YOUR MISSION: USE THE F-RESPONSE IMAGER TO COLLECT INDIVIDUAL FILES/FOLDERS TO A CONTAINER

Note: F-Response Imager is a free tool designed for use with F-Response products. This guide assumes you are familiar with your current F-Response product and have a connected F-Response presented target you are looking to image.

Often a collection will involve only specific files for a custodian, and sometimes from various resources i.e.,computer hard drive, cloud storage, webmail. In cases like this it is nice to be able to consolidate the collection into a single container which can then be processed into an expert witness file (E01) or VHD for preservation and analysis.

STEP 1: NOTE YOUR F-RESPONSE TARGET(S)

Take note of the volume letter assigned for the F-Response attached target. In this example, here we have a virtual device attached using F-Response Universal, specifically a DiscoveryShare[™] from a Windows subject.

**Note the term "virtual device" includes network shares (DiscoveryShares™, MemoryShares™), and F-Response



connector volumes. Please refer to the F-Response Imager Manual for more details.**

STEP 2: START THE F-RESPONSE IMAGER CONSOLE

Once you have your F-Response target connected you'll want to start the **F-Response Imager Console**:



The Imager will open with the default folder structure:

 F-Response Imager File Image Containers View Help 					-		×
F-Response Devices	Active Images						
F-Response Devices Virtual Devices F-Response Devic	Name	Source Device	Last Status				
Containers ×	Completed Imag	Jes					×
Name	Name	Sour	ce				
Ready							

STEP 3: CREATE A CONTAINER

So, we need to create a container for our files of interest. A container is just as it sounds—a holding place for the list of files and folders we intend to collect. Remember that files and folders in the container <u>are not preserved</u> until the container is converted to an image.

To create a container, go to File – New Container...



The Create Container... window will open. Here we will give the container a name and location.

Create Containe	er		>
Container Name	SuspectA_Data		
Container Path	C:\Collections		Browse
Total Available Space	e = 25470MB	Create	Cancel

Click the Create button and you will find your new container in the Containers pane in the console window:



STEP 4: POPULATE THE CONTAINER

So, we are now ready to add files and folders to the container. A nice feature of F-Response Imager is that it is integrated with Windows Explorer. You can browse your data for a quick review/triage and then simply right click on the file or folder to add it to the container:

> This PC > x64-win81-sub-Disc	overyShare-C (\\X64-WIN10) (E:) > Users >		5 V	Search Users
	Name	Date modified	Туре	Size
	All Users	8/22/2013 10:45 AM	File folder	
	Default	8/22/2013 3:10 PM	File folder	
	Default User	8/22/2013 10:45 AM	File folder	
	feastast	3/19/2014 10:54 PM	File folder	
	Open	5/7/2015 4:44 PM	File folder	
	Open in new window	8/22/2013 11:36 AM	File folder	
	Pin to Quick access Restore previous versions Pin to Start	8/22/2013 11:34 AM	Configuration sett	1 KB
	F-Response Imager >	Add to Logical I	Evidence Container "Su	ispectA_Data"

Continue to browse and add the needed files and folders to your container. When you are ready, you can review what is in the container by right clicking on the container in the console and choosing **Show Contents...**, or simply double clicking on the container:

Jundanier En	try		
X64-WIN10	x64-win81-sub-D	scoveryShare-C\Users\frestest\ntuser.dat.LOG1	
X64-WIN10	x64-win81-sub-D	scoveryShare-C\Users\frestest\ntuser.dat.LOG2	
X64-WIN10	x64-win81-sub-D	scoveryShare-C\Users\frestest\NTUSER.DAT	
X64-WIN10	\s3-jumbo\29f3a6	9e854c8fabd35f67c489d329bealligator - test.jpg	
X64-WIN10	\s3-jumbo\25b23b	de3fc57b921f54ce25a0d32e15F-Response Summ	ary-May2009.doc
X64-WIN10	\s3-jumbo\4f80a9	o77ad 194b4851498beca9dc82fMissionGuide-FRes	sponseConsultantEdition-Windows.pdf
X64-WIN10	\s3-jumbo\1de458	fec9be17b39c550dd59eaf3af2~\$Response Summ	nary-May2009.doc
X64-WIN10	\s3-jumbo\FRespo	nse_Latest	
	1		Convert to Taylor

Here you can adjust the files/folders you are about to image from the various resources by adding or removing accordingly. Click **Refresh** to give it a final review and when you are happy with the results click the **Convert to Image** button.

F-Response Mission Guide Use the F-Response Imager to collect files to a Container Rev 2.0 March 15, 2016

STEP 5: CONVERT TO AN IMAGE

Once you click Convert to Image the details window will open:

Format	Both 🗸	
Path for Image Files	M:\	
Hash	MD5 V	
Compression	None 🗸	
Examiner Name	Mr. Examiner	
Case Number	123	
Evidence Number	1	
Unique Description	Suspect A Data	
Notes	File collection from Suspect A	hard drive and Amazon acct

We'll work through this window from the top down. First, we'll set the Format—you have a choice **E01** (Expert Witness), **VHD** (Virtual Hard Disk), or **Both**. This option determines what the Imager will provide at the end of the collection.

The **Path for Image Files** determines our destination drive—this must be a physical drive attached to our examiner machine (we cannot image to a network share).

Next we can chose 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 6: REVIEW

The details window will close and you can monitor the status of your image in Active Images pane of the console window.

Active images		
Name	Source Device	Last Status
SuspectA Data	29%	

When the image has completed it will be moved under the **Completed Images** pane. If you right click on the completed image in the list, you can choose **Open Image Path** to view your collection.

→ This PC → Destination (M:) V					Search I
55	Name	Date modified	Туре	Size	
	f-response-hash-SuspectA_Data	10/12/2015 4:29 PM	CSV File		10 KB
	SuspectA_Data.E01	10/12/2015 4:29 PM	E01 File	2,097,	155 KB
	SuspectA_Data.E02	10/12/2015 4:29 PM	E02 File	1,421,	698 KB
	SuspectA_Data	10/12/2015 4:29 PM	Text Document		2 KB
ts	🕳 SuspectA_Data	10/12/2015 4:29 PM	Hard Disk Image File	102,	676 KB
ts	SuspectA_Data	10/12/2015 4:29 PM	Hard Disk Image File	102,	676 KB

Here you will find your image files, a CSV listing of the collected files with their corresponding hashes, and text file report.

1	target-file	md5	sha
2	\\?\Volume{00000037-0000-0000-007e-00000000000}\X64-WIN10\F-Response-899b8313349d15c2-en_US\s3-jumbo\Headshot.JPG	1e1250548f71b88bd415d8b49fce4005	fa034d864cdbc4c5259ece64e138cfe6c35eec84
3	\\?\Volume(00000037-0000-0000-007e-00000000000)\X64-WIN10\F-Response-899b8313349d15c2-en_U\$\s3-jumbo\MissionGuide-FResponseConsulta	4f80a9b77ad194b4851498beca9dc82f	23aa7635c53efaebd6c0936fe1017a7655eefdde
4	\\?\Volume(00000037-0000-0000-007e-00000000000}\X64-WIN10\F-Response-899b8313349d15c2-en_US\s3-jumbo\MissionGuide-FResponseEnterpri	451efc2d86fc1de226e66e18a5e2b473	4a025f387adb858fdaaf1b3bb97cd4e948070a3c
5	\\?\Volume{00000037-0000-0000-007e-00000000000}\X64-WIN10\x64-win81-sub-DiscoveryShare-C\ProgramData\ntuser.pol	4ae547bf6d5edda81fd343399d14884e	83555f53351f7fbd26a266831815d002fc6c3a66
6	\\?\Volume(00000037-0000-0000-007e-00000000000)\X64-WIN10\F-Response-899b8313349d15c2-en_US\s3-jumbo\MissionGuide-FResponseEnterpri	76f6a8f0eeb70ae2d8c26f3170bc47be	74588bade88582a38f4a0352ca33e2d8635c4d1f

If you open the text file report you will find all your notes and the complete details for the collection:

SuspectA_Data - Notepad X File Edit Format View Help [Collection Information] Examiner Name: Mr. Examiner Case Number: 123 Evidence Number: 2 Unique Description: Suspect A Data Case Notes: File collection from Suspect A Hard drive and Amazon [Evidence Details] VHD File: M:\SuspectA Data.vhd Device Size: 3602421760 Bytes Per Sector: 512 Total Sectors: 7035980 [Image Details] Created using F-Response Imager Version 2.0.1.7. Image Format: E01 & VHD Image Type: Specific Files (Logical Container) MD5 Source Hash: 96da4f7a1540cfc716062bdbd13b87eb SHA1 Source Hash: 9cc47094e4cbcfc2a8323b970a57a491b518bbb4 Image file Segment list: SuspectA Data.E01 SuspectA Data.E02 Acquisition Start Time: 10-12-2015:20:28:54 UTC(0) Acquisition End Time: 10-12-2015:20:29:50 UTC(0) Total Collection Duration:: 00:00:55

And that's it! You can now make a backup/working copy of your image and load it into your forensic or eDiscovery tool(s) for verification.