YOUR MISSION: USE F-RESPONSE NOW WITH F-RESPONSE IMAGER FOR TARGETED COLLECTION OF A GEOGRAPHICALLY REMOTE MACHINE

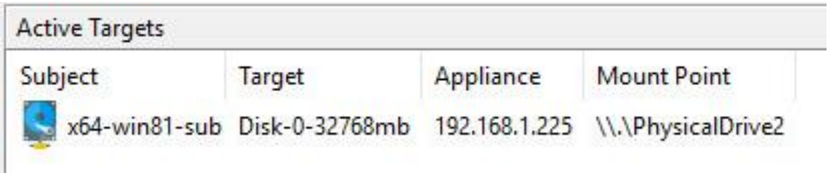
Often a collection will involve only specific files from a custodian and many times that custodian resides in another state or even another country. F-Response NOW is an on demand cloud service designed to provide write-protected access to remote custodian data virtually anywhere in the world.

This guide assumes:

1. *You have purchased a NOW instance in a region close to your subject or examiner machine for best performance, and followed the instructions received to setup your NOW software to connect to your subject machine.*
2. *You have F-Response Imager installed. F-Response Imager is a free tool designed for use with F-Response products. The latest version of F-Response Imager can be downloaded directly from our website.*

STEP 1: CONNECT TO THE DEVICE

You may see slightly better speed when connecting to the remote machine's physical hard drive if your target is a Windows machine. In the case of Apple or Linux subjects, use the DiscoveryShare option to review the data on your Windows examiner computer.

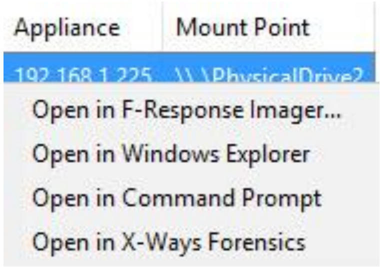


Active Targets

Subject	Target	Appliance	Mount Point
x64-win81-sub	Disk-0-32768mb	192.168.1.225	\\.\PhysicalDrive2

STEP 2: TRIAGE… SPECIFIC OR "EVERYTHING!"

While F-Response NOW and Imager products are designed to connect and collect as effectively as possible over an Internet connection, you are still subject to the ever varying speeds/routing of the Internet. While you can take steps to mitigate potential bottlenecks by working with a NOW instance in a region close to the subject and placing your examiner on a good network connection, what happens in between much beyond your influence.

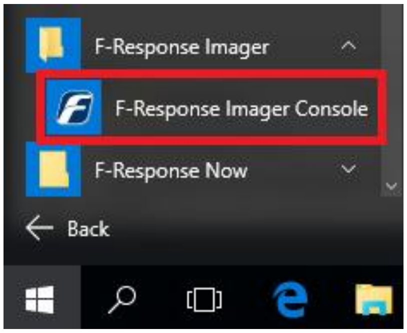


However you can exercise control over what data needs to be collected. If you right click on the mount point, you will see a list of options to review or image. Choose the option to Open in Windows Explorer to review.

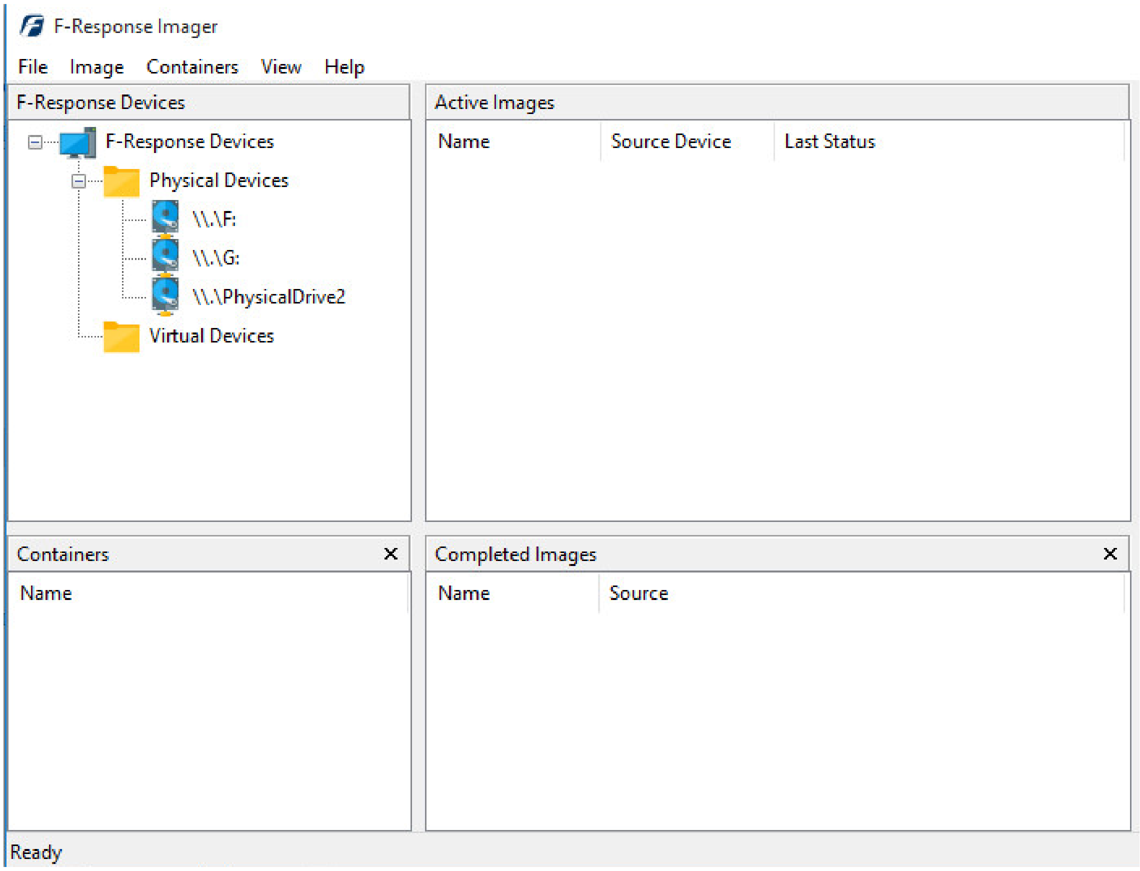
After a review of the remote machines files/folders, if you decide you can cull down the collection to a smaller size (recommended whenever possible), you can use the F-Response Imager tool to optimize your collection process. If you decide you still need "all the data", you can simply choose Open in F-Response Imager… to begin the collection process. However this guide will focus on targeted collection so let's continue…

STEP 3: START F-RESPONSE IMAGER

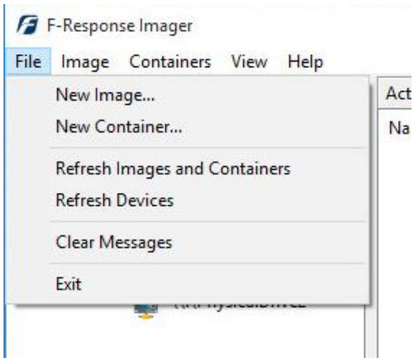
We'll begin the imaging process by opening the F-Response Imager Console:



The Imager will open with the default folder structure:



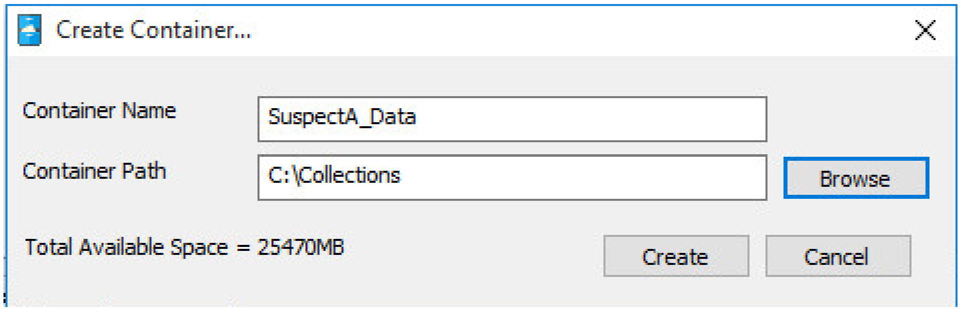
STEP 4: CREATE A CONTAINER



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. **Note: This does not have to be on your destination drive and depending on the size of your destination drive, you may choose to place the temporary container on the local hard drive of your examiner machine.**

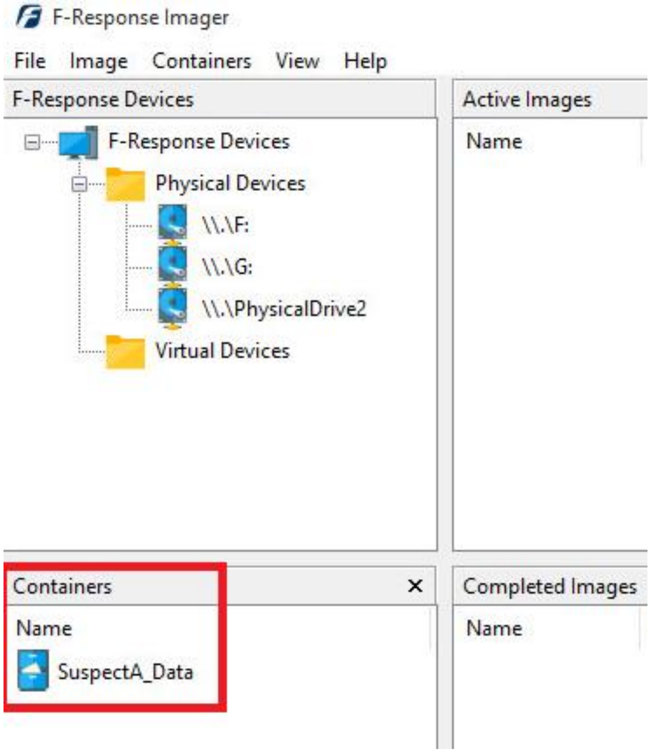


Container Name SuspectA_Data

Container Path C:\Collections

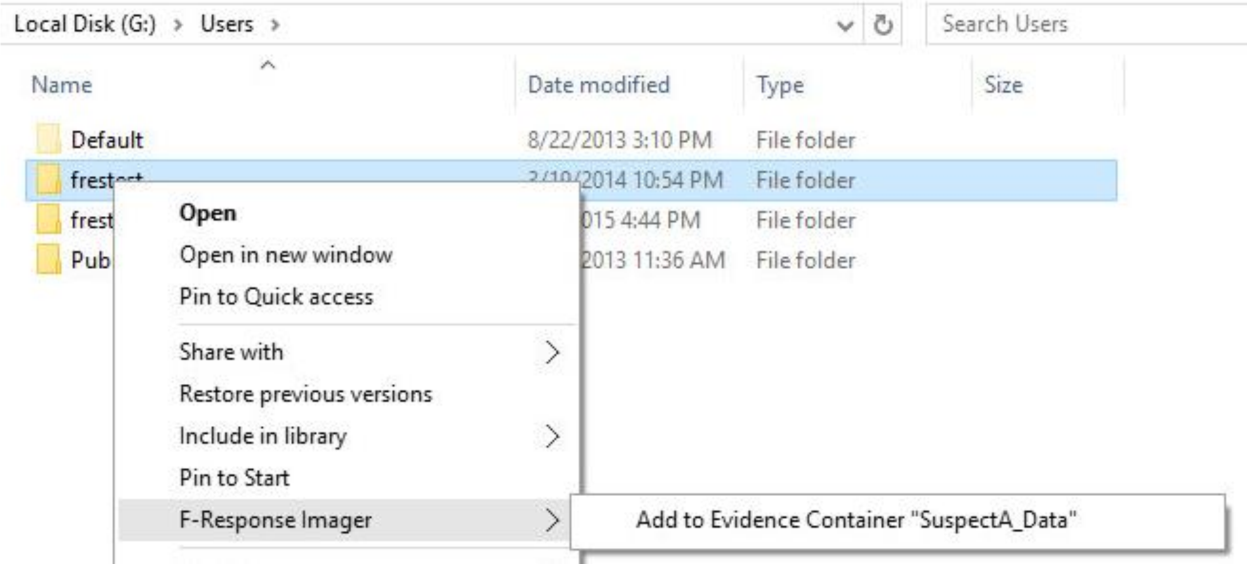
Total Available Space = 25470MB

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

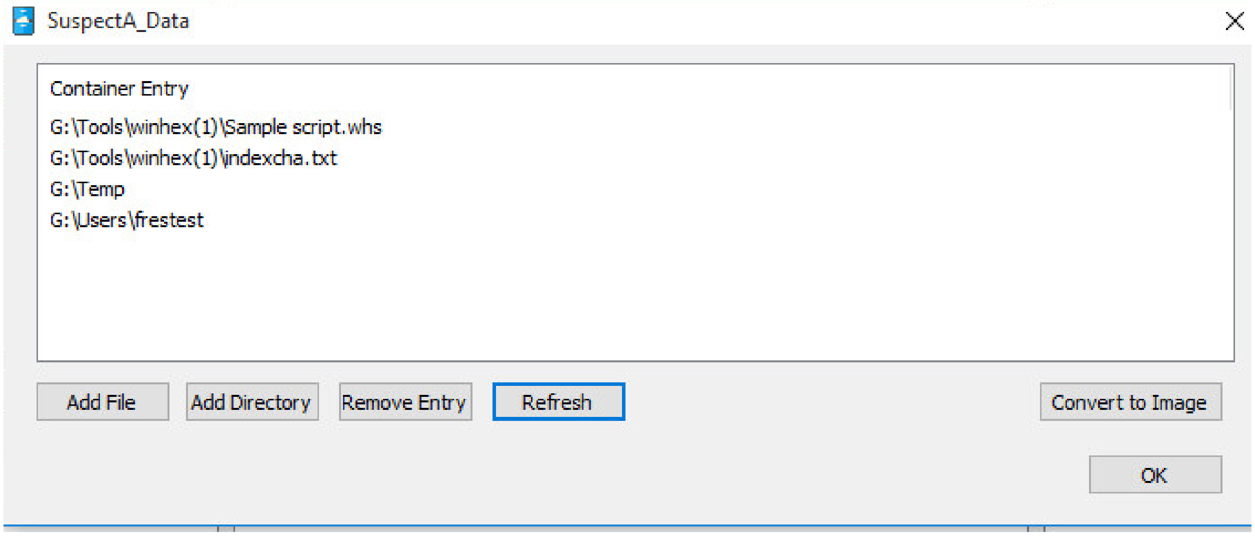


STEP 5: POPULATE THE CONTAINER

Now we are ready to add your targeted 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:



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:

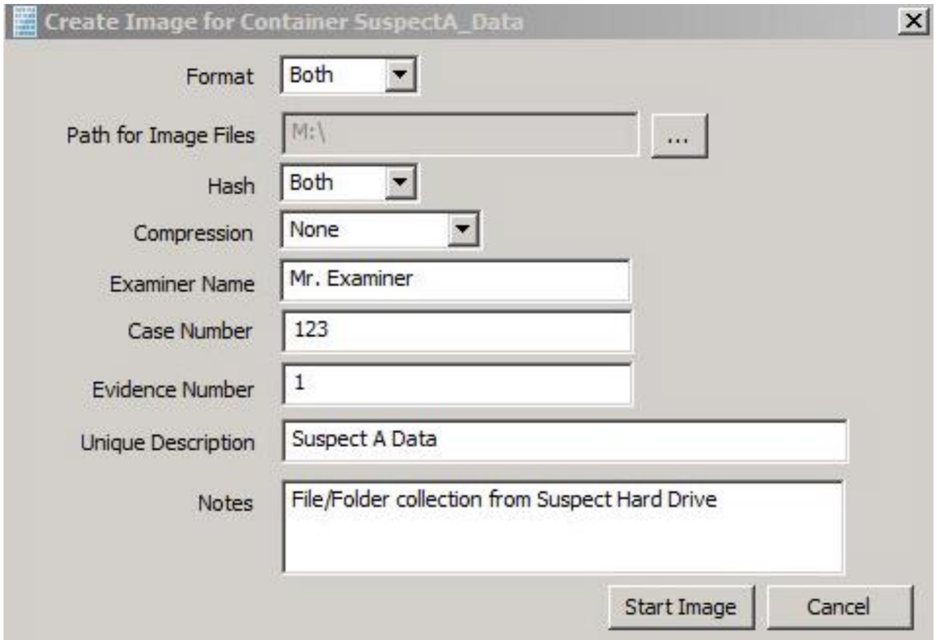


Container Entry
G:\Tools\winhex(1)\Sample script.whs
G:\Tools\winhex(1)\indexcha.txt
G:\Temp
G:\Users\frestest

Here you can adjust the files/folders you are about to image 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.

STEP 6: CONVERT TO AN IMAGE

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



Create Image for Container SuspectA_Data

Format: Both
Path for Image Files: M:\
Hash: Both
Compression: None
Examiner Name: Mr. Examiner
Case Number: 123
Evidence Number: 1
Unique Description: Suspect A Data
Notes: File/Folder collection from Suspect Hard Drive

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.

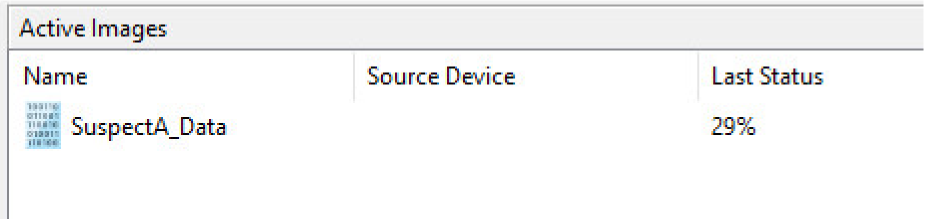
The **Path for Image Files** determines our destination drive—this must be a physical drive attached to our examiner machine (we cannot image to a network share).

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 7: REVIEW

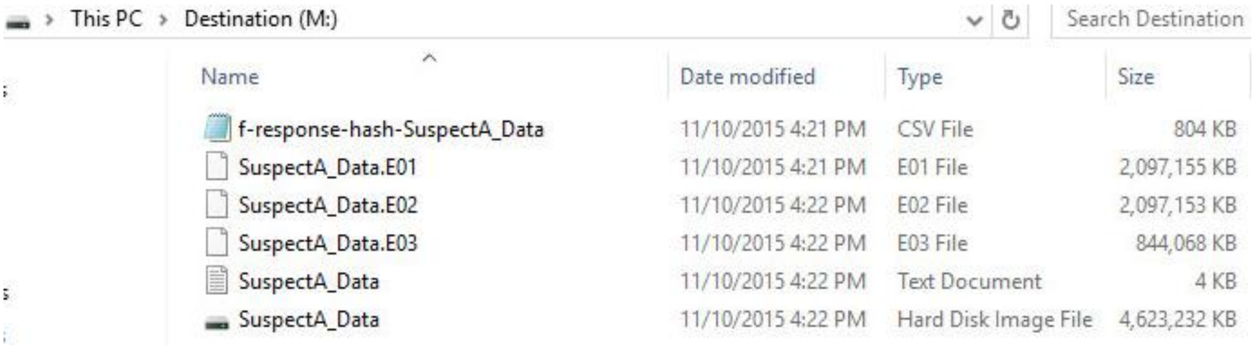
The details window will close and you can monitor the status of your image in Active Images pane of the console window. Again, the length of time to collect the data will depend on size, location, and the Internet itself.



Active Images

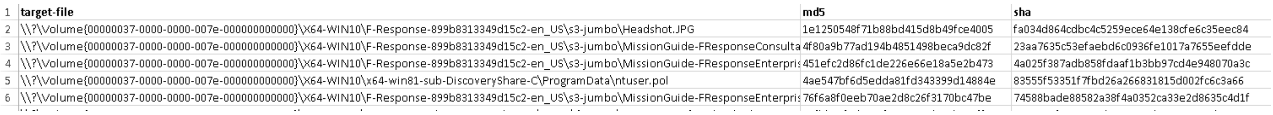
Name	Source Device	Last Status
SuspectA_Data		29%

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.



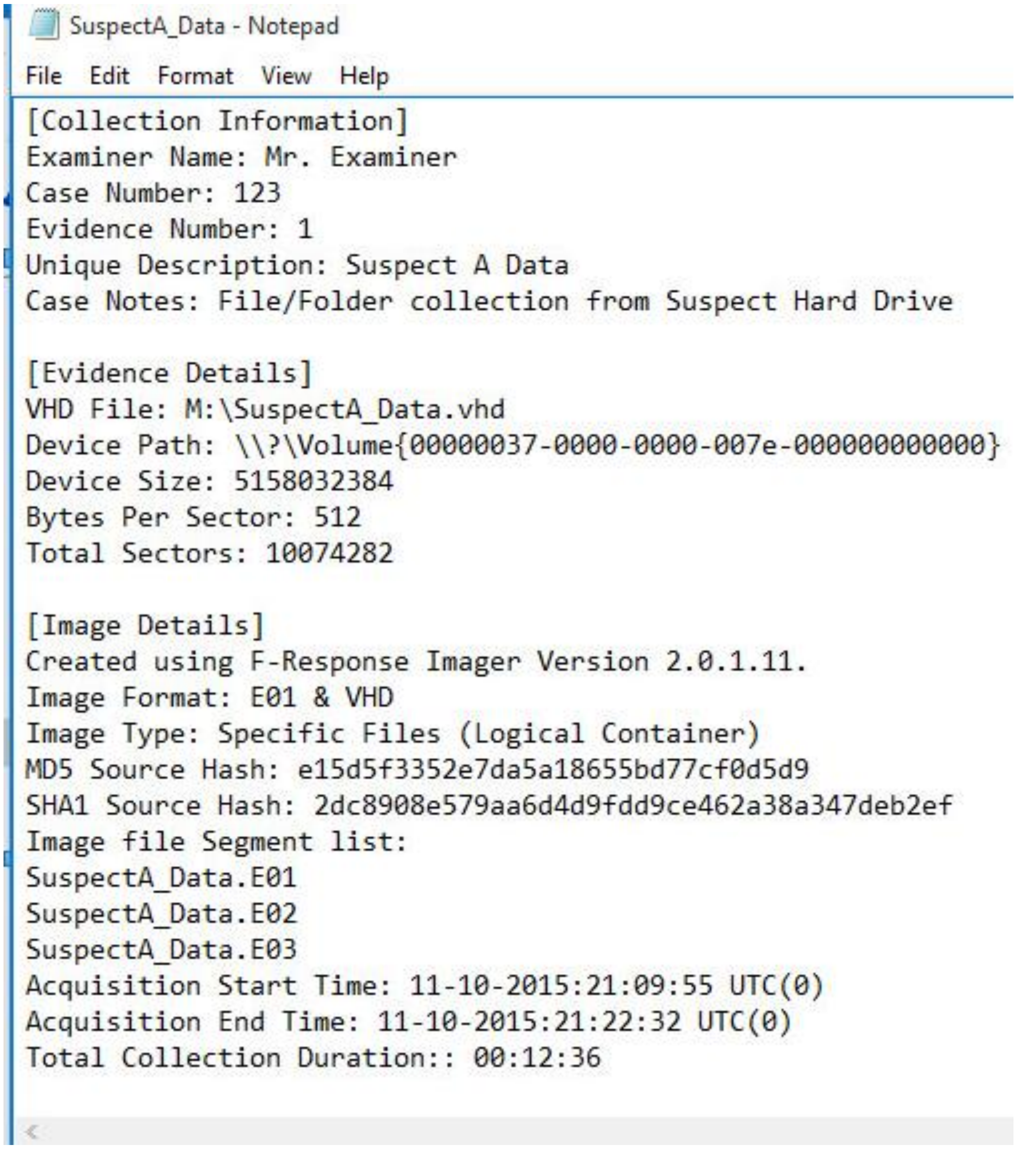
Name	Date modified	Type	Size
f-response-hash-SuspectA_Data	11/10/2015 4:21 PM	CSV File	804 KB
SuspectA_Data.E01	11/10/2015 4:21 PM	E01 File	2,097,155 KB
SuspectA_Data.E02	11/10/2015 4:22 PM	E02 File	2,097,153 KB
SuspectA_Data.E03	11/10/2015 4:22 PM	E03 File	844,068 KB
SuspectA_Data	11/10/2015 4:22 PM	Text Document	4 KB
SuspectA_Data	11/10/2015 4:22 PM	Hard Disk Image File	4,623,232 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-000000000000}\X64-WIN10\F-Response-899b8313349d15c2-en_US\s3-jumbo\Headshot.JPG	1e1250548f71b88bd415d8b49fce4005	fa034d864cdbc4c5259ece64e138cfe6c35eec84
3	\\?\Volume{00000037-0000-0000-007e-000000000000}\X64-WIN10\F-Response-899b8313349d15c2-en_US\s3-jumbo\MissionGuide-FResponseConsulta	4f80a9b77ad194b4851498beca9dc82f	23aa7635c53efaebd6c0936fe1017a7655eefdde
4	\\?\Volume{00000037-0000-0000-007e-000000000000}\X64-WIN10\F-Response-899b8313349d15c2-en_US\s3-jumbo\MissionGuide-FResponseEnterpris	451efc2d86fc1de226e66e18a5e2b473	4a025f387adb858fdaaf1b3bb97cd4e948070a3c
5	\\?\Volume{00000037-0000-0000-007e-000000000000}\X64-WIN10\x64-win81-sub-DiscoveryShare-C\ProgramData\ntuser.pol	4ae547bf6d5edda81fd343399d14884e	83555f53351f7fbd26a266831815d002fc6c3a66
6	\\?\Volume{00000037-0000-0000-007e-000000000000}\X64-WIN10\F-Response-899b8313349d15c2-en_US\s3-jumbo\MissionGuide-FResponseEnterpris	76f6a8f0eeb70ae2d8c26f3170bc47be	74588bade88582a38f4a0352ca33e2d8635c4d1f

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: 1
Unique Description: Suspect A Data
Case Notes: File/Folder collection from Suspect Hard Drive

[Evidence Details]
VHD File: M:\SuspectA_Data.vhd
Device Path: \\?\Volume{00000037-0000-0000-007e-000000000000}
Device Size: 5158032384
Bytes Per Sector: 512
Total Sectors: 10074282

[Image Details]
Created using F-Response Imager Version 2.0.1.11.
Image Format: E01 & VHD
Image Type: Specific Files (Logical Container)
MD5 Source Hash: e15d5f3352e7da5a18655bd77cf0d5d9
SHA1 Source Hash: 2dc8908e579aa6d4d9fdd9ce462a38a347deb2ef
Image file Segment list:
SuspectA_Data.E01
SuspectA_Data.E02
SuspectA_Data.E03
Acquisition Start Time: 11-10-2015:21:09:55 UTC(0)
Acquisition End Time: 11-10-2015:21:22:32 UTC(0)
Total Collection Duration:: 00:12:36
```

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.