F-Response Mission Guide
Connecting to a Windows target using F-Response Field Kit
Rev 1.1
June 14, 2010

Email:support@f-response.com
Website:www.f-response.com
YahooIM:fresponse_s
Phone: 1-800-317-5497

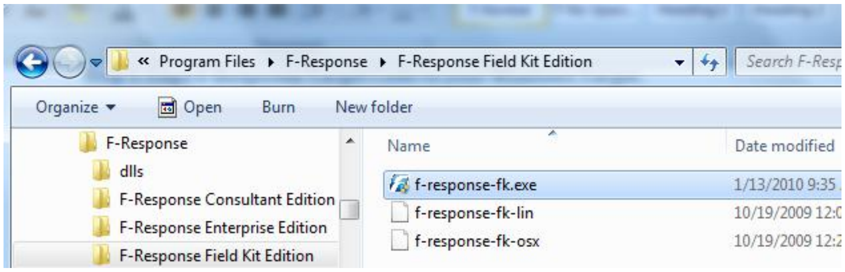
Your Mission: Connect to a remote Windows target disk using F-Response Field Kit.

Note: This guide assumes you have installed F-Response Field Kit on your Windows analyst machine and if you are using Windows XP or Windows 2003 you have installed Microsoft's iSCSI initator on your analyst machine. For more information, please reference the F-Response User Manual, or the F-Response Field Kit Edition Training Video on the F-Response Website.

F-Response FK 3.09.08 supports Windows 2000, 2003, XP, Vista, 2008, 7 (32 & 64 Bit)

Step 1: Copy F-Response Target Code to your Windows Target.

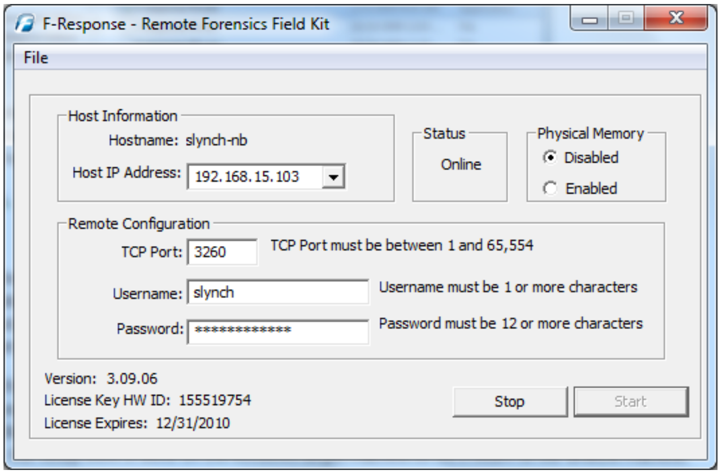
There are a few ways to deploy F-Response to a Windows target machine, but for our mission we'll use a simple USB thumb drive. If you've installed F-Response on your analyst machine using the standard default, the F-Response Windows target code is located in the C:\Program Files\F-Response\F-Response Field Kit Edition directory.


« Program Files ▸ F-Response ▸ F-Response Field Kit Edition
Search F-Resp
Organize ▾
Open
Burn
New folder
F-Response
dlls
F-Response Consultant Edition
F-Response Enterprise Edition
F-Response Field Kit Edition

Name	Date modified
f-response-fk.exe	1/13/2010 9:35
f-response-fk-lin	10/19/2009 12:0
f-response-fk-osx	10/19/2009 12:2

Copy the f-response-fk.exe file (shown on the left) to your USB thumb drive.

Next, move over to your Windows target machine and plug in the USB thumb drive along with the F-Response dongle. With both USB hardware devices inserted you are ready to start F-Response. Browse the USB thumb drive and double click on the f-response-fk.exe executable. The Remote Forensics Field Kit window will open (shown on the right).



Hostname: slynch-nb
Host IP Address: 192.168.15.103
Status: Online
Physical Memory: ● Disabled ○ Enabled
TCP Port: 3260 TCP Port must be between 1 and 65,554
Username: slynch Username must be 1 or more characters
Password: ************* Password must be 12 or more characters
Version: 3.09.06
License Key HW ID: 155519754
License Expires: 12/31/2010

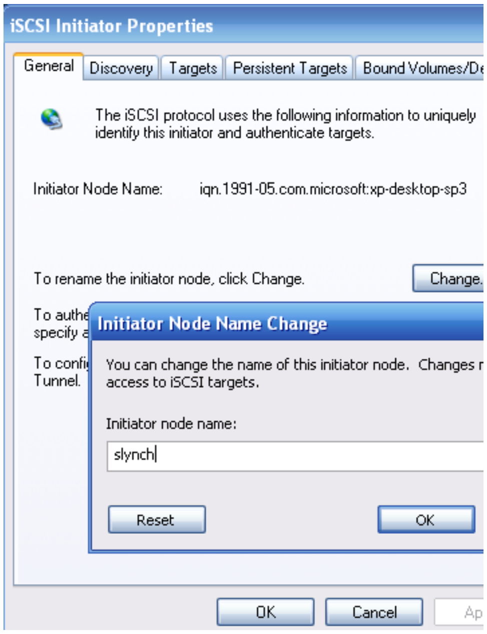
Here most of the information has already been populated so we'll leave the default settings. The hostname and IP address of this Windows target has been entered for you. F-Response has the ability to capture physical memory and present it as a local disk but that is not part of our objective for this mission so we'll leave it disabled. You'll also want to leave the default TCP port at 3260.

So, you simply need to create a username and password for F-Response to use. You can make the username and password anything you like but make note of it because you'll be using it in the configuration on your analyst machine. Click the Start button and F-Response will make any necessary Windows Firewall exceptions and actively listen on port 3260. Our setup work is done on the Windows target machine so we'll return to our analyst machine.

Step 2: Configure the iSCSI initiator on your Analyst machine.

When F-Response was installed on your analyst machine, Microsoft's iSCSI initiator should have been installed as part of the process[1]. Start the iSCSI initator on your analyst machine by double clicking on the iSCSI Initiator icon either in the Control Panel or in the Control Panel->Administrative Tools folder. There are several configuration steps here but we'll outline all the details to get you connected to the disk(s) on your target machine.

First, we'll rename the initiator node to the F-Response username we created in Step 1. Click the Change button and enter the F-Response user account name you created in step 1 then click OK.



The iSCSI protocol uses the following information to uniquely identify this initiator and authenticate targets.

Initiator Node Name: iqn.1991-05.com.microsoft:xp-desktop-sp3

To rename the initiator node, click Change.

To authe
specify a

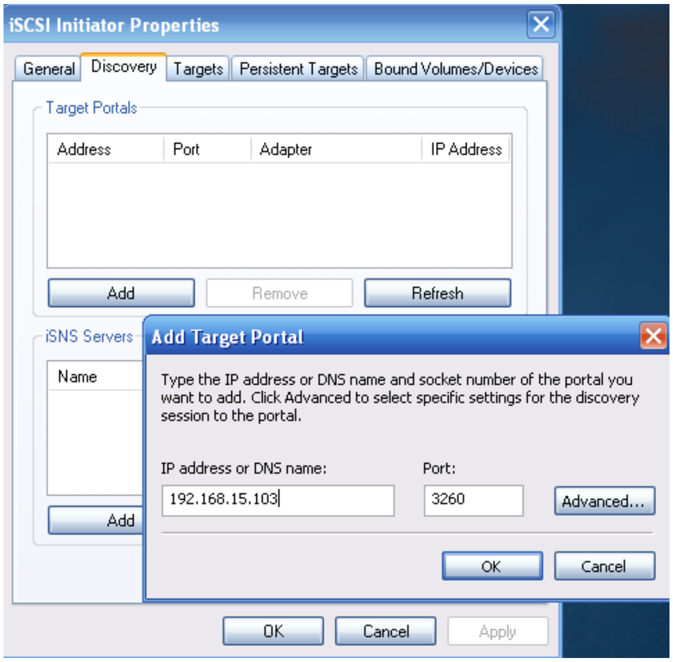
To confi
Tunnel.

Initiator Node Name Change

You can change the name of this initiator node. Changes r
access to iSCSI targets.

Initiator node name: slynch

Now click on the Discovery Tab. Under the Target Portals section you can click on the Add button to enter the IP address or Hostname of the Windows target machine. Leave the Port at the default 3260 and click on the Advanced… button.



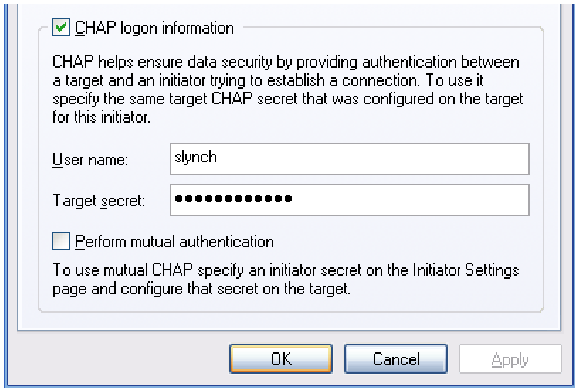
Type the IP address or DNS name and socket number of the portal you want to add. Click Advanced to select specific settings for the discovery session to the portal.

IP address or DNS name: 192.168.15.103

Port: 3260

Here under the Advanced Settings you can check the box for CHAP logon information. The User name: field should already be populated with the F-Response user account you created so you'll only need to enter the password in the Target Secret: field.

And that's it—click OK to exit both windows and return to the main iSCSI Initiator Properties window.



☑ CHAP logon information

CHAP helps ensure data security by providing authentication between a target and an initiator trying to establish a connection. To use it specify the same target CHAP secret that was configured on the target for this initiator.

User name: slynch

Target secret: ●●●●●●●●●●●●

□ Perform mutual authentication

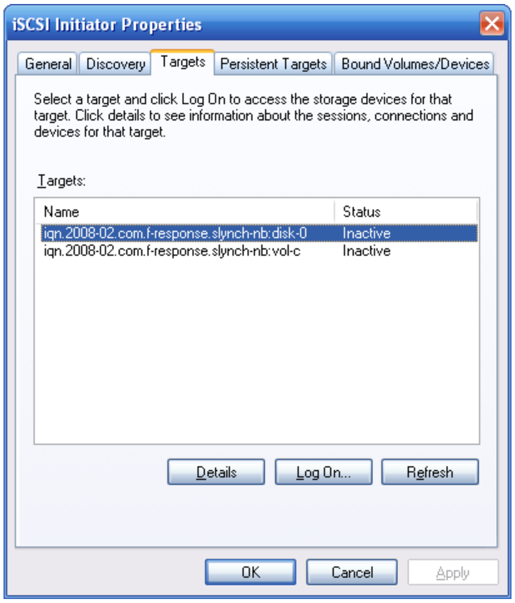
To use mutual CHAP specify an initiator secret on the Initiator Settings page and configure that secret on the target.

[1] Windows Vista, Windows 2008, and Windows 7 come with the iSCSI Initiator installed by default.

Step 3: Login to the F-Response target disk.

Back at the iSCSI Initiator Properties window select the Targets tab where you will find a listing of available physical disks and logical volumes on your Windows target machine. See the Understanding F-Response Disk section below for more information on F-Response disk naming convention.

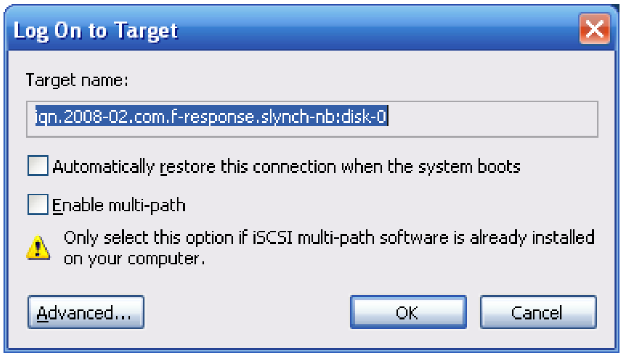
Here you will highlight the target disk or volume you wish to connect to and click Log On… The Log On to Target window will appear:



Select a target and click Log On to access the storage devices for that target. Click details to see information about the sessions, connections and devices for that target.

Targets:

Name	Status
iqn.2008-02.com.f-response.slynch-nb:disk-0	Inactive
iqn.2008-02.com.f-response.slynch-nb:vol-c	Inactive



Target name:
iqn.2008-02.com.f-response.slynch-nb:disk-0

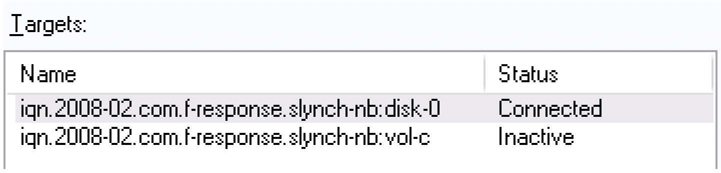
□ Automatically restore this connection when the system boots

□ Enable multi-path

Only select this option if iSCSI multi-path software is already installed on your computer.

Here you will click on the Advanced… button and the Advanced Settings window you saw in Step 2 will open. Again, you will check the box for CHAP Logon Information and enter your F-Response password in the Target Secret field to connect.

Click OK to exit back to your iSCSI Initiator Properties window where you will see the Status for your target disk has changed to Connected.



Targets:

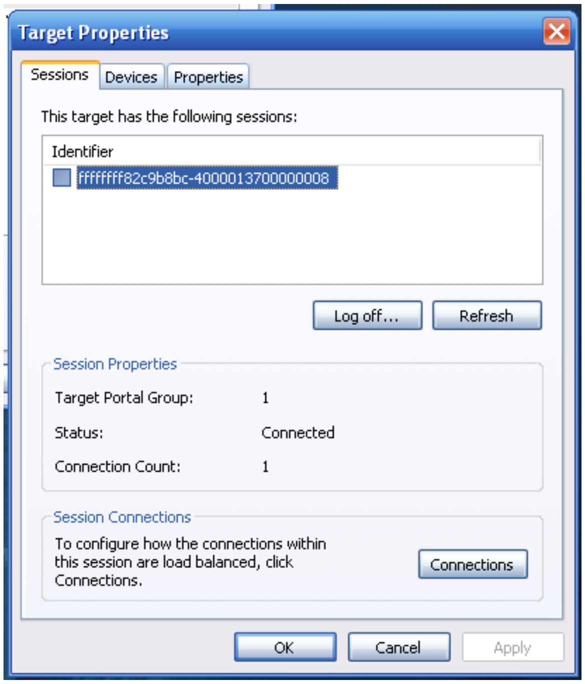
Name	Status
iqn.2008-02.com.f-response.slynch-nb:disk-0	Connected
iqn.2008-02.com.f-response.slynch-nb:vol-c	Inactive

Step 4: Fire up the tool of your choice!

F-Response is a vendor neutral product. Once F-Response presents the remote target disk as a write blocked local connection, we step out of your way so that you can select the right tool to get your job done. At this point, you can reach into your toolbox and apply the tool of your choice to the target disk(s).

Step 5: Removing F-Response:

When you have finished using F-Response on the target machine, highlight the target disk you want to disconnect from and click the details button. The Target Properties window will open:



This target has the following sessions:

Identifier
□ ffffffff82c9b8bc-4000013700000008

Session Properties

Target Portal Group: 1
Status: Connected
Connection Count: 1

Session Connections

To configure how the connections within this session are load balanced, click Connections.

Under the Identifier section, check the box and click Log Off… Click the OK button twice to exit the iSCSI initiator. Don't forget to take your F-Response dongle with you!

Understanding F-Response Disk Naming

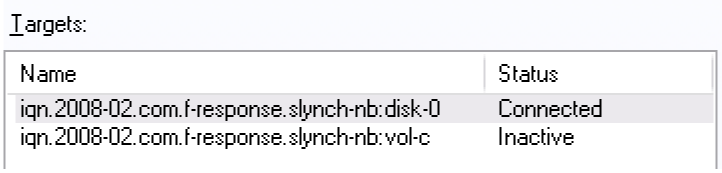
F-Response uses the following naming convention for target disks:

iqn.2008-02.com.f-response.HOSTNAME.O/S disk name

We are only concerned with the "HOSTNAME.O/S disk name" portion of the name.

HOSTNAME is the name of your Windows target machine.

For the "O/S disk name," F-Response can access both remote physical disks and the logical volumes on those disks. Windows identifies hard disks using the format "disk-#". The '#' portion is a number, starting with zero, representing the physical drive. Windows identifies logical volumes in the format "vol-*", where "*" is a letter corresponding to a volume on the remote physical disk. For example:


Targets:

Name	Status
iqn.2008-02.com.f-response.slynch-nb:disk-0	Connected
iqn.2008-02.com.f-response.slynch-nb:vol-c	Inactive

The first target in this list is on the target machine named 'slynch-nb' We can tell by the last portion of the name (disk-0) this is physical disk 1 (and any logical volumes it may contain). The second target in this list is on the same machine but is logical volume C as indicated by the 'vol-c' portion of the naming convention.