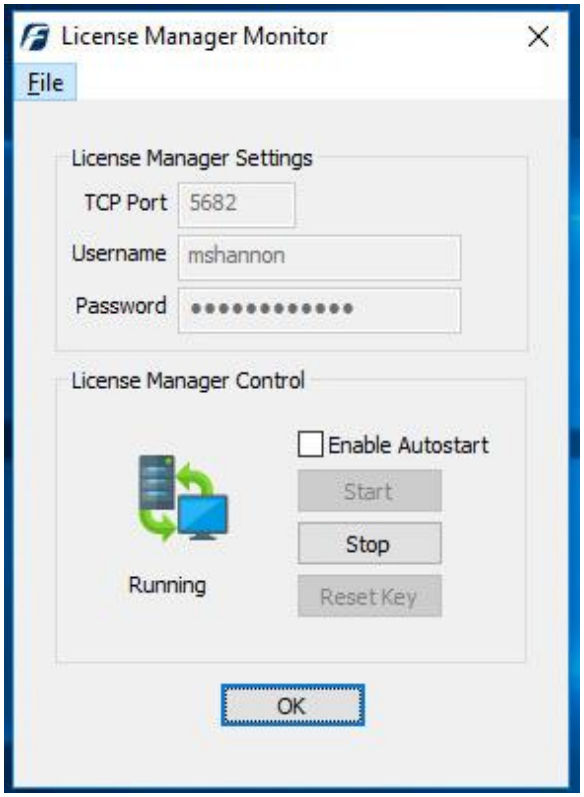
Mission Guide: GUI Windows

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

Using F-Response to connect to a remote Windows 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)

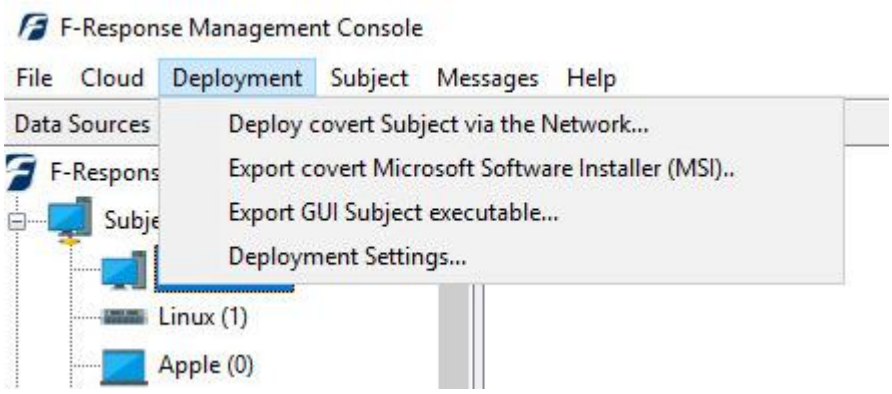
Open the F-Response License Manager Monitor and make sure you have input an F-Response specific username and password. These credentials are purely to control access to F-Response on the remote subject, they are NOT a domain account or system account. Once you have set the username and password be sure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



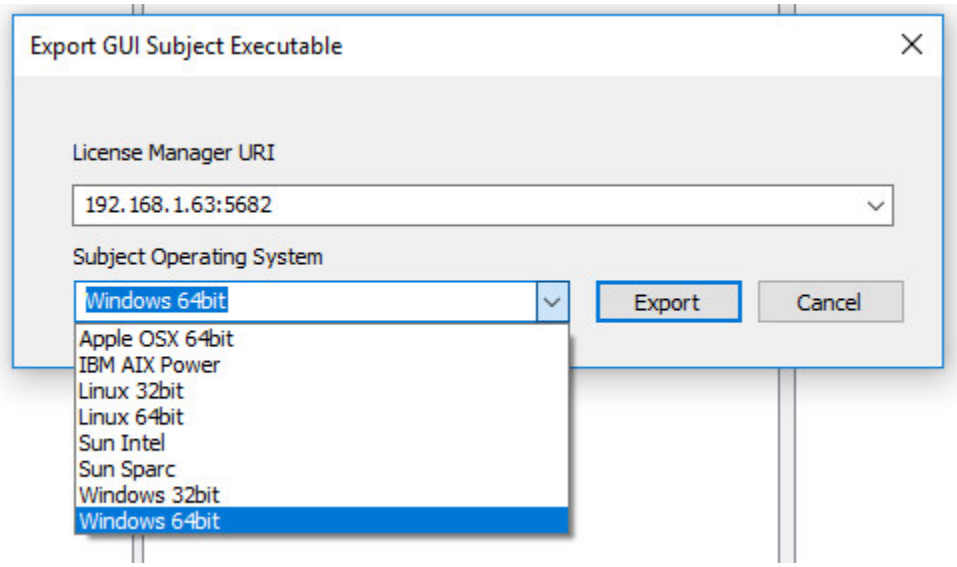
F-Response License Manager Monitor

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 the Port number that F-Response will attempt to use to locate your license manager (see step 1). Most of the time it will be easy to

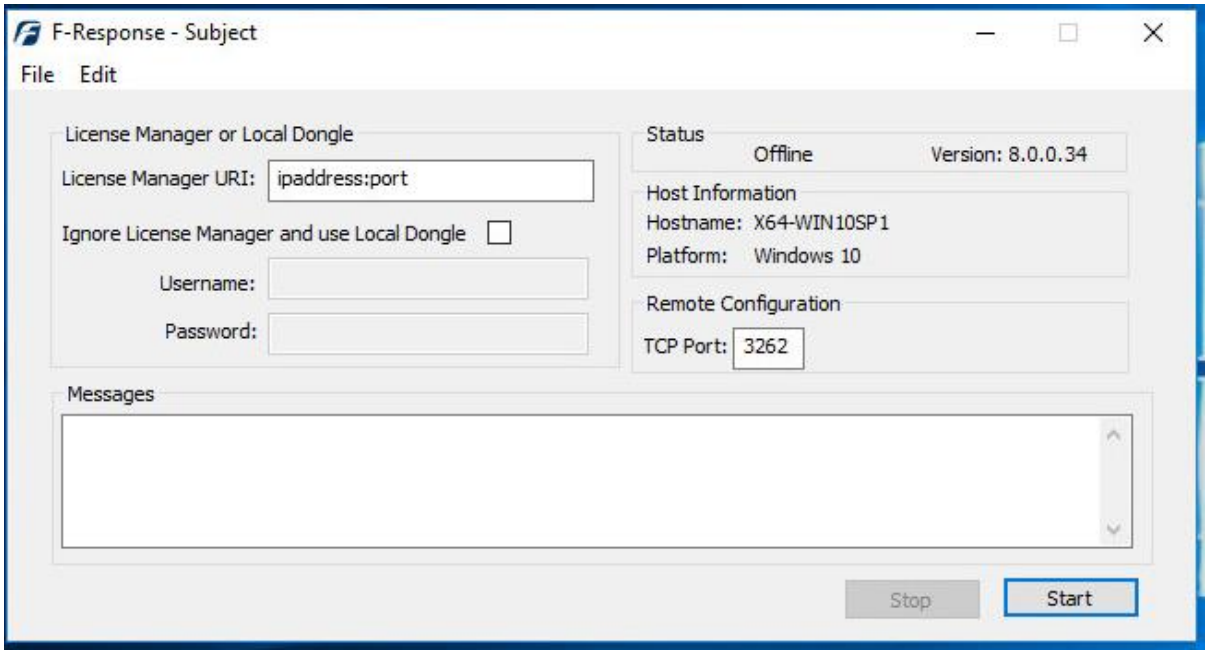
determine what to select from the dropdown menu here, however keep in mind the address you select must be accessible from the remote subject machine.

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

Use the Export button to open a save dialog to save off the exported executable, then use any of the numerous mechanisms available to get the exported executable to the remote machine (network share, usb, cdrom, etc.).

Step 3: Start F-Response on the remote machine

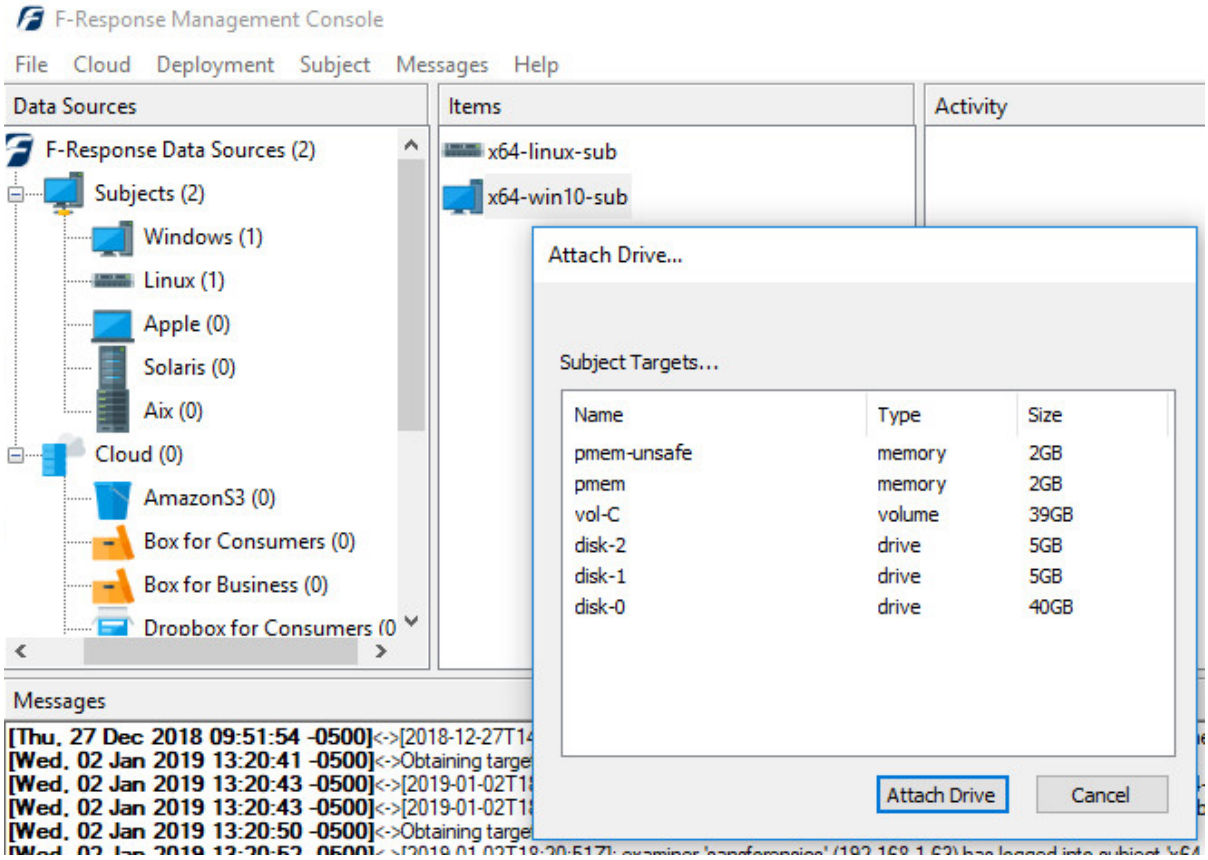
After exporting F-Response for Windows (64bit) and copying it to the remote machine we must execute it as an administrator. Simply click the Start button and the Status will change to Online.



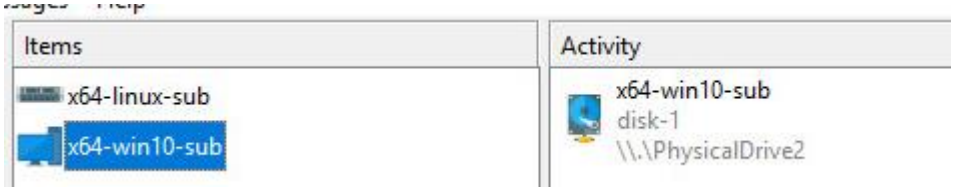
F-Response will then run and use the information contained in the filename to locate the licensing server (your analyst machine). Presented targets can then be seen on your analyst machine in the F-Response Management Console. Repeat Steps 2 and 3 for each Windows target machine you would like to view in the Management Console on your analyst machine.

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

After successfully starting F-Response on one or more remote machines you should see those machines in the Items panel. Double-Click on any subject or use the Subjects->Image Subject Target… or Attach Subject Target… menu item to either image a subject's device directly, or attach it to your machine.



Attach Drive or Image Directly

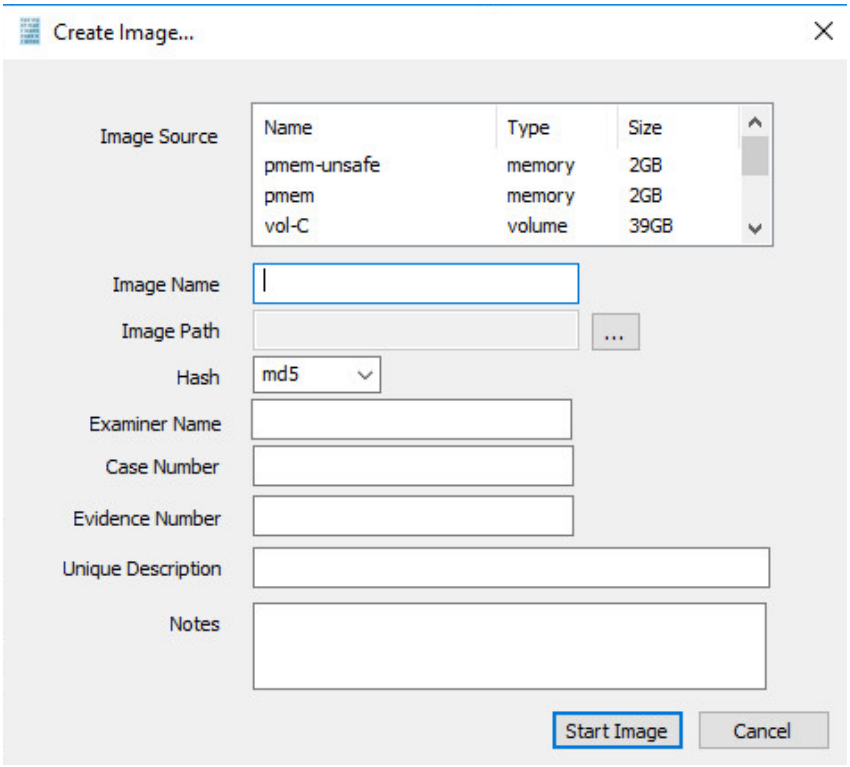


Active Targets

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 5: Create Image of target (optional)

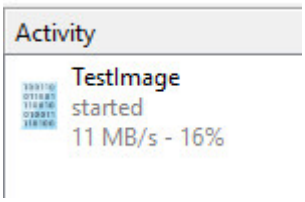
After successfully deploying F-Response to one or more remote machines you should be able to see those machines by selecting Subjects or a specific platform in the Data Sources panel. The subject entries will appear in the Items panel. Right click on any subject item and select the Image Subject Target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



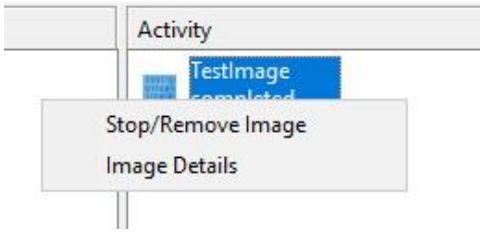
We'll work through this window from the top down. First, select your **Image Source** and then create a name for your image in the **Image Name** field. Click the ellipsis button and choose the destination drive—this must be a physical drive attached to our examiner machine (we cannot image to a network share). Next you'll choose a Hash type (MD5 or SHA1). 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.

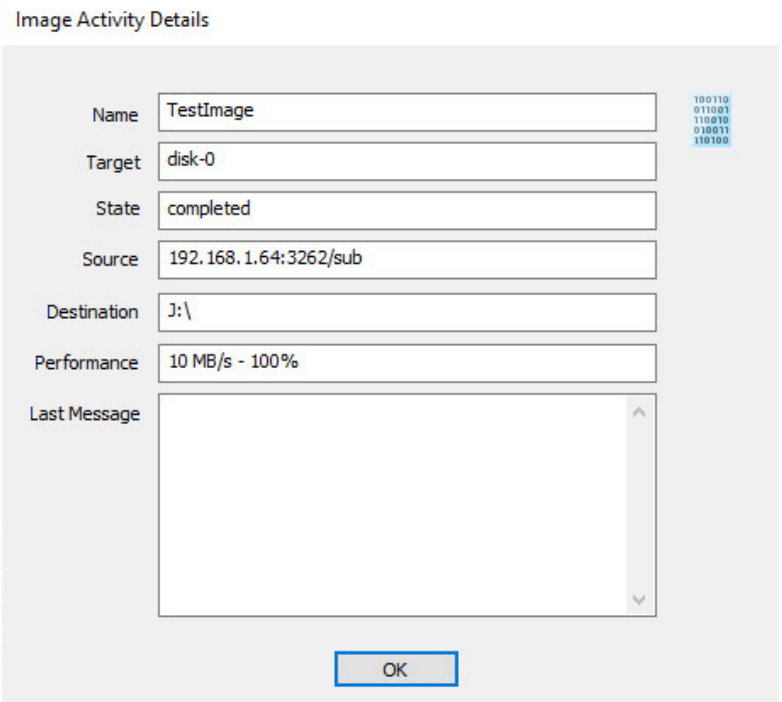
Step 7: Review the Image

Once started the dialog will close and you'll be able to monitor the image using the Activity panel.

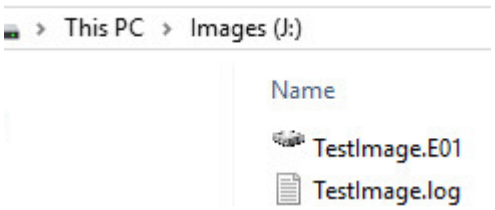


Right click on the image and choose Image details at any time to view the current state of the image. When the Image completes the status will show as completed.

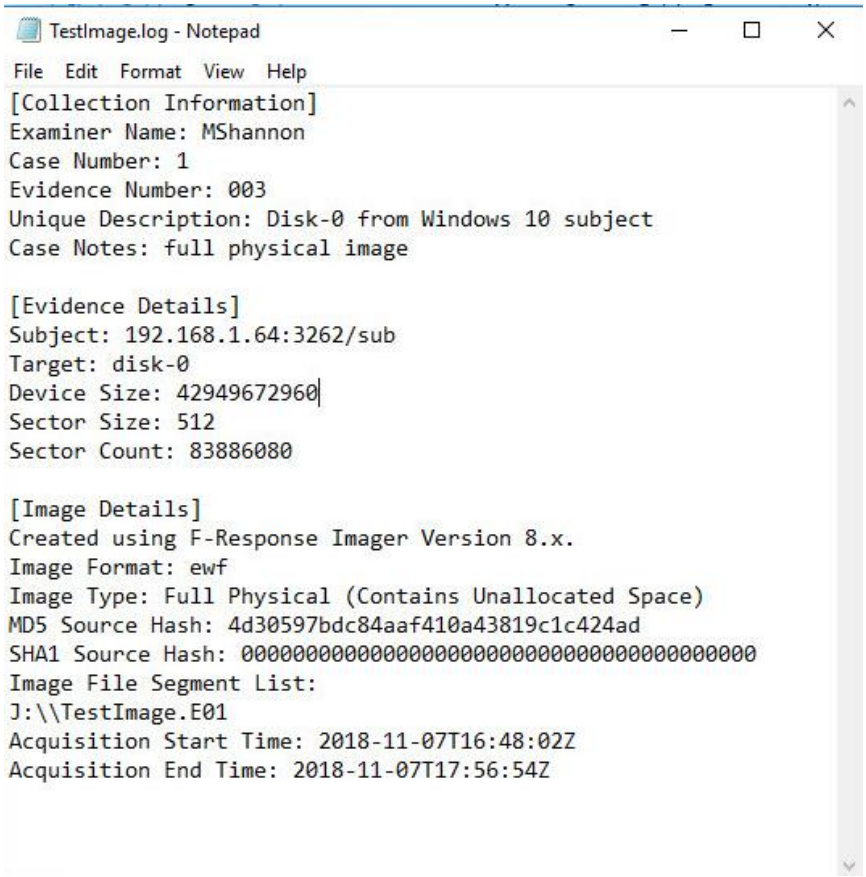




Step 8: Review the Completed Image



Once the image completes the status will show as completed. In the destination directory you will find your log file along with the image file

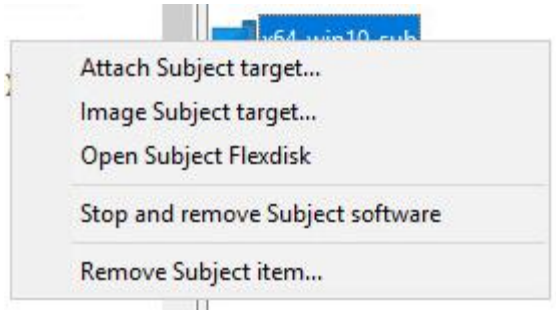


Reviewing the completed image.

Step 9: 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 right-clicking on them and choosing "Detach

Drive". 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.