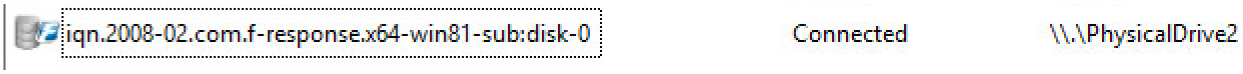
YOUR MISSION: USE THE F-RESPONSE IMAGER TO CREATE A PHYSICAL IMAGE IN EXPERT WITNESS FILE FORMAT (E01)

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 device you are looking to image.

STEP 1: NOTE YOUR F-RESPONSE TARGET

Take note of the locally assigned physical drive of your remote F-Response target. For example, here we have a remote target machine's physical disk-0 attached as physical drive-1 on our examiner machine:

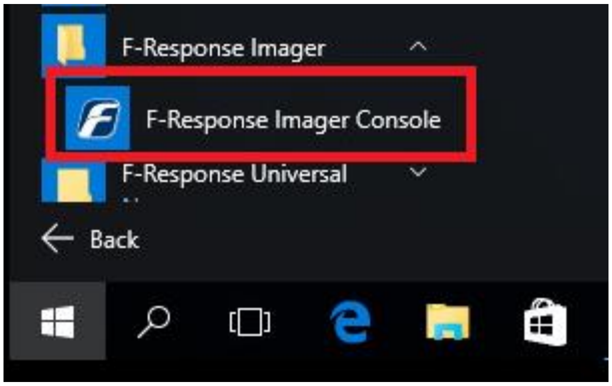


iqn.2008-02.com.f-response.x64-win81-sub:disk-0 Connected \\.\PhysicalDrive2

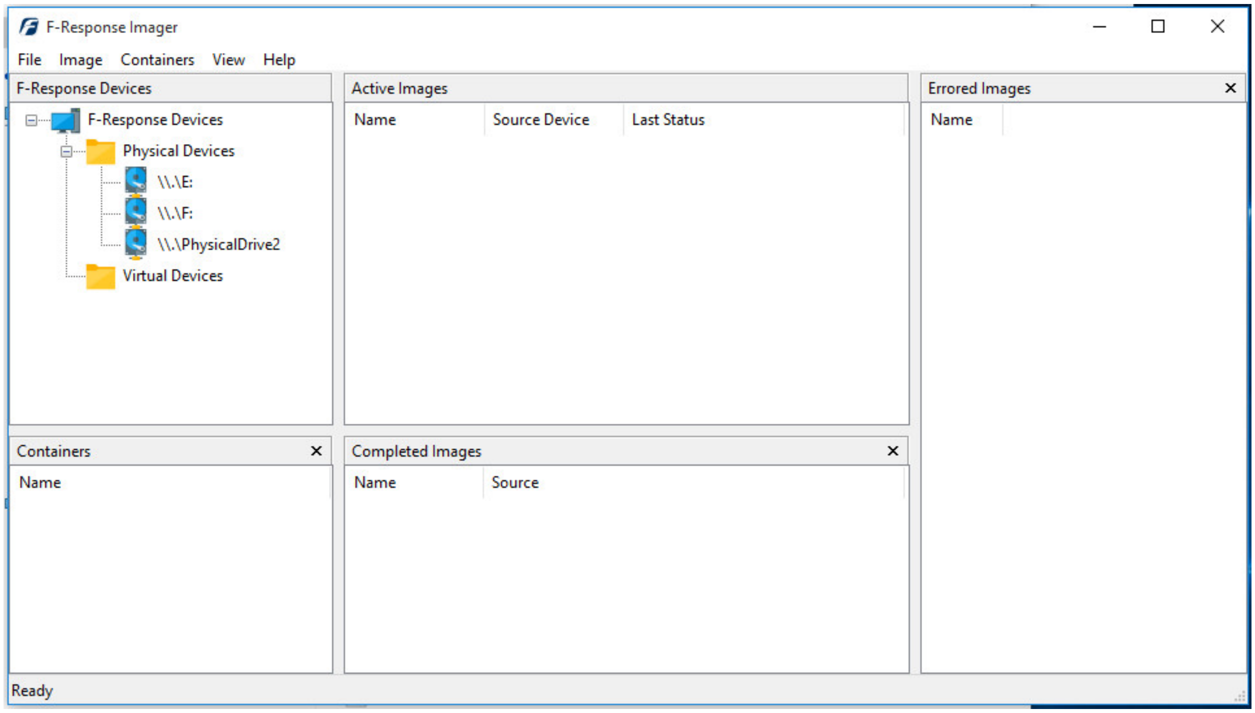
Note some F-Response tools present subject resources as a virtual device. Virtual devices include network shares, (DiscoveryShares™, MemoryShares™), and F-Response Connector volumes. Please refer to the F-Response Imager Manual or Mission guide available on our website to learn about creating a container or logical image of these virtual devices.

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:



Go to **File – New Image…** or double click on **\\.\PhysicalDrive2** to open the imaging options.

STEP 3: SPECIFY THE IMAGE DETAILS

In the **Image Physical or Virtual Device** window we'll set all the details and begin the imaging process:

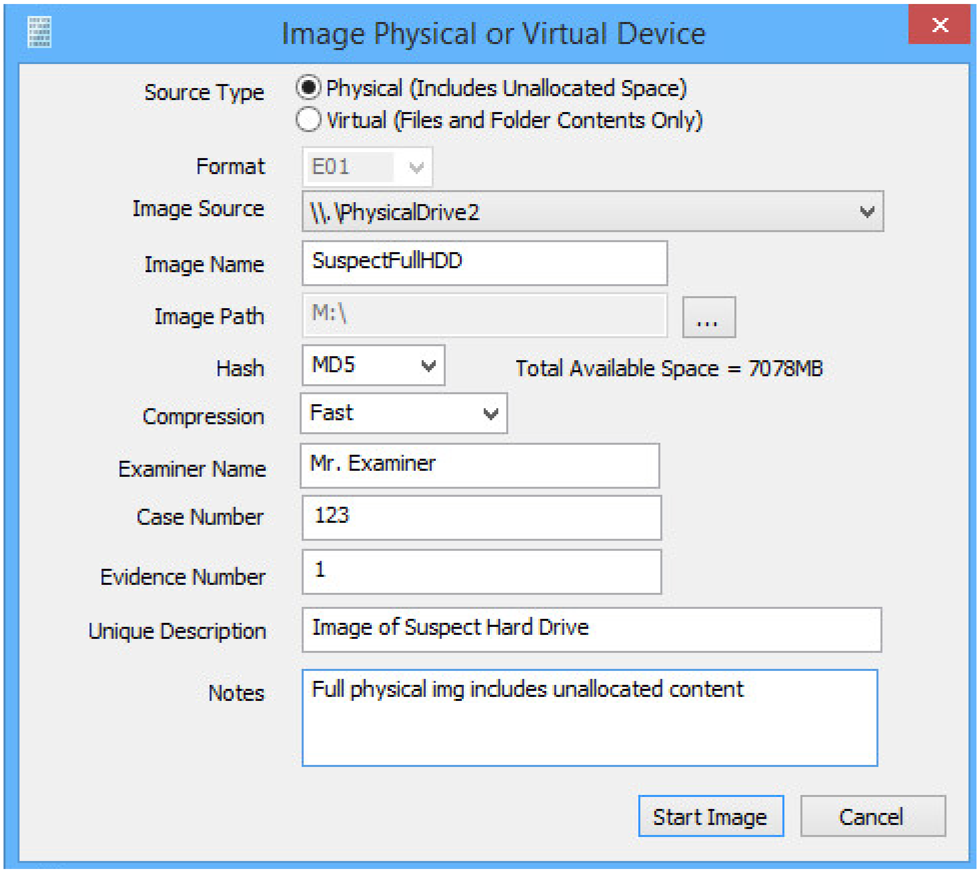


Image Physical or Virtual Device

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

Format: E01

Image Source: \\.\PhysicalDrive2

Image Name: SuspectFullHDD

Image Path: M:\

Hash: MD5

Total Available Space = 7078MB

Compression: Fast

Examiner Name: Mr. Examiner

Case Number: 123

Evidence Number: 1

Unique Description: Image of Suspect Hard Drive

Notes: Full physical img includes unallocated content

We'll work through this window from the top down. First, we can see the **Source Type** is set to **Physical** by default. This will create a full disk image of the subject including unallocated content.

The **Image Source** should be populated with the drive to be imaged. If needed we can select the dropdown and choose the correct physical drive from step 1.

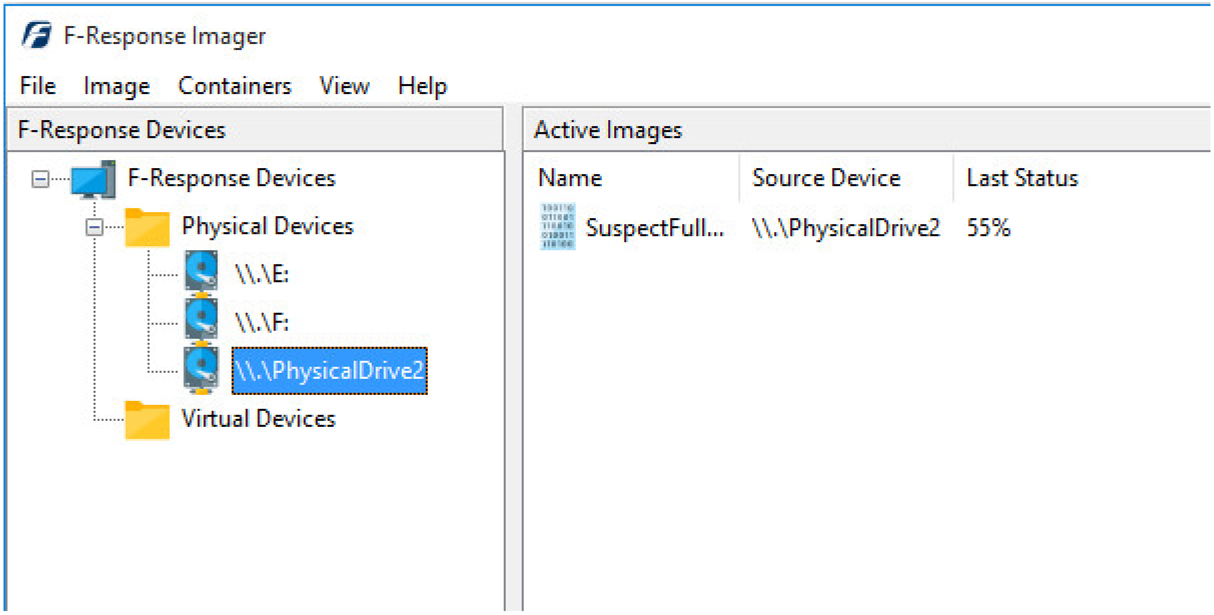
Assign a name for your image file in the **Image Name** field. For **Image Path** we need to choose our destination drive—this must be a physical drive attached to our examiner machine (we cannot image to a network share).

Lastly we can chose a **Hash** format and **Compression** level (compressing the resulting image is optional). 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.

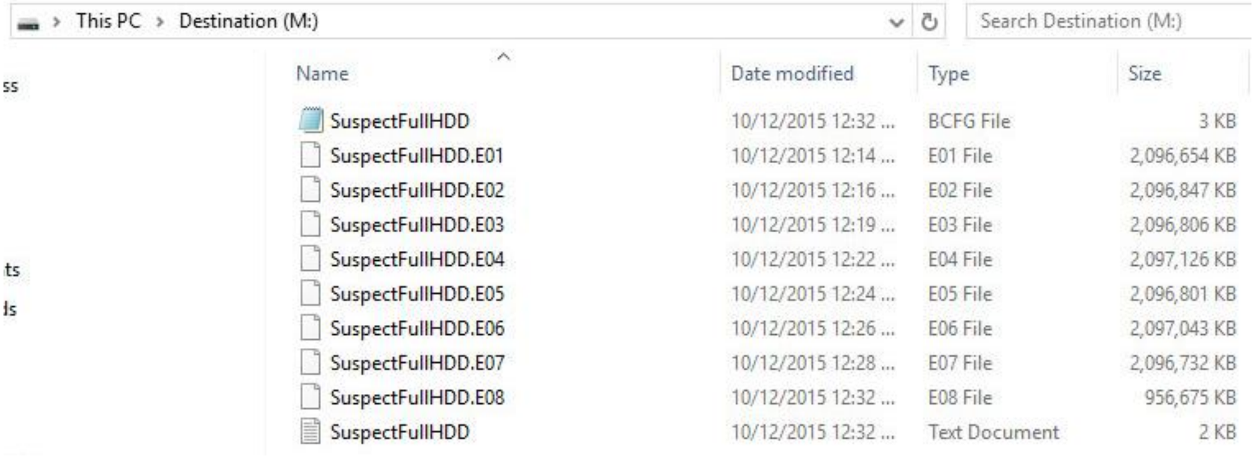
STEP 4: REVIEW

The details window will close and you can monitor the progress of your image in the console window.



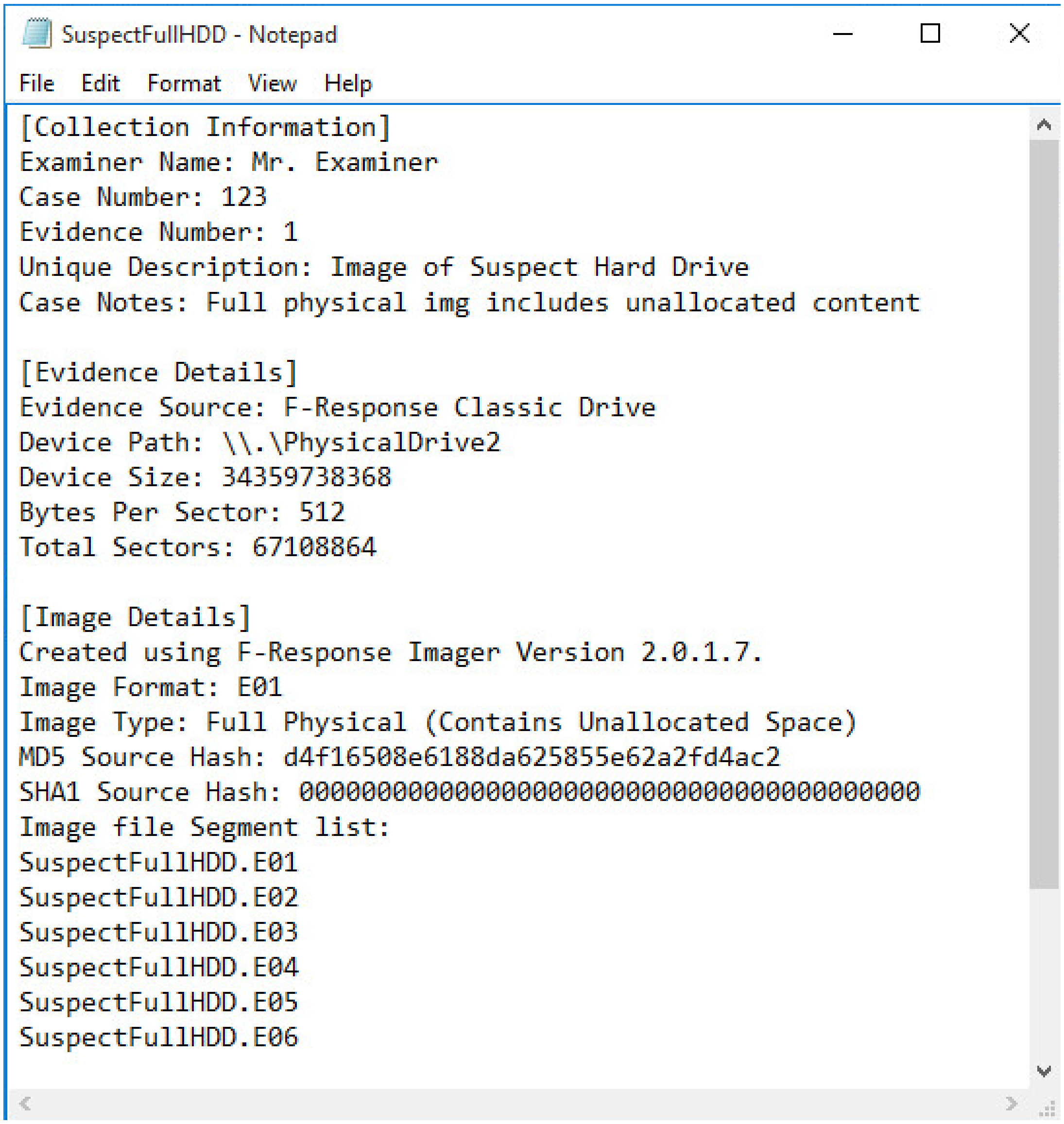
Name	Source Device	Last Status
SuspectFull...	\\.\PhysicalDrive2	55%

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



Name	Date modified	Type	Size
SuspectFullHDD	10/12/2015 12:32 ...	BCFG File	3 KB
SuspectFullHDD.E01	10/12/2015 12:14 ...	E01 File	2,096,654 KB
SuspectFullHDD.E02	10/12/2015 12:16 ...	E02 File	2,096,847 KB
SuspectFullHDD.E03	10/12/2015 12:19 ...	E03 File	2,096,806 KB
SuspectFullHDD.E04	10/12/2015 12:22 ...	E04 File	2,097,126 KB
SuspectFullHDD.E05	10/12/2015 12:24 ...	E05 File	2,096,801 KB
SuspectFullHDD.E06	10/12/2015 12:26 ...	E06 File	2,097,043 KB
SuspectFullHDD.E07	10/12/2015 12:28 ...	E07 File	2,096,732 KB
SuspectFullHDD.E08	10/12/2015 12:32 ...	E08 File	956,675 KB
SuspectFullHDD	10/12/2015 12:32 ...	Text Document	2 KB

Here you will find your evidence files along with a text file report. If you open the 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: 1
Unique Description: Image of Suspect Hard Drive
Case Notes: Full physical img includes unallocated content

[Evidence Details]
Evidence Source: F-Response Classic Drive
Device Path: \\.\PhysicalDrive2
Device Size: 34359738368
Bytes Per Sector: 512
Total Sectors: 67108864

[Image Details]
Created using F-Response Imager Version 2.0.1.7.
Image Format: E01
Image Type: Full Physical (Contains Unallocated Space)
MD5 Source Hash: d4f16508e6188da625855e62a2fd4ac2
SHA1 Source Hash: 0000000000000000000000000000000000000000
Image file Segment list:
SuspectFullHDD.E01
SuspectFullHDD.E02
SuspectFullHDD.E03
SuspectFullHDD.E04
SuspectFullHDD.E05
SuspectFullHDD.E06
```

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