd használd az sftp parancsot!

Ezután a fenti ’sftp>’ prompt-ot fogod visszakapni.

A legtöbb parancshoz tartozik egy ’l’ prefixes megfelelője is, mely a lokális gépre vonatkozik (ahonnan sftp-zel). Például:

- ls -> a távoli gépen hajt végre egy listázást az aktuális könyvtárra
- lls -> a lokális gépen hajt végre egy listázást.



Fájlokat úgy tudod a saját gépedre másolni, ha használod a ’get’ parancsot.