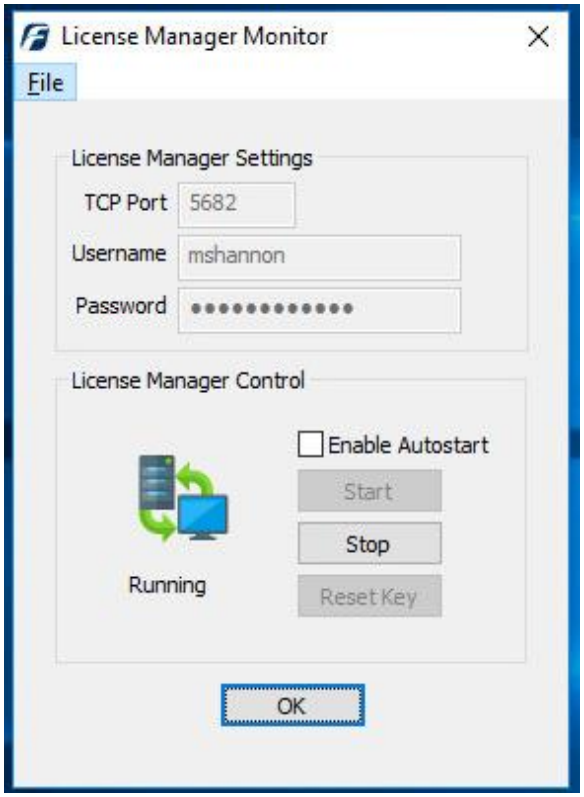
Mission Guide: Non-Windows

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

Step 1: Open and start the F-Response License Manager Monitor (If you have not already done so)

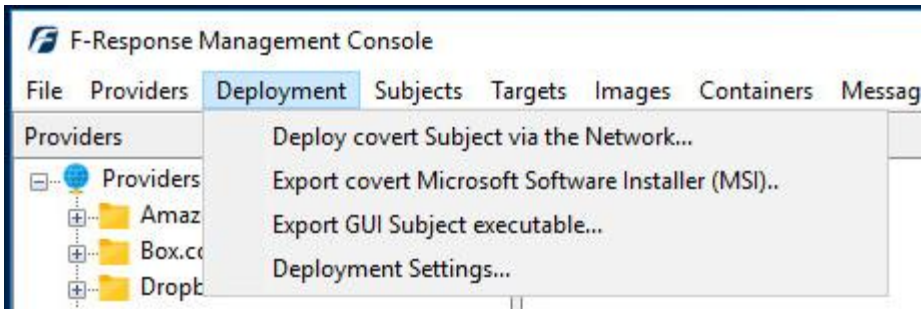
Open the F-Response License Manager Monitor and make sure you have input an F-Response specific username and password. These credentials are purely to control access to F-Response on the remote subject, they are NOT a domain account or system account. Once you have set the username and password be sure to press "Start" to start the License Manager Service.



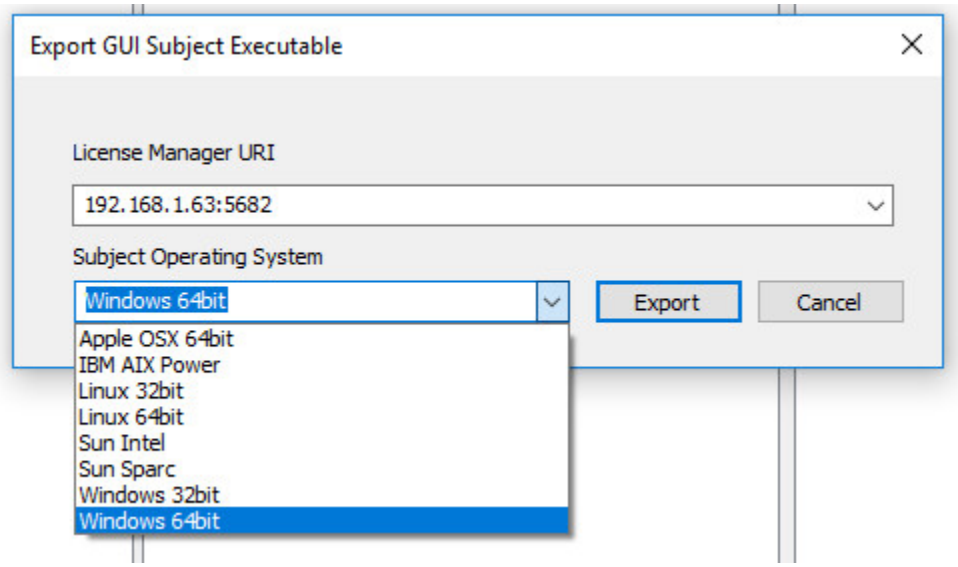
F-Response License Manager Monitor

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, however keep in mind the address you select must be accessible to the remote machine.

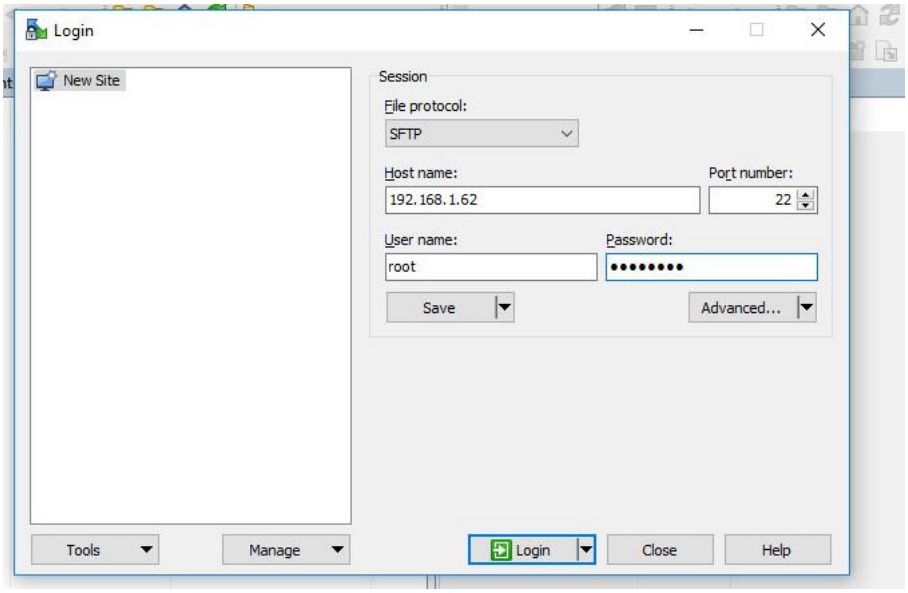
Subject Operating System: Select the appropriate operating system and build, in this instance our remote subject is 64 bit Linux, therefore we will select the Linux 64bit operating system.

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

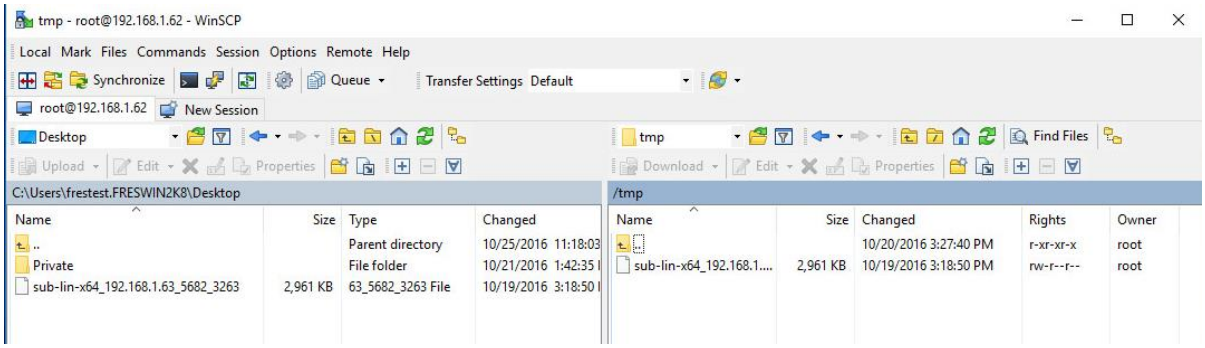
Step 3: Get the exported Non-Windows executable to your remote machine

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:



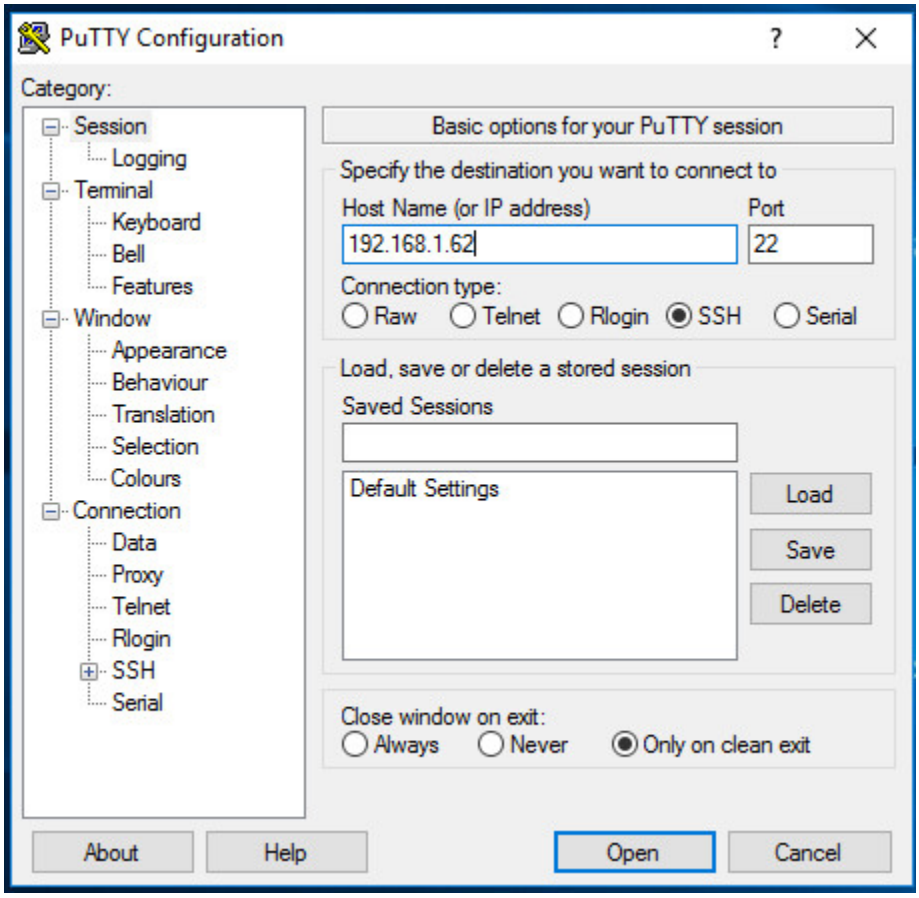
Here you can enter the IP or Host name for the Linux target machine into the Host name field. Fill in the login and password for your target machine and click the Login button. After connecting you'll be greeted with a file copy dialog that resembles the Windows Explorer interface.



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, 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:

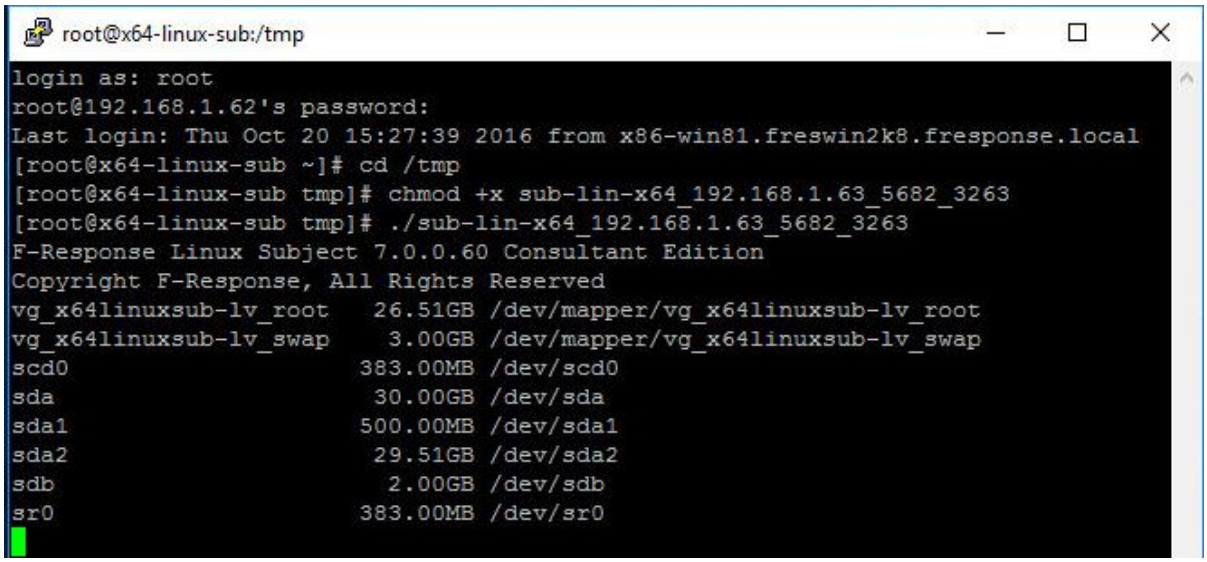
If you logged in as root, you will type
./<name of the file>[ENTER]

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]

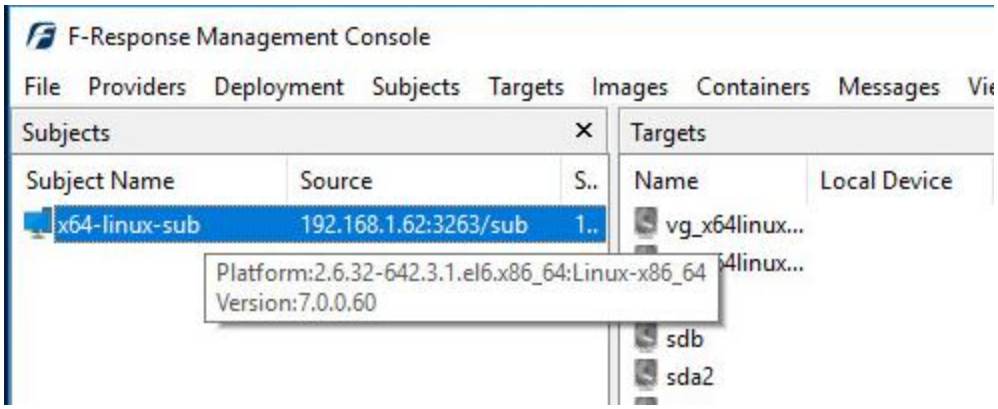


In this example, we logged in using the root account. Then we changed to the temp directory where the F-Response files have been copied. We then modified F-Response as an executable. Finally, we typed the command to start F-Response. F-Response will then run and use the bundled information contained in the fresponse.ini file 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

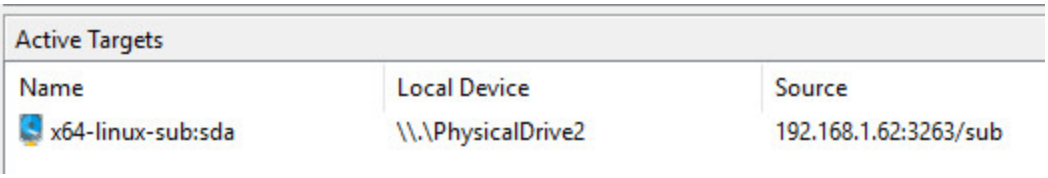
Step 5: List the available targets and attach one or more to your local machine

After successfully deploying F-Response to one or more remote machines you should see those machines in the Subjects panel (use the View->Subjects menu to show the Subjects panel if it is hidden). Hovering over any subject will give you the version of F-Response deployed and the operating system of the subject. Double-Click on any subject or use the Targets->Scan for Targets menu item to get a listing of targets in the Targets panel.

Mounting one or more targets is a simple matter of either double-clicking on the target or selecting the target and using the Targets->Attach Target menu item. Once attached additional target details will appear in the Active Targets panel.



Subject and Targets

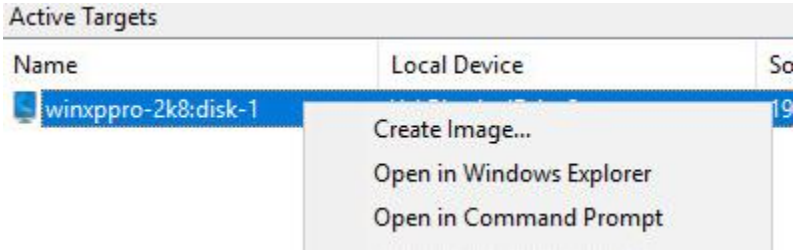


Active Targets

The remaining steps in this mission guide go over making an image of the newly attached device using the F-Response Imaging capability. This is completely optional, at this point you have a fully read-only locally attached disk that you can interact with, analyze, etc. using any of the forensic, incident response, or e-discovery tools you have at your disposal.

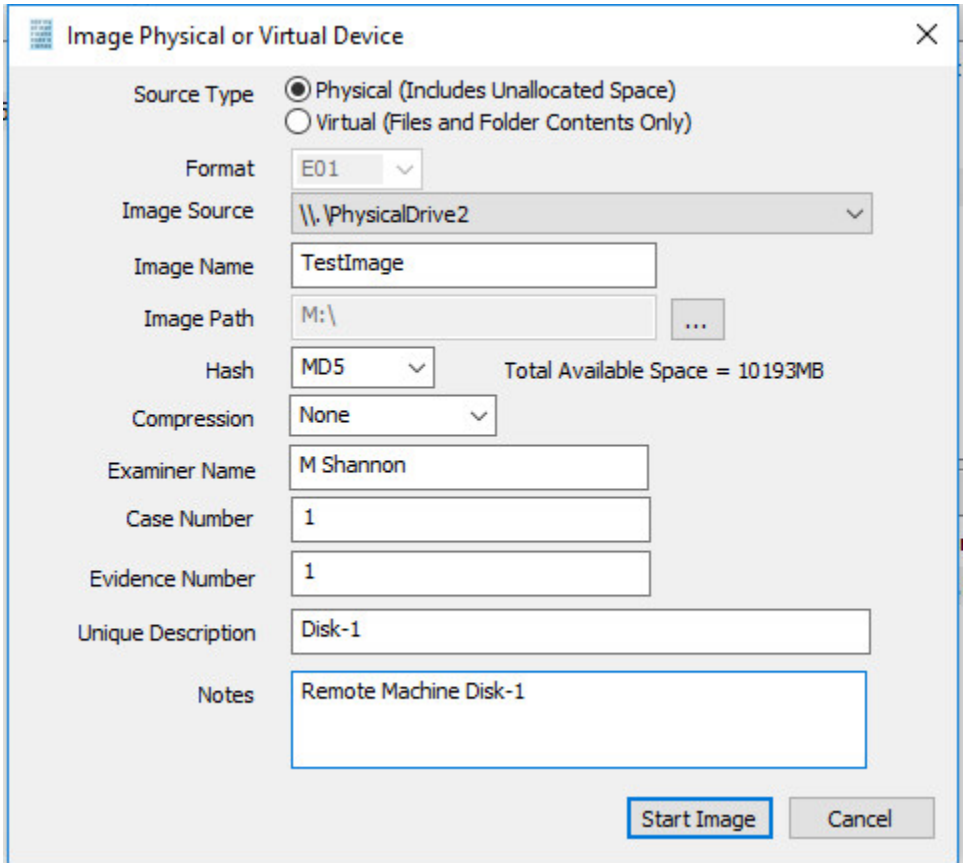
Step 6: Create Image of attached device

Select the newly attached target and right click on it in the Local Device column. Use the "Create Image…" option to open the "Image" dialog to begin imaging the device.



Start Imaging Process…

Step 7: Complete Imaging Options…



We'll work through this window from the top down. First, the **Source Type** is set to **Physical** (by default) to be able to create an image of the connected Physical device data.

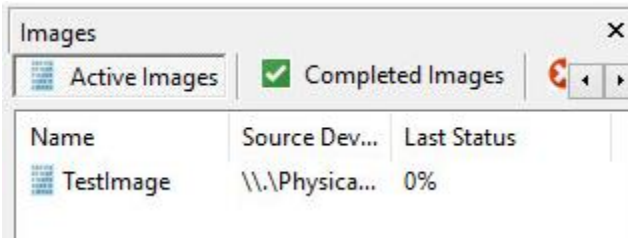
For **Image Path** we need to choose our destination drive—this must be a physical drive attached to our examiner machine (we cannot image to a network share).

Next we can choose a **Hash** format and the **Compression** level if you wish to compress the resulting image file. The remaining fields are specific to your case and can be filled out accordingly. These fields will be included in the resulting log file for the image.

Once you have all your information entered simply click the **Start Image** button to begin the process.

Step 8: Review the Image

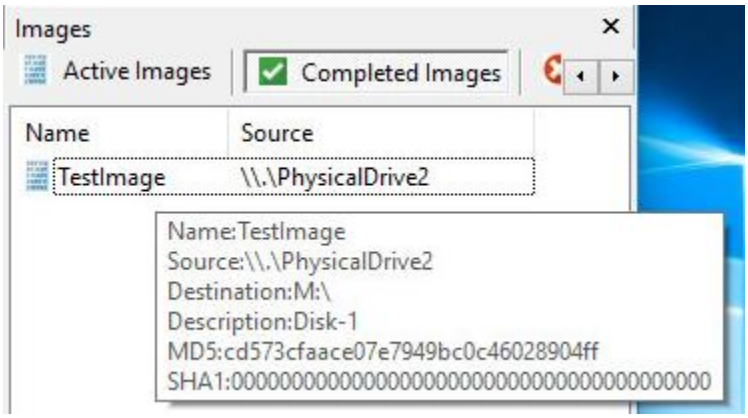
Once started the dialog will close and you'll be able to monitor the image using the Active Images panel (Use View->Images to display the Images panel if it is hidden). When the Image completes you will see it move to Completed Images.



Imaging started and running…

Step 9: Review the Completed Image

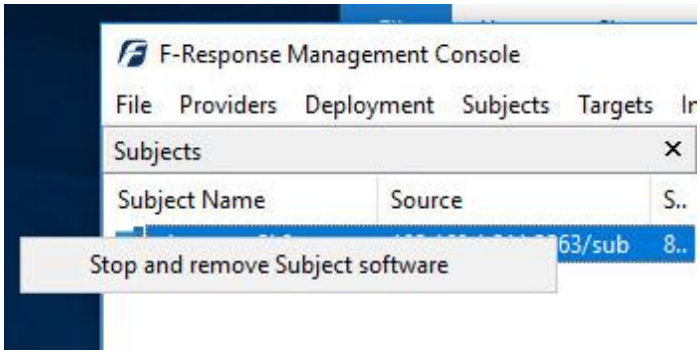
Right click on the completed image to access the Image Path, Log, and File List. These logs and listings contain details about the image, the image itself, and a file listing of files collected.



Reviewing the completed image.

Step 10: 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 targets by either double-clicking on them, or using the Target->Detach Target menu item. Once all targets are detached, simply select the subject machine in the Subjects panel and right-click to select the "Stop and Remove Subject Software" to stop and remove all F-Response software from the remote machine.



Stopping and removing F-Response from the remote machine.