# 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.

ıram Files 🔹 F-Responsev8 🔌 F-Respons	e Subjects 🗸 🗸 Č	) Search F-Res	ponse Subjects 🛛 🔎
Name	Date modified	Туре	Size
📋 sub-aix-powerpc-consultant	10/29/2018 8:25 AM	File	1,557 KB
subject_srv	10/29/2018 8:53 AM	Application	1,147 KB
subject_srv-x64	10/29/2018 8:53 AM	Application	1,273 KB
sub-lin-i386-consultant	10/29/2018 8:25 AM	File	1,308 KB
📄 sub-lin-i386-fieldkit	10/29/2018 8:25 AM	File	1,606 KB
sub-lin-x86_64-consultant	10/29/2018 8:25 AM	File	1,297 KB
sub-lin-x86_64-fieldkit	10/29/2018 8:25 AM	File	1,654 KB
sub-osx-x86_64-consultant	10/29/2018 8:25 AM	File	2,076 KB
sub-osx-x86_64-fieldkit	10/29/2018 8:25 AM	File	1,985 KB
📋 sub-sun-i386-consultant	10/29/2018 8:25 AM	File	1,425 KB
sub-sun-sparc-consultant	10/29/2018 8:25 AM	File	1,532 KB
🔏 sub-win-i386-consultant	10/29/2018 8:52 AM	Application	1,721 KB
🔏 sub-win-i386-fieldkit	10/29/2018 8:53 AM	Application	2,064 KB
🔏 sub-win-x86_64-consultant	10/29/2018 8:53 AM	Application	2,064 KB
✓ sub-win-x86_64-fieldkit	10/29/2018 8:52 AM	Application	1,721 KB

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:

SFTP V Host name: Port number: 192.168.1.110 22 User name: Password: root • Advanced	🚰 New Site	Session File protocol:	
Host name: Port number: 192.168.1.110 22 User name: Password: root ● Save ▼ Advanced		SFTP V	
192.168.1.110 22   User name: Password:   root •••••••   Save ✓   Advanced		Host name:	Po <u>r</u> t number:
User name: Password: root •••••• Save ▼ Advanced		192.168.1.110	22
root ••••••• Save 💌 Advanced		User name:	Password:
Save 🔽 Advanced		root	•••••
		Save 🗸	Advanced
		1	

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.

🌆 F-Response Subjects - root@192.16	8.1.110 - WinSCI	2				- 62	<del></del>	
Local Mark Files Commands Sessi	on Options Re	mote Help						
🖶 🚉 📚 Synchronize 🗾 🦑 🛛		ueue 👻 🛛 Transf	er Settings Default	• 🥵 •				
📮 root@192.168.1.110 💣 New Sess	ion							
🐛 C: Local Disk 🔹 🦉 🔽	<b>◆ •</b> • •	🖻 🖾 🏠 🎜	5	📘 tmp 🔹 🚰 🚺	7	» · 🗈 🗖 🏠 🎜	<b>G</b> Find Files	2
📑 📑 Upload 👻 📝 Edit 👻 🚮 🕻	Properties		1	I 🔐 Download 🖌 📝 Edit	- ×	🔓 Properties 📑 🔂	+ - V	
C:\Program Files\F-Responsev7\F-Resp	onse Subjects			/tmp				
Name	Size	Туре	Changed	Name	Size	Changed	Rights	Owner
<b>t.</b>		Parent directory	10/25/2016 3:40:22	±		10/25/2016 4:27:09 PM	r-xr-xr-x	root
sub-aix-powerpc-consultant	949 KB	File	10/19/2016 3:20:48	keyring-yKnIDO		10/26/2016 9:20:10 AM	rwx	root
subject_srv.exe	1,141 KB	Application	10/19/2016 3:57:02	orbit-gdm		10/26/2016 9:20:09 AM	rwx	gdm
subject_srv-x64.exe	1,264 KB	Application	10/19/2016 3:57:28	orbit-root		10/26/2016 9:20:24 AM	rwx	root
sub-lin-i386-consultant	2,505 KB	File	10/19/2016 3:19:12	pulse-RRxUgjd6Blfd		10/26/2016 9:20:11 AM	rwx	root
sub-lin-i386-fieldkit	2,568 KB	File	10/19/2016 3:19:14	pulse-TYZBIJcE7xs7		10/26/2016 9:20:29 AM	rwx	gdm
sub-lin-x86_64-consultant	2,961 KB	File	10/19/2016 3:18:50 1	sub-lin-x86_64-fieldkit	3,037 KB	10/19/2016 3:18:52 PM	rw-rr	root
sub-lin-x86_64-fieldkit	3,037 KB	File	10/19/2016 3:18:52	vgdb-pipe-from-vgd	0 KB	10/3/2016 10:45:54 AM	rw	root
sub-osx-x86_64-consultant	1,110 KB	File	10/19/2016 3:21:04	vgdb-pipe-to-vgdb-f	0 KB	10/3/2016 10:45:54 AM	rw	root
Cheve and A field hit	1 160 VD	Ella	10/10/2016 2:21:061					

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:

ogoij.		
Session	Basic options for your Pu	TTY session
	Specify the destination you want to	connect to
- Teminal Keyboard	Host Name (or IP address)	Port
Bell	192.168.1.110	22
Features	Connection type:	● SSH ○ Serial
Appearance Behaviour Translation Selection	Load, save or delete a stored sessi Saved Sessions	on
Colours	Default Settings	Load
Data		Save
Telnet Rlogin		Delete
i⊡- SSH I Serial	Close window on exit:	ily on clean exit

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 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 ~]# [root@centos6-x64-dev tmp	cd /tmp ]# chmod ·	+x sub-lin-x86 64-fieldkit			^
[root@centos6-x64-dev tmp 456	] <b># ./s</b> ub-:	lin-x86_64-fieldkit -u mshannon	-p ms	hannoi	n123
F-Response Linux Subject	7.0.0.60	Field Kit Edition			
Copyright F-Response, All	Rights R	eserved			
vg centos6x64dev-lv root	13.91GB	/dev/mapper/vg centos6x64dev-1	v root		
vg_centos6x64dev-lv_swap	1.60GB	/dev/mapper/vg_centos6x64dev-1	v 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 3: 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>.

After you have successfully added a subject, use the Attach button to select and attach a disk target as a local device.

F-Response D	evice Connect	or		
Username	mshannon			Save
Password	•••••	••••		
Subjects				
Subject He	ostname	Source		Add
Add Subjects				Demons
Input one or 192.168.0.3	more Subject UF 10:3262/sub	Is separated by a comm Vis separated by a communication	na:	
			Add	Cancel
<			>	
Messages				
				~
				ОК

#### Adding a Subject URI

	mshannon			Save
Password	•••••	••••		
ubjects				
Subject Ho	ostname	Source		Add
🛒 scylla		192.168.0.30	:3262/sub	Remove
	20			Refrest
ttach Driv	e			Attach
Name	2	Туре	Size	Detach
pmem-uns	safe	memory	8GB	
pmem		memory	8GB	
Vol-E		volume	1GB	
VOI-C		volume	11B	
disk-0		drive	1TB	-

Listing Targets

#### Troubleshooting

#### 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.

### 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.