

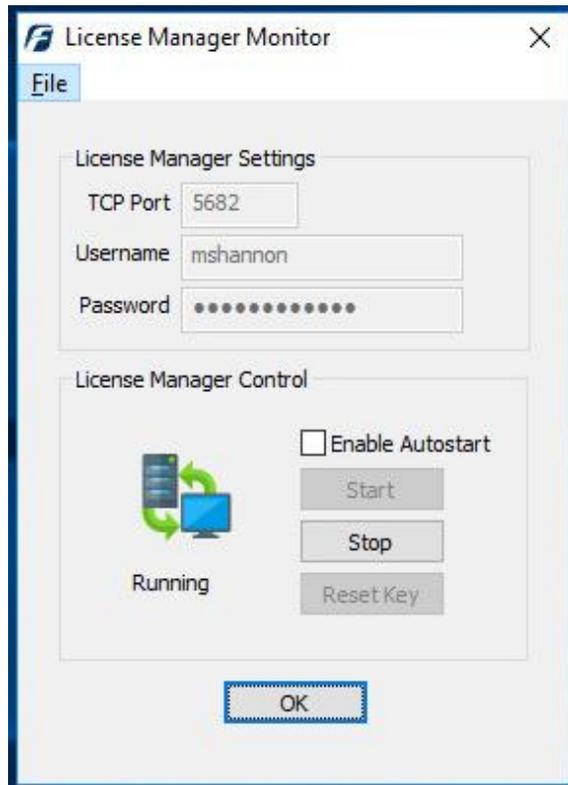
Your Mission: Use F-Response to connect to a remote Non-Windows machine



*Using F-Response to connect to a remote Non-Windows (Linux, OSX, AIX, etc) machine and access one or more targets. **Note SIP must be disabled for OSX, more details can be found here: <https://f-response.com/blog/f-response-apple-sip-ohm> ***

Step 1: Open and start the F-Response License Manager Monitor

If you have not already done so, open the F-Response License Manager Monitor and create a username and password that will be used specifically for F-Response. These credentials are purely to control access to F-Response on the remote subject, they are NOT a domain account or system account. Once you have set the username and password be sure to press "Start" to start the License

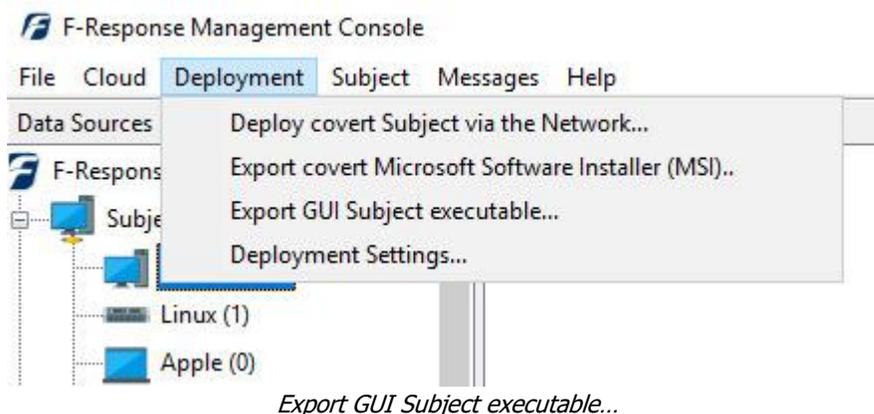


Manager Service.

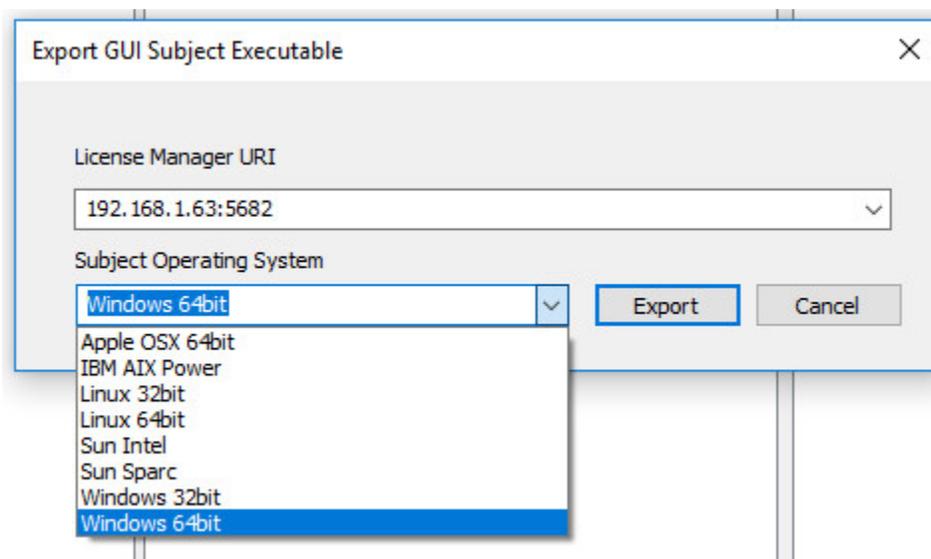
F-Response License Manager Monitor

Step 2: Export the appropriate executable for your remote subject

Open the F-Response Management Console and go to Deployment->Export GUI Subject executable...



Export GUI Subject executable...



Export GUI Subject Executable

Many of the options will be pre-populated for you, however you are welcome to adjust them to meet your needs.

License Manager URI: This is the IP or Hostname plus Port that F-Response will attempt to use to locate your license manager (see step 1). Most of the time it will be easy to determine what to select here from the dropdown list, however keep in mind the address you select must be accessible from the remote subject machine.

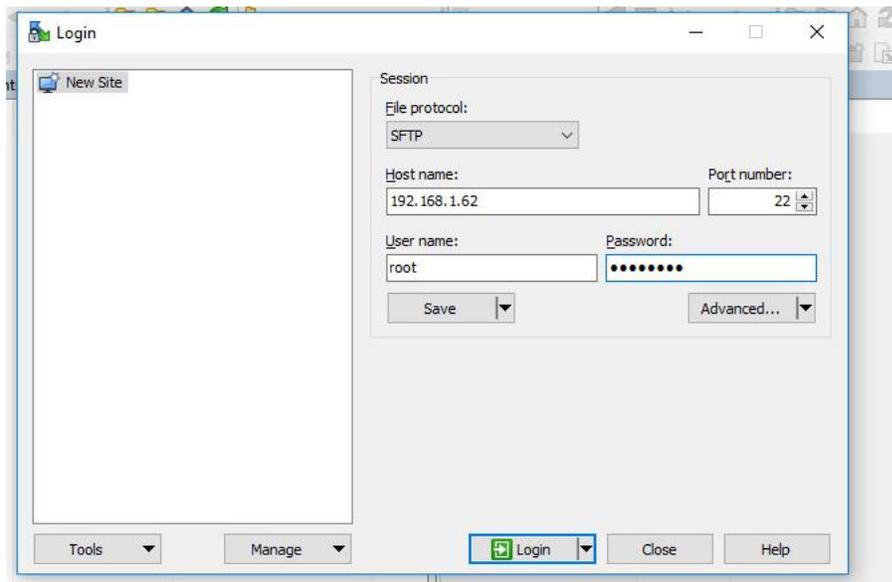
Subject Operating System: Select the appropriate operating system and build, in this instance our remote subject is 64 bit Linux, therefore we will select the Linux 64bit operating system.

Use the Export button to open a save dialog to save off the exported executable.

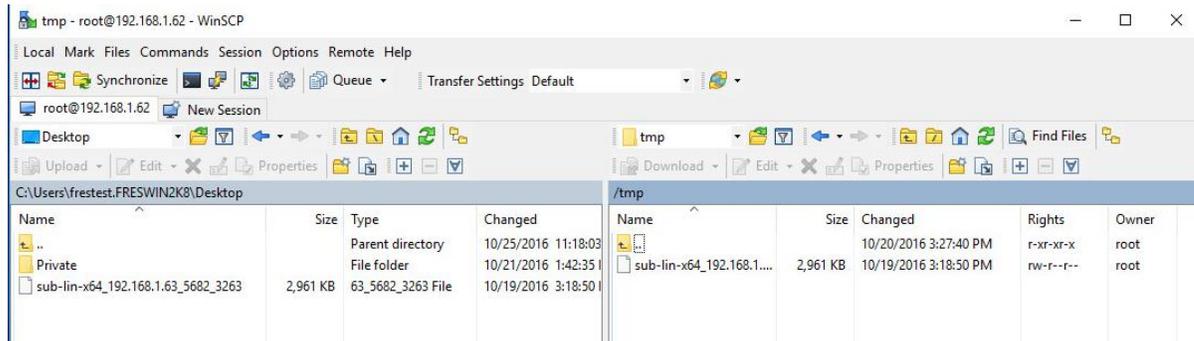
Step 3: Get the exported Non-Windows executable to your remote machine

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 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 Linux target(s) over the network. If you don't have WinSCP installed, you can download and install it from www.winscp.net. Start up WinSCP and you will be greeted with a Login Window:



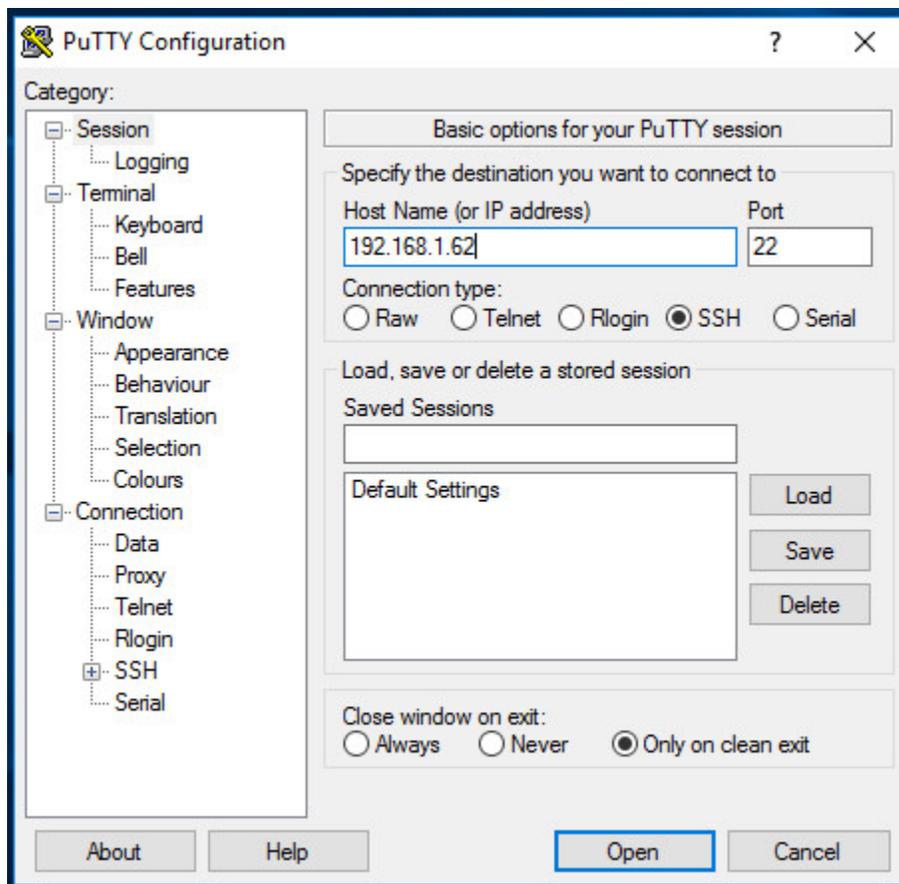
Here you can enter the IP or Host name for the Linux target machine into the Host name field. Fill in the login and password for your target machine and click the Login button. After connecting you'll be greeted with a file copy dialog that resembles the Windows Explorer interface.



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 4: Start F-Response on the remote machine

Let's use another nice free 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 Linux target 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, 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>[ENTER]

Let's take a 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>[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>[ENTER]

```

CentOS release 6.9 (Final)
Kernel 2.6.32-696.28.1.el6.x86_64 on an x86_64

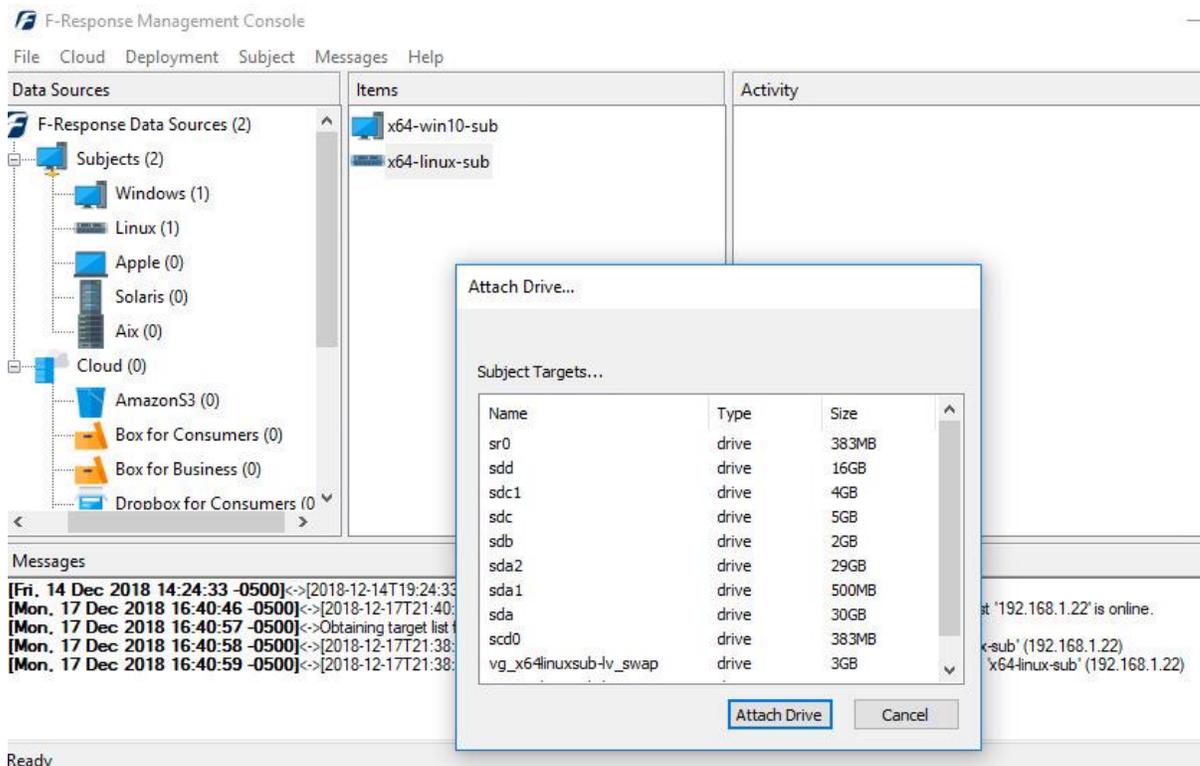
x64-linux-sub login: root
Password:
Last login: Mon Jan  7 12:47:15 from desktop-01osuuq.fresponse.local
[root@x64-linux-sub ~]# cd /tmp
[root@x64-linux-sub tmp]# chmod +x sub-lin-x64_192.168.1.63_5682_3262
[root@x64-linux-sub tmp]# ./sub-lin-x64_192.168.1.63_5682_3262
F-Response Linux Subject Consultant Edition 8.0.0.52
Copyright F-Response, All Rights Reserved
vg_x64linuxsub-lv_root    26.51GB /dev/mapper/vg_x64linuxsub-lv_root
vg_x64linuxsub-lv_swap   3.00GB /dev/mapper/vg_x64linuxsub-lv_swap
scd0                      383.00MB /dev/scd0
sda                       30.00GB /dev/sda
sda1                     500.00MB /dev/sda1
sda2                     29.51GB /dev/sda2
sdb                       2.00GB /dev/sdb
sdc                       5.00GB /dev/sdc
sdc1                     5.00GB /dev/sdc1
sdd                      16.00GB /dev/sdd
sr0                      383.00MB /dev/sr0

```

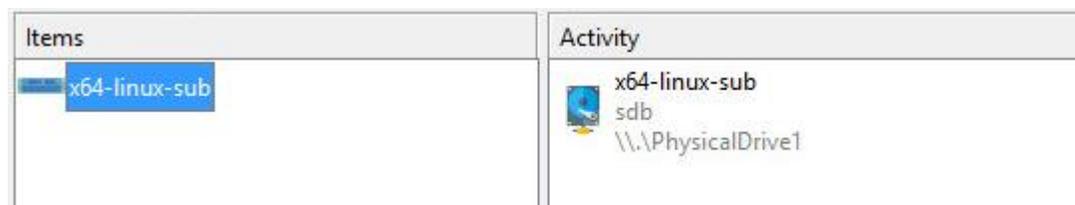
In this example, we logged in using the root account. Then we changed to the temp directory where the F-Response files have been copied. We then modified F-Response as an executable. Finally, we typed the command to start F-Response. F-Response will then run and use the bundled information contained in the executable file name to locate the licensing server (your analyst machine). 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 Management Console. Repeat Steps 2 and 3 for each Non-Windows target machine you would like to view in the Management Console on your analyst machine.

Step 5a: List the available targets and attach one or more to your local machine

After successfully deploying F-Response to one or more remote machines you should be able to see those machines by selecting Subjects or a specific platform in the Data Sources panel. The subject entries will appear in the Items panel. Double-Click on any subject to open a dialog for attaching a subject disk, or use the Subject menu for attaching a disk or starting a direct image of one or more subject targets.



Subject and Targets



Active Targets

Step 5b: List the available targets and image one or more to your local machine directly(optional)

Please remember F-Response is first and foremost a vendor-neutral connectivity tool. You can use any forensic/eDiscovery/IR tool you'd like against the write-protected F-Response connected disk. That being said, the F-Response Console does have a built-in full-disk imaging option that will maximize the F-Response connection to its fullest capabilities (for individual file collection, you'd need to leverage a different imaging tool from your kit). For full details on imaging from the F-Response Console, please refer to the manual on our website.

After successfully deploying F-Response to one or more remote machines you should be able to see those machines by selecting Subjects or a specific platform in the Data Sources panel. The subject entries will appear in the Items panel. Right click on any subject and select Image Subject Target menu option to commence a direct image of one or more subject targets.

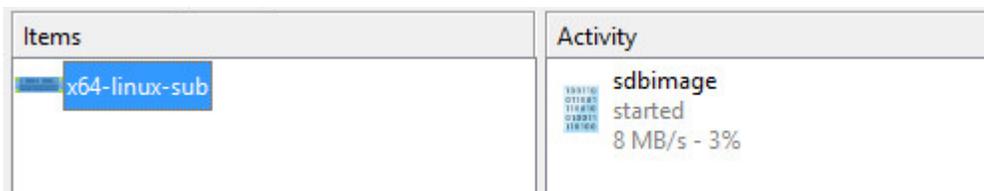
The screenshot shows the 'Create Image...' dialog box with the following fields and values:

Image Source	Name	Type	Size
	scd0	drive	383MB
	vg_x64linuxsub-lv_swap	drive	3GB
	vg_x64linuxsub-lv_root	drive	26GB

Image Name: sdbimage
Image Path: J:\ ...
Hash: md5 Total Available Space = 12189MB
Examiner Name: Joe
Case Number: fres2
Evidence Number: 2
Unique Description: SDB
Notes: Direct Image of remote disk

Buttons: Start Image, Cancel

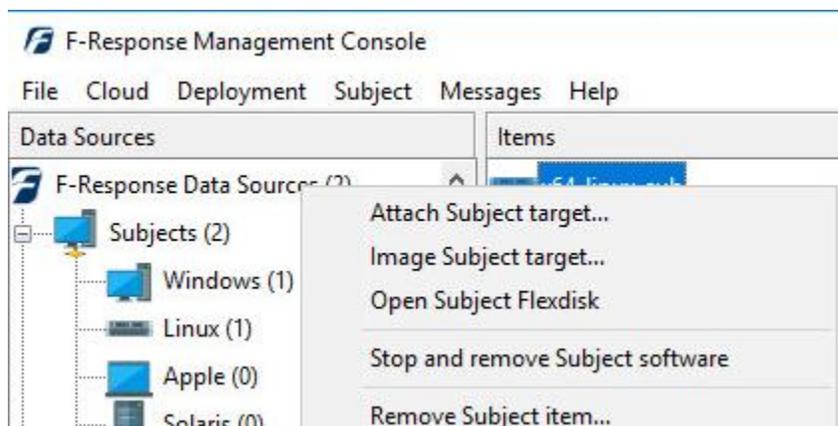
Start Imaging Process...



Active Images

Step 6: Removing F-Response from the remote machine

When you are finished using F-Response on the remote machine it can be readily removed using the Subject menu. First disconnect any active disks or images by right clicking on them in the Activity panel and selecting Cancel/Detach. Once all targets are detached, simply select the subject machine in the Items panel and right-click to select the "Stop and Remove Subject Software" to stop the F-Response software on the remote machine. If you wish to remove the software completely you can use WinSCP or delete the executable from the command line.



Stopping and removing F-Response from the remote machine.