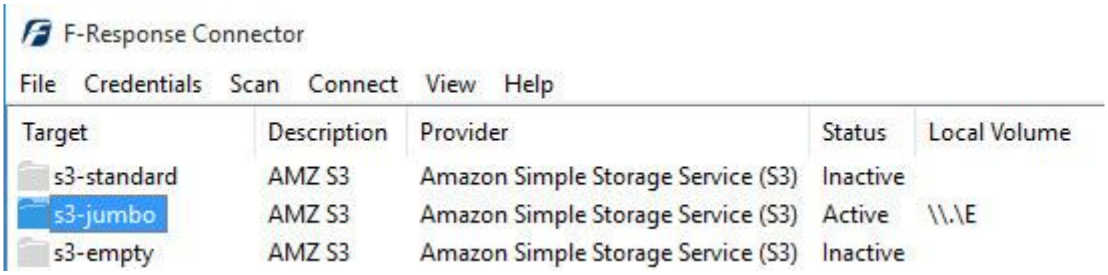
YOUR MISSION: USE THE F-RESPONSE IMAGER TO CREATE A VIRTUAL DEVICE IMAGE

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.

STEP 1: NOTE YOUR F-RESPONSE TARGET

Take note of the volume letter assigned for the F-Response attached device. For example, here we have an Amazon S3 container attached to our examiner machine using the F-Response Connector:

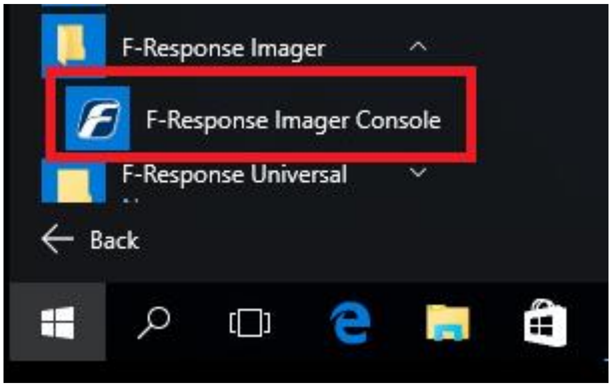


Target	Description	Provider	Status	Local Volume
s3-standard	AMZ S3	Amazon Simple Storage Service (S3)	Inactive	
s3-jumbo	AMZ S3	Amazon Simple Storage Service (S3)	Active	\\.\E
s3-empty	AMZ S3	Amazon Simple Storage Service (S3)	Inactive	

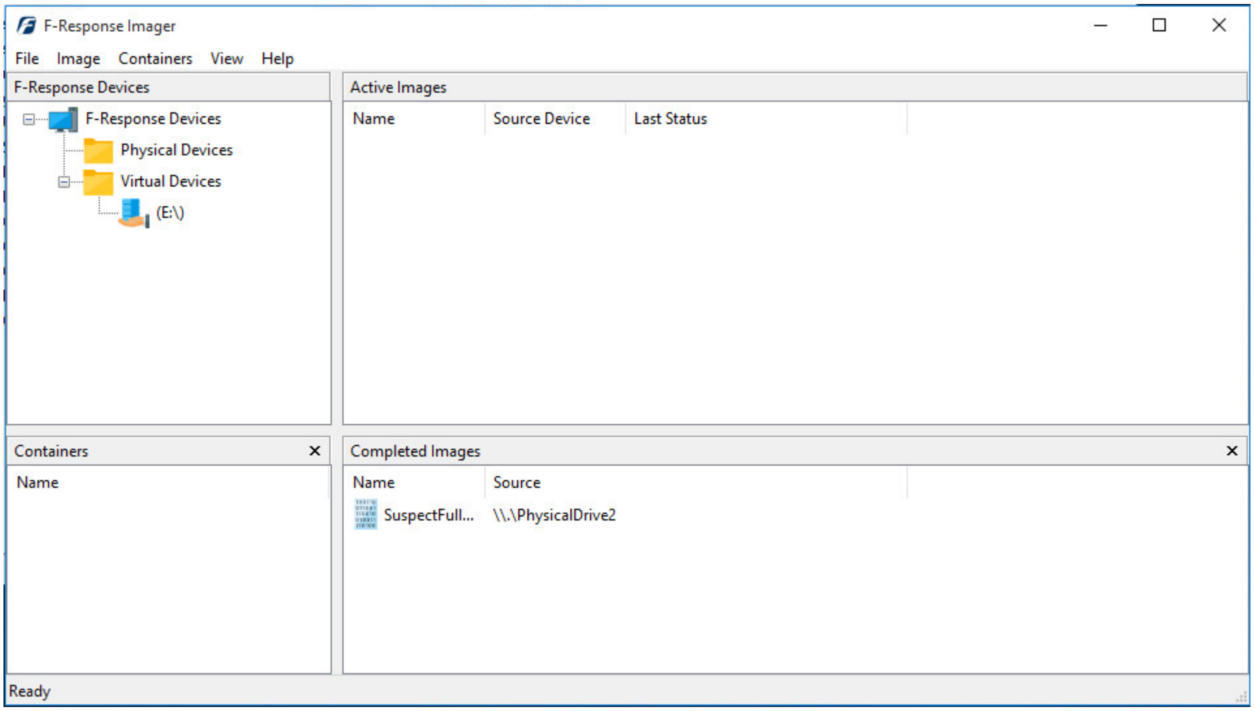
Note the term “virtual device” includes network shares (DiscoveryShares™, MemoryShares™), and F-Response Connector volumes. Please refer to the F-Response Imager Manual for more details.

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**:



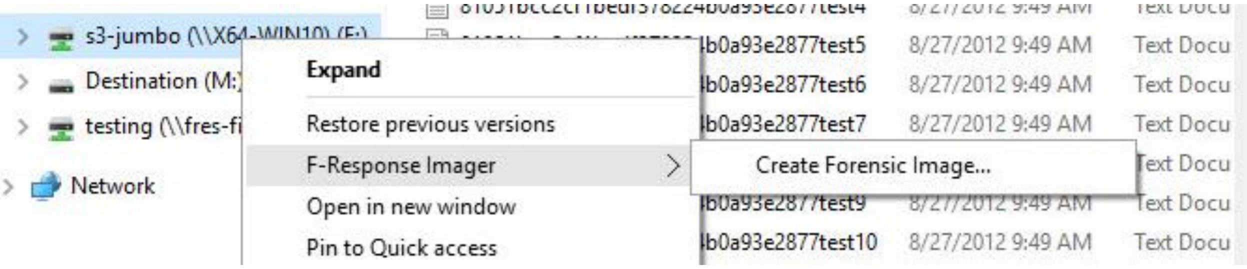
The Imager will open with the default folder structure:



If you do not see your Virtual Device listed, go to **File – Refresh Devices** to update the Imager Console.

STEP 3: SPECIFY THE IMAGE DETAILS

So, you are now ready to set up your image. A nice feature of F-Response Imager is that it is integrated with Windows Explorer. You can browse your data for a quick check/triage and then simply right click on the volume to start the image setup:



Right-click and choose **F-Response Imager - Create Forensic Image…** to open the **Image Physical or Virtual Device** window where we'll set all the details and begin the imaging process:

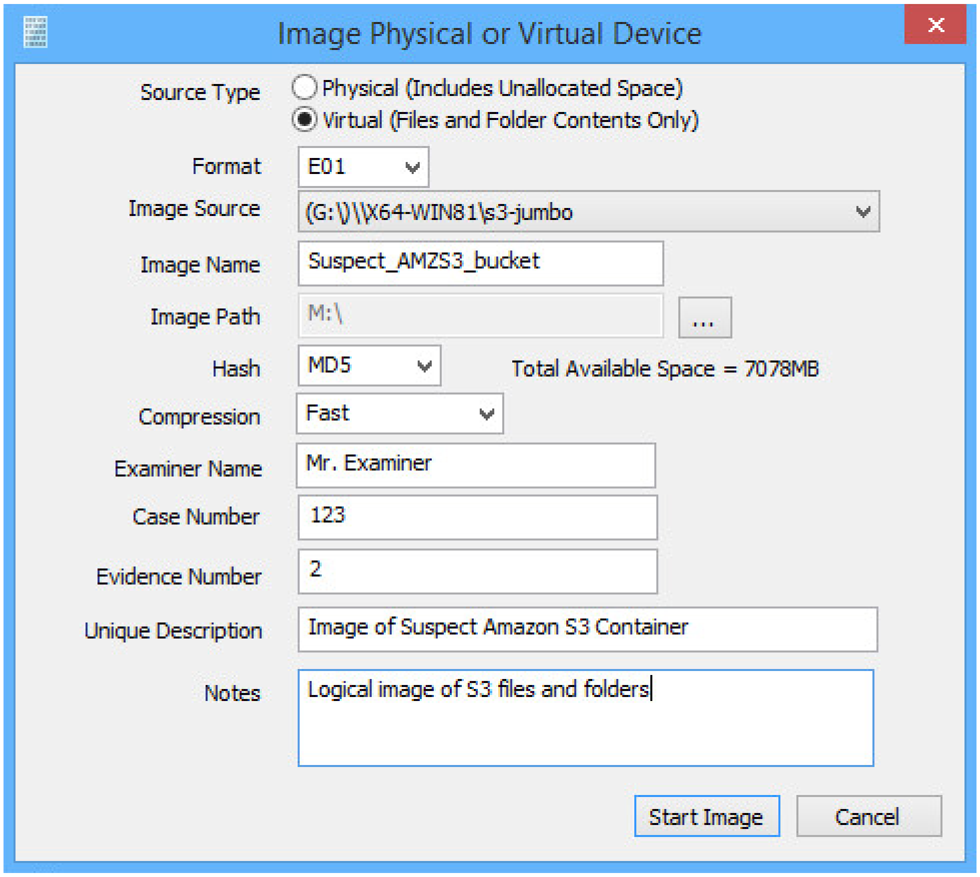


Image Physical or Virtual Device

Source Type ○ Physical (Includes Unallocated Space)
● Virtual (Files and Folder Contents Only)

Format: E01
Image Source: (G:\)\\X64-WIN81\s3-jumbo
Image Name: Suspect_AMZS3_bucket
Image Path: M:\
Hash: MD5
Total Available Space = 7078MB
Compression: Fast
Examiner Name: Mr. Examiner
Case Number: 123
Evidence Number: 2
Unique Description: Image of Suspect Amazon S3 Container
Notes: Logical image of S3 files and folders

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

Next you can select the image **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.

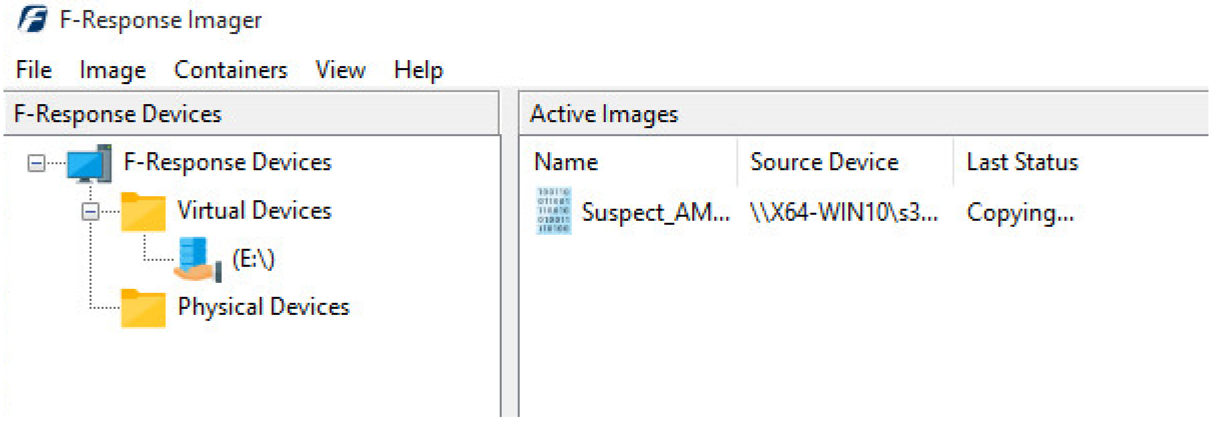
Image Source should be populated if we opened this window from Windows Explorer, just verify the drive letter is correct from Step 1. For **Image Path** we need to choose our destination drive—this must be a physical drive attached to our examiner machine (we cannot image to a network share).

Next we can 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.

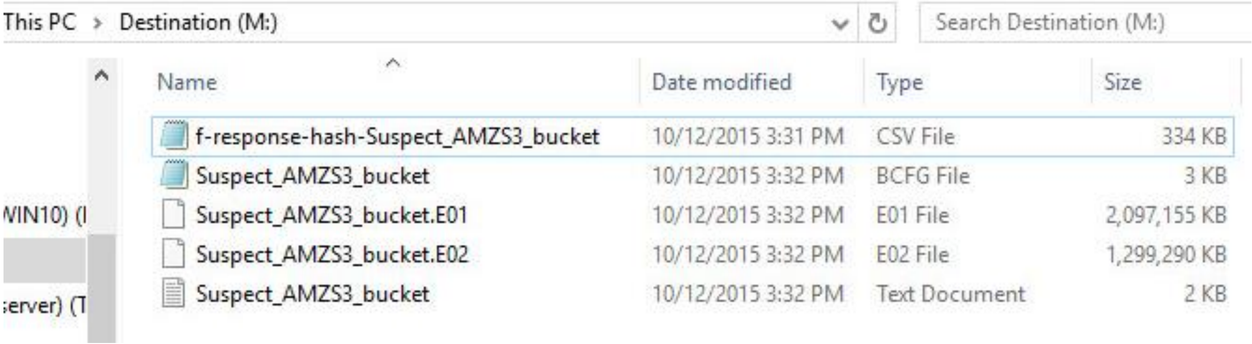
STEP 4: REVIEW

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



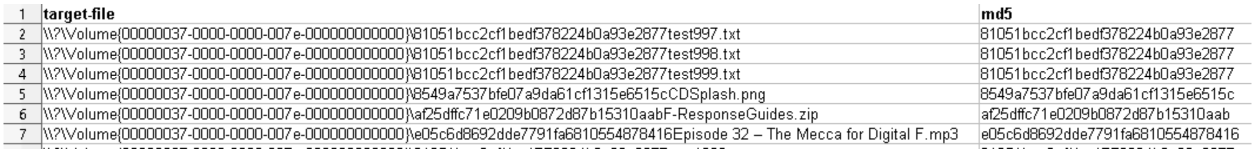
Name	Source Device	Last Status
Suspect_AM...	\\X64-WIN10\s3...	Copying...

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.



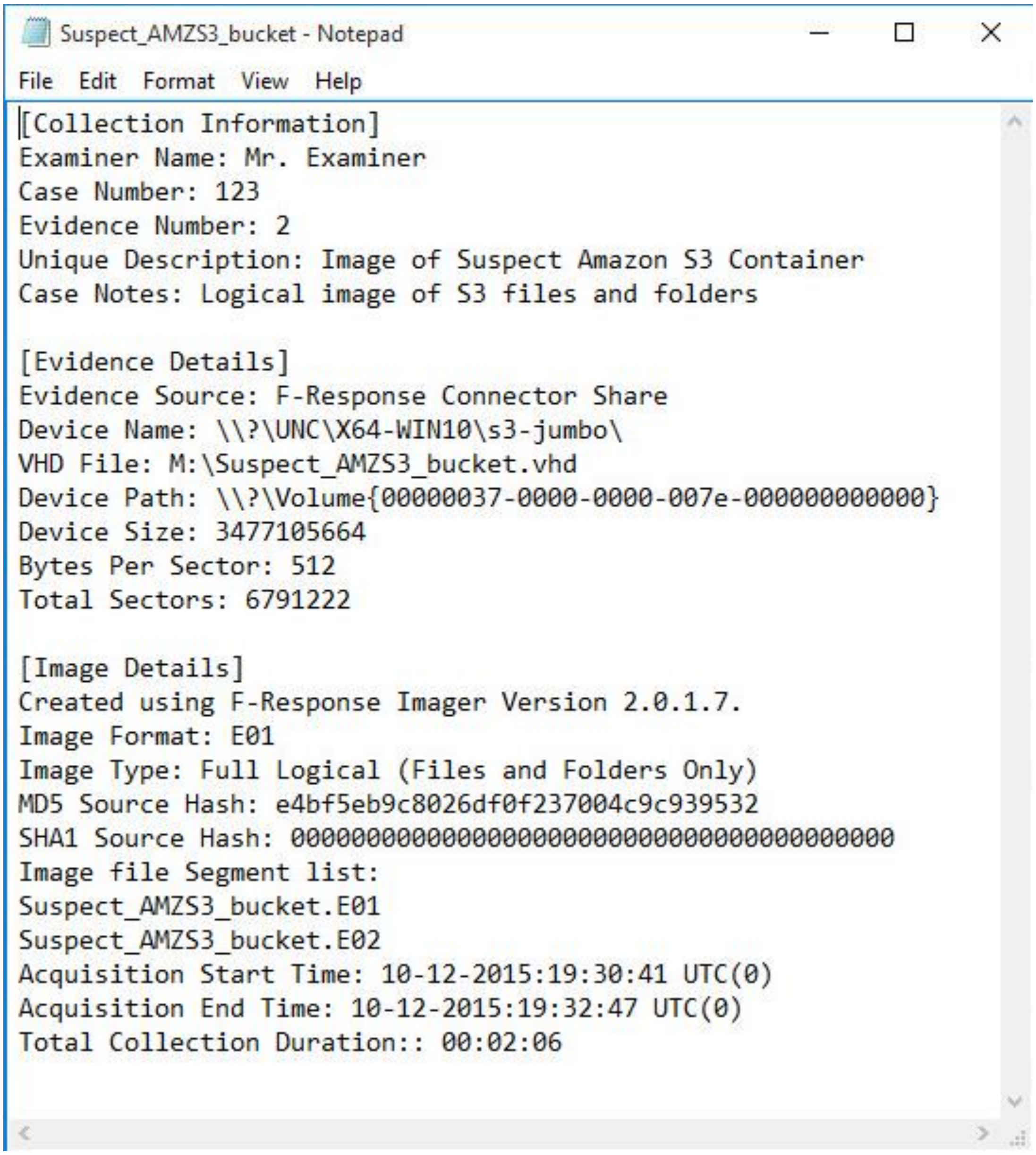
Name	Date modified	Type	Size
f-response-hash-Suspect_AMZS3_bucket	10/12/2015 3:31 PM	CSV File	334 KB
Suspect_AMZS3_bucket	10/12/2015 3:32 PM	BCFG File	3 KB
Suspect_AMZS3_bucket.E01	10/12/2015 3:32 PM	E01 File	2,097,155 KB
Suspect_AMZS3_bucket.E02	10/12/2015 3:32 PM	E02 File	1,299,290 KB
Suspect_AMZS3_bucket	10/12/2015 3:32 PM	Text Document	2 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**
2	\\?\Volume{00000037-0000-0000-007e-000000000000}\81051bcc2cf1bedf378224b0a93e2877test997.txt	81051bcc2cf1bedf378224b0a93e2877
3	\\?\Volume{00000037-0000-0000-007e-000000000000}\81051bcc2cf1bedf378224b0a93e2877test998.txt	81051bcc2cf1bedf378224b0a93e2877
4	\\?\Volume{00000037-0000-0000-007e-000000000000}\81051bcc2cf1bedf378224b0a93e2877test999.txt	81051bcc2cf1bedf378224b0a93e2877
5	\\?\Volume{00000037-0000-0000-007e-000000000000}\8549a7537bfe07a9da61cf1315e6515cCDSplash.png	8549a7537bfe07a9da61cf1315e6515c
6	\\?\Volume{00000037-0000-0000-007e-000000000000}\af25dffc71e0209b0872d87b15310aabF-ResponseGuides.zip	af25dffc71e0209b0872d87b15310aab
7	\\?\Volume{00000037-0000-0000-007e-000000000000}\e05c6d8692dde7791fa6810554878416Episode 32 – The Mecca for Digital F.mp3	e05c6d8692dde7791fa6810554878416

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



```
[Collection Information]
Examiner Name: Mr. Examiner
Case Number: 123
Evidence Number: 2
Unique Description: Image of Suspect Amazon S3 Container
Case Notes: Logical image of S3 files and folders

[Evidence Details]
Evidence Source: F-Response Connector Share
Device Name: \\?\UNC\X64-WIN10\s3-jumbo\
VHD File: M:\Suspect_AMZS3_bucket.vhd
Device Path: \\?\Volume{00000037-0000-0000-007e-000000000000}
Device Size: 3477105664
Bytes Per Sector: 512
Total Sectors: 6791222

[Image Details]
Created using F-Response Imager Version 2.0.1.7.
Image Format: E01
Image Type: Full Logical (Files and Folders Only)
MD5 Source Hash: e4bf5eb9c8026df0f237004c9c939532
SHA1 Source Hash: 0000000000000000000000000000000000000000
Image file Segment list:
Suspect_AMZS3_bucket.E01
Suspect_AMZS3_bucket.E02
Acquisition Start Time: 10-12-2015:19:30:41 UTC(0)
Acquisition End Time: 10-12-2015:19:32:47 UTC(0)
Total Collection Duration:: 00:02:06
```

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 and analysis.