

Your Mission: Use F-Response Field Kit to connect to a remote Non-Windows machine



Using F-Response to connect to a remote Non-Windows (Linux or OSX) machine and access one or more targets

Step 1: Locate the appropriate executable for your subject machine

Open the Program Files folder on the machine you installed F-Response Field Kit on and locate the F-Response folder. Inside you will find the F-Response Subjects folder. This folder contains all the subject executables by type and platform.

The screenshot shows a file explorer window with the path: Program Files > F-Responsev7 > F-Response Subjects. The window displays a list of files and folders with columns for Name, Date modified, and Type. The files are organized by platform and architecture.

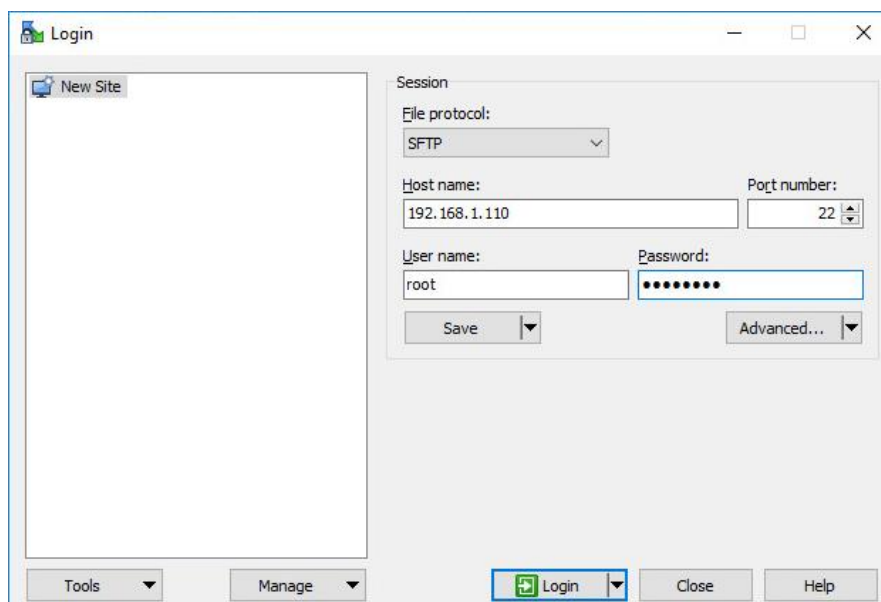
Name	Date modified	Type
sub-aix-powerpc-consultant	10/19/2016 3:20 PM	File
subject_srv	10/19/2016 3:57 PM	Application
subject_srv-x64	10/19/2016 3:57 PM	Application
sub-lin-i386-consultant	10/19/2016 3:19 PM	File
sub-lin-i386-fieldkit	10/19/2016 3:19 PM	File
sub-lin-x86_64-consultant	10/19/2016 3:18 PM	File
sub-lin-x86_64-fieldkit	10/19/2016 3:18 PM	File
sub-osx-x86_64-consultant	10/19/2016 3:21 PM	File
sub-osx-x86_64-fieldkit	10/19/2016 3:21 PM	File
sub-sun-i386-consultant	10/19/2016 3:19 PM	File
sub-sun-sparc-consultant	10/19/2016 3:20 PM	File
sub-win-i386-consultant	10/19/2016 3:56 PM	Application
sub-win-i386-fieldkit	10/19/2016 3:56 PM	Application
sub-win-x86_64-consultant	10/19/2016 3:56 PM	Application
sub-win-x86_64-fieldkit	10/19/2016 3:56 PM	Application

Subject Executables

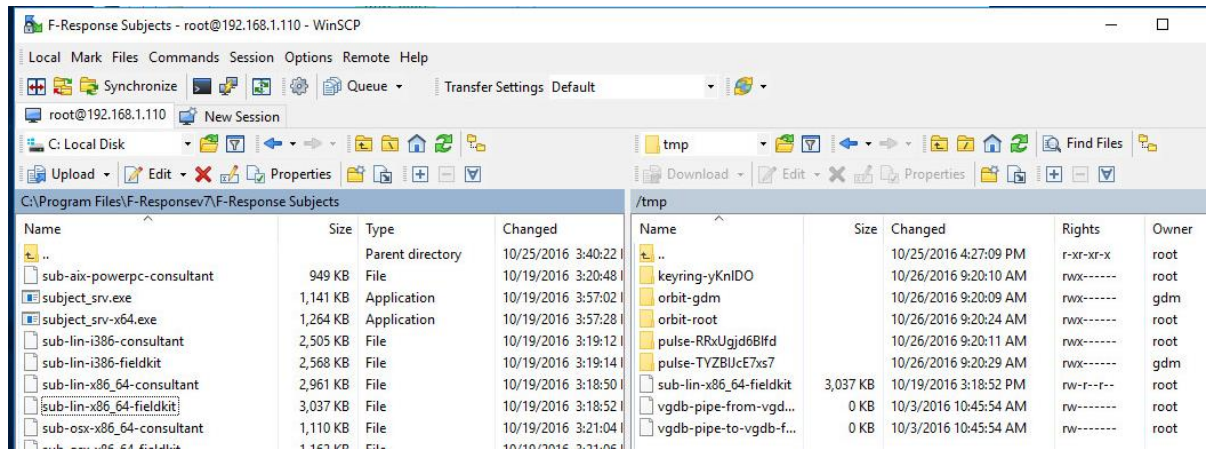
Step 2: Get the selected Non-Windows executable to your remote machine

You can do this however you would like by copying both files to a CD, USB thumb drive or network share as an example of some of the most common options.

However, working from the comfort of our chair, we are going to use a free tool called WinSCP to distribute the file to our Non-Windows Subject(s) over the network. If you don't have WinSCP installed, you can download and install it from www.winscp.net. Startup WinSCP and you will be greeted with a Login Window:



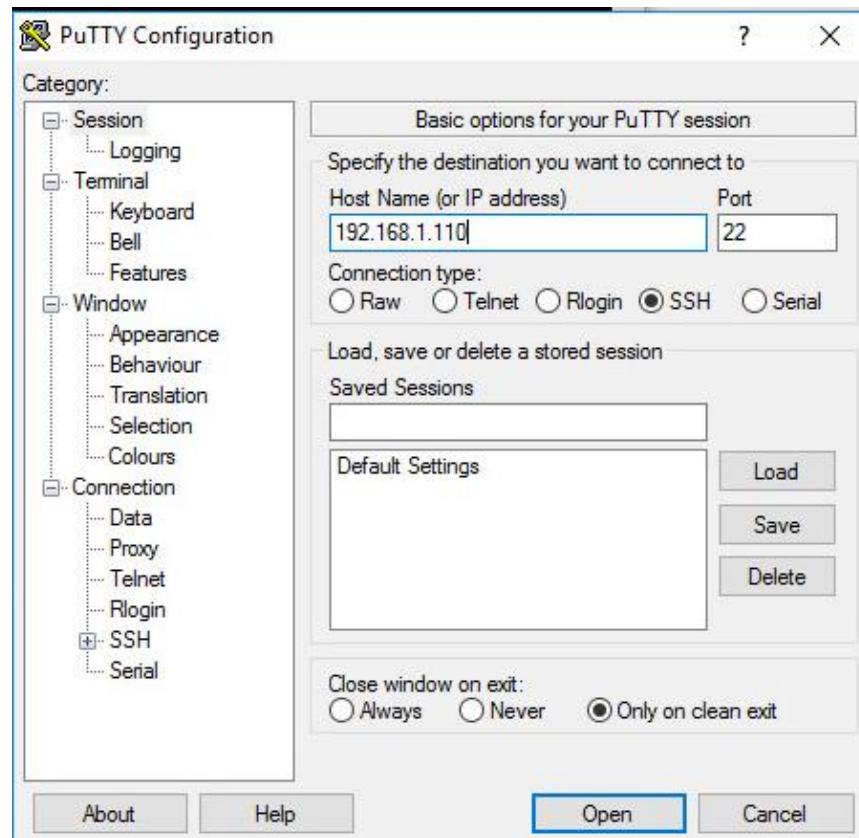
Here you can enter the IP or Host name for the Subject machine into the Host name field. Fill in the login and password for your target machine and click the Login button. After connecting you'll be greeted with a file copy dialog that resembles the Windows Explorer interface.



In the left pane you can browse to the location where you saved the F-Response file, in this case the Desktop. Then we'll copy the files to the /<root> /tmp directory on the Non-Windows target by browsing to the folder, then highlighting and dragging the files into the right pane.

Step 3: Insert your license dongle into the remote machine and start F-Response

Let's use another nice, free, and easy tool to start F-Response on the Non-Windows subject(s). If you don't already have it installed, download a copy of puTTY. Start puTTY and you are greeted with the following window:



Simply enter the Subject name or IP address into the Host Name field and click the Open button (leave everything else at the default setting). Putty will start the connection and then prompt you for a Username and Password. Generally, there are two types of accounts for our purposes: the all-powerful administrator "root" account, and a general user account that can assume root privileges for a time. To log into the subject with the root account, type 'root' for the login, and enter the password when prompted. You will see the prompt change to a # sign. Given the power of the root account, it is more likely you will be using a general user account that will assume root privileges. The two possibilities for accomplishing this with your user account are su and sudo but first you'll need to login with your user account by entering your login and password at the prompt.

Once you are logged in, you recall copying the F-Response file to the /tmp directory. You can change to this directory by typing the command "cd /tmp" and pressing enter. Because the file was copied locally, the executable file needs to be defined as an executable, which is done by the command: "chmod a+x <name of the file>". Now, to start F-Response:

If you logged in as root, you will type

```
./<name of the file> -u <FRESPONSE Username> -p <FRESPONSE Password> [ENTER]
```

Let's look at these two possibilities, Sudo, or "SuperUser Do" is used to execute a command as root.

The command to start F-Response using sudo is:

```
sudo ./<name of the file> -u <FRESPONSE Username> -p <FRESPONSE Password> [ENTER]
```

Su can be used to assume root privileges. Once we have assumed root, the command to start F-Response is the same as if we are logged in with the root account.

To start F-Response using su, type:

```
su
```

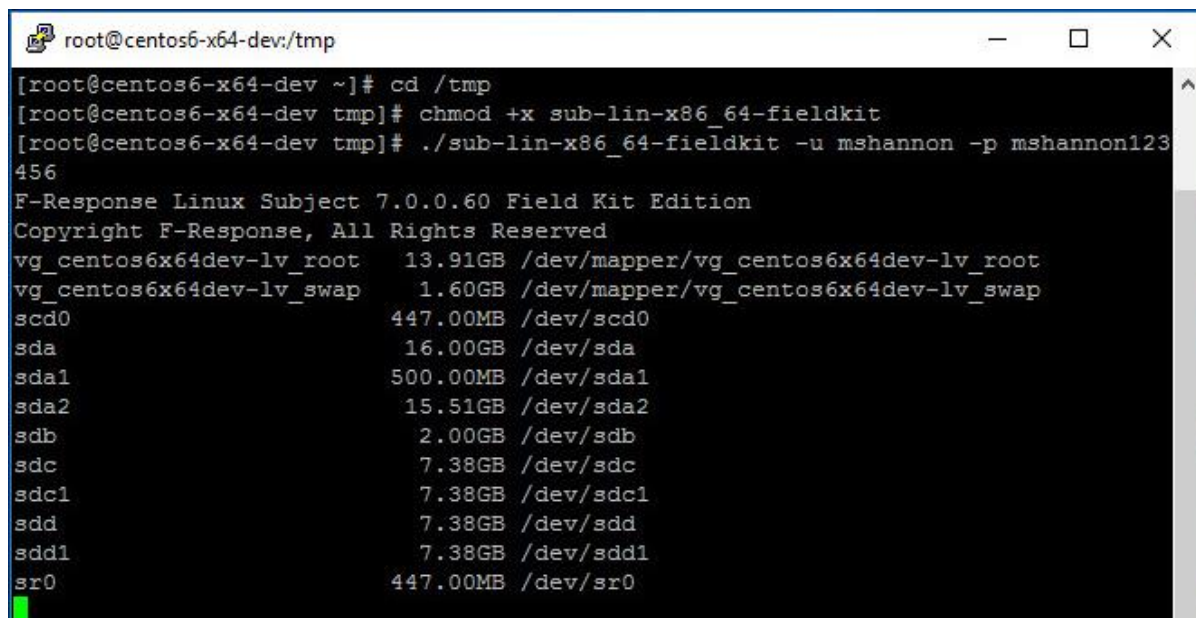
```
[ENTER]
```

```
Type
```

```
the root password
```

```
[ENTER]
```

```
./<name of the file> -u <FRESPONSE Username> -p <FRESPONSE Password>[ENTER]
```



```
root@centos6-x64-dev:/tmp
[root@centos6-x64-dev ~]# cd /tmp
[root@centos6-x64-dev tmp]# chmod +x sub-lin-x86_64-fieldkit
[root@centos6-x64-dev tmp]# ./sub-lin-x86_64-fieldkit -u mshannon -p mshannon123456
F-Response Linux Subject 7.0.0.60 Field Kit Edition
Copyright F-Response, All Rights Reserved
vg_centos6x64dev-lv_root    13.91GB /dev/mapper/vg_centos6x64dev-lv_root
vg_centos6x64dev-lv_swap   1.60GB /dev/mapper/vg_centos6x64dev-lv_swap
scd0                       447.00MB /dev/scd0
sda                        16.00GB /dev/sda
sda1                       500.00MB /dev/sda1
sda2                       15.51GB /dev/sda2
sdb                         2.00GB /dev/sdb
sdc                         7.38GB /dev/sdc
sdc1                       7.38GB /dev/sdc1
sdd                         7.38GB /dev/sdd
sdd1                       7.38GB /dev/sdd1
sr0                        447.00MB /dev/sr0
```

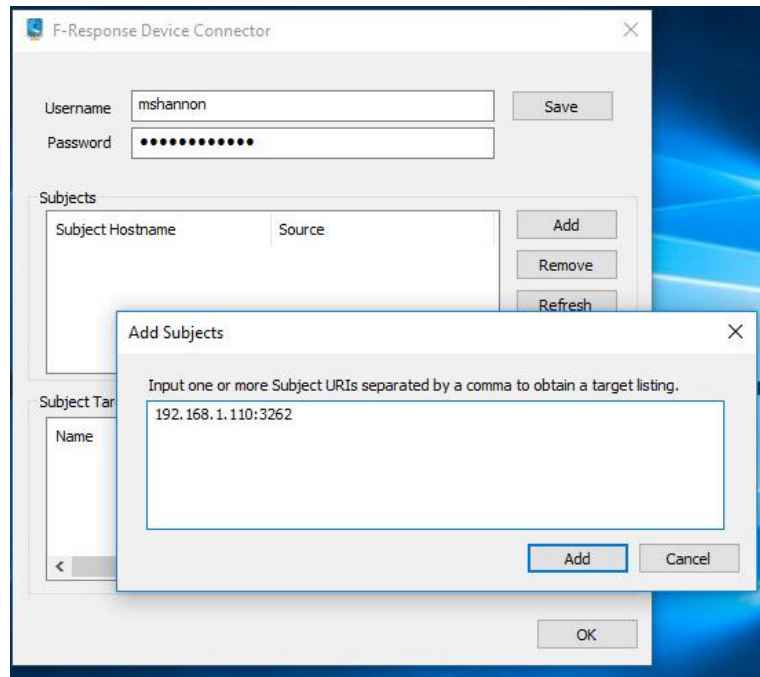
In this example, we logged in using the root account. Then we changed to the temp directory where

the F-Response files have been copied. We then modified F-Response as an executable. Lastly, we typed the command to start F-Response. Once your analyst machine has been successfully located, F-Response will list each available write-blocked device on the Non-Windows subject in the terminal window. These targets can then be seen on your analyst machine in the F-Response Device Connector Control Panel Applet.

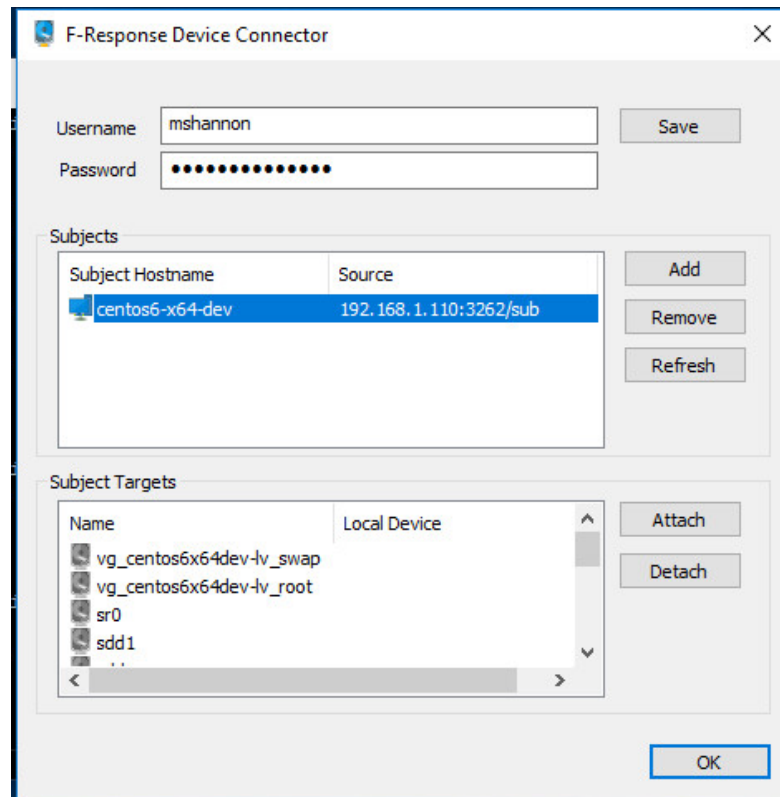
Step 4: List the available targets and attach one or more to your local machine

After successfully starting F-Response on a remote machine you must use the "F-Response Device Connector" in the Control Panel to list the available targets and attach to one or more targets.

First start by setting the Username and Password to the same value you set for the F-Response Field Kit Subject executable. Then use the Add button to add the Subject URI of your remote subject, this is in the format <IP or Host>:<Port>.



Adding a Subject URI



Listing Targets

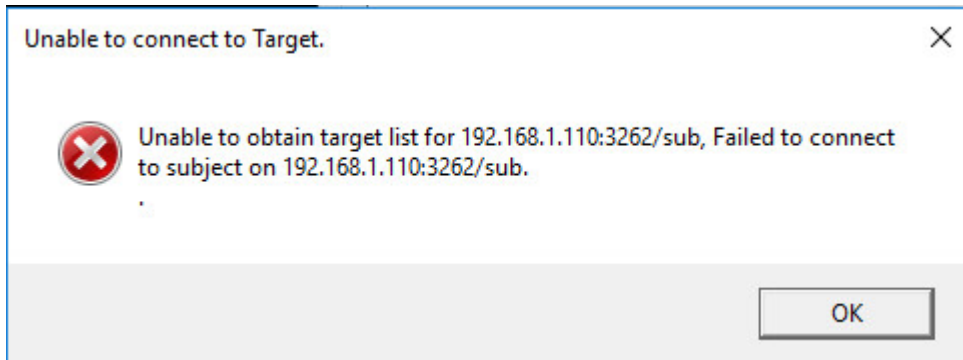
Select one or more targets in the Subject Targets listing and press "Attach" to attach those targets as a local device.

Troubleshooting

Trying to start the Field Kit on my Linux machine results in an error related to libusb, what do I do?

You need to install libUSB on your remote linux machine. The mechanism for doing this is distribution dependent.

Trying to add the Subject I receive the following response:



This typically indicates there is a firewall blocking access to F-Response on the remote machine, either disable the firewall temporarily or set an exception for F-Response.