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

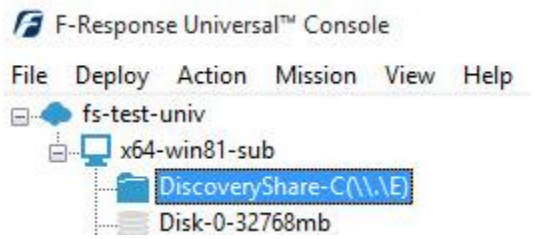
YOUR MISSION: USE THE F-RESPONSE IMAGER TO COLLECT INDIVIDUAL FILES/FOLDERS TO A CONTAINER

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)

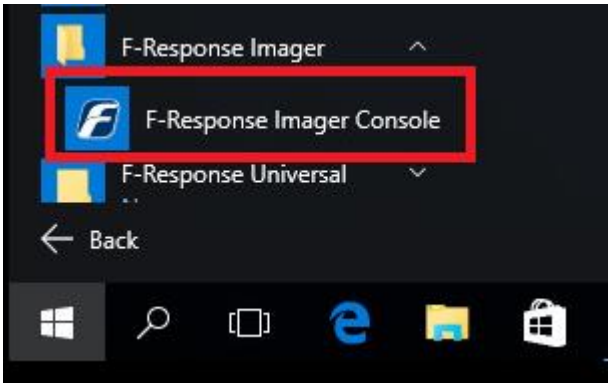
Take note of the volume letter assigned for the F-Response attached target. In this example, here we have a virtual device attached using F-Response Universal, specifically a DiscoveryShare™ from a Windows subject.



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.

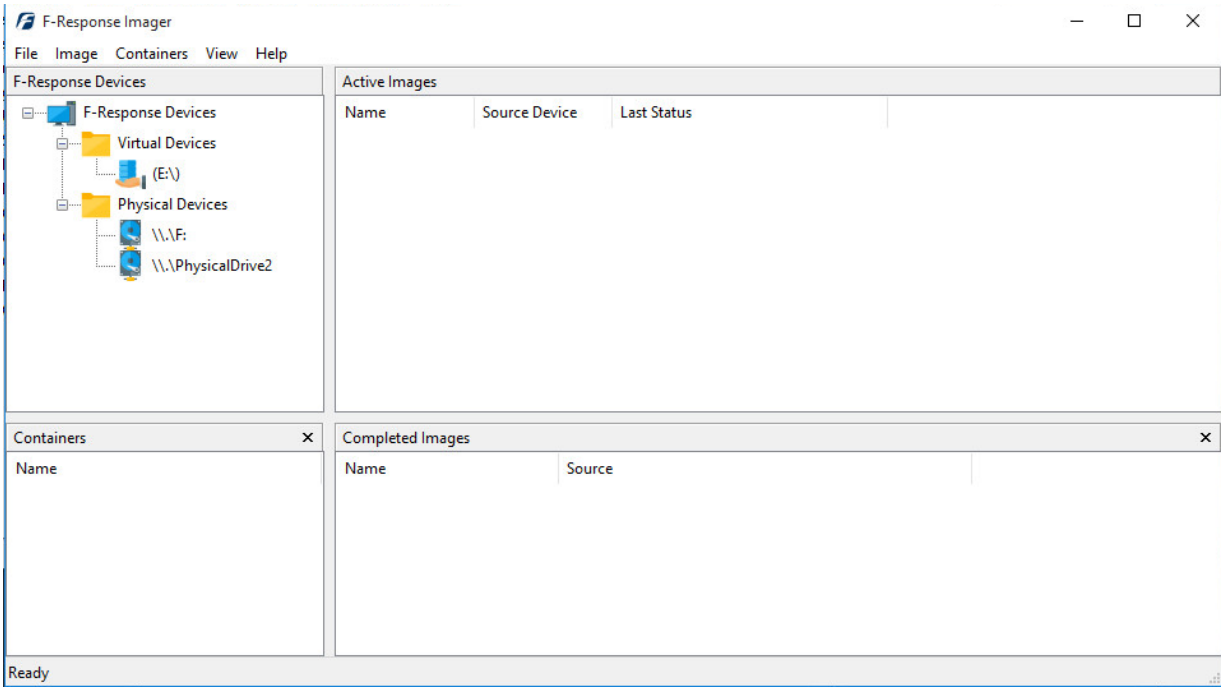
STEP 2: START THE F-RESPONSE IMAGER CONSOLE

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



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

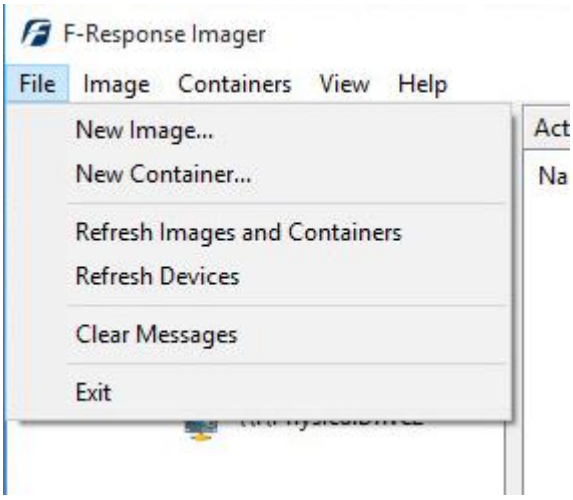
The Imager will open with the default folder structure:



STEP 3: CREATE A CONTAINER

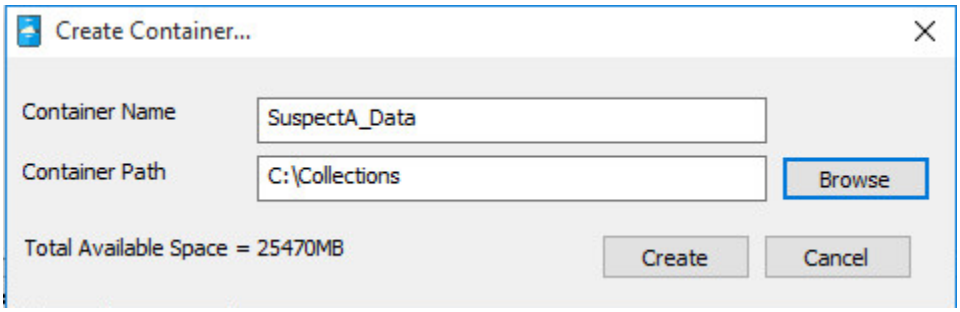
So, we need to create a container for our files of interest. A container is just as it sounds—a holding place for the list of files and folders we intend to collect. Remember that files and folders in the container are not preserved until the container is converted to an image.

To create a container, go to **File – New Container…**

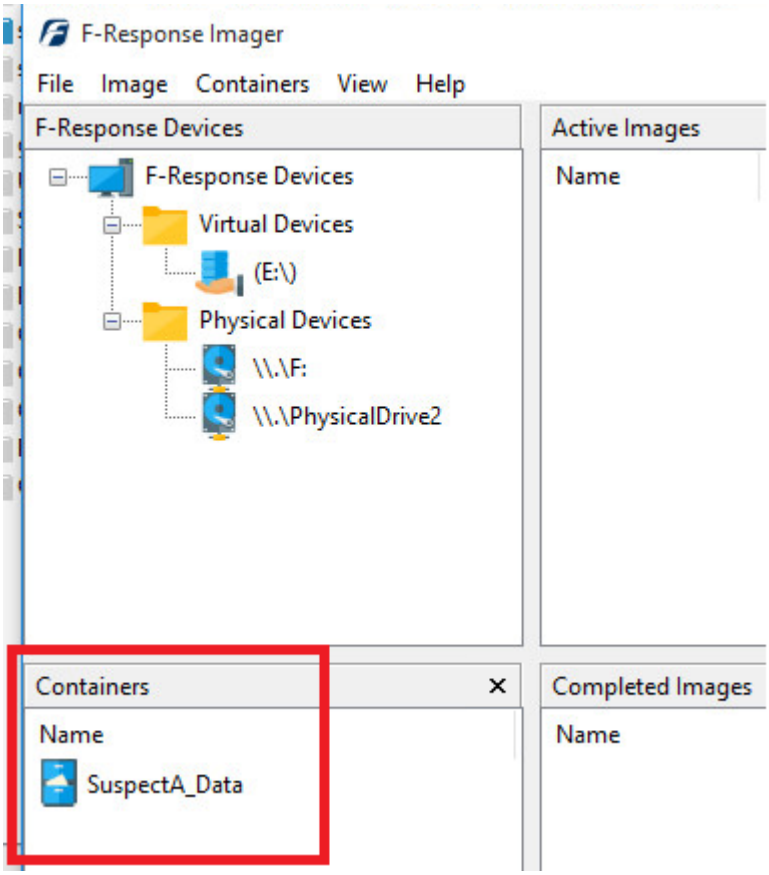


Email:support@f-response.com
Website:www.f-response.com
Phone: 1-800-317-5497

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



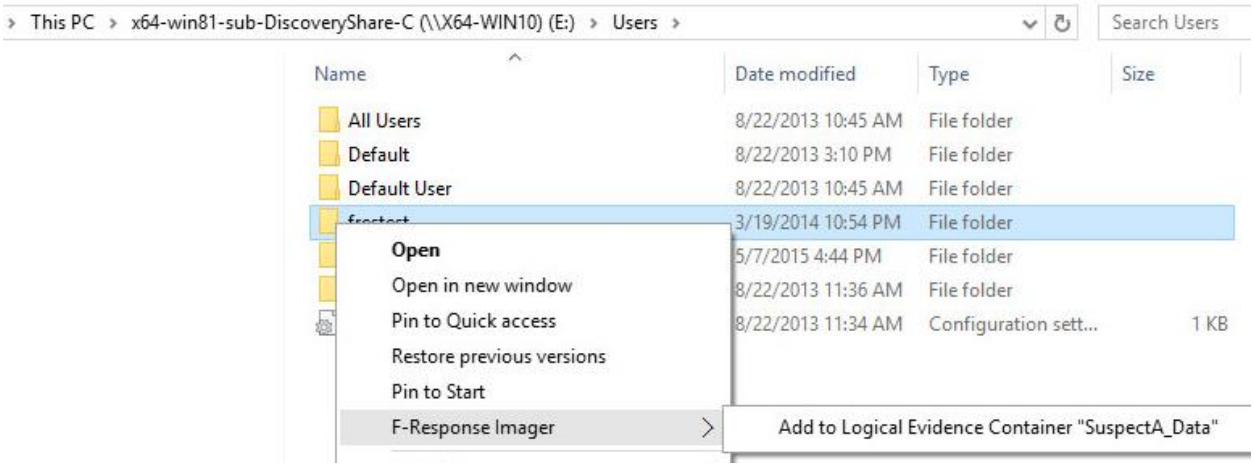
Click the Create button and you will find your new container in the Containers pane in the console window:



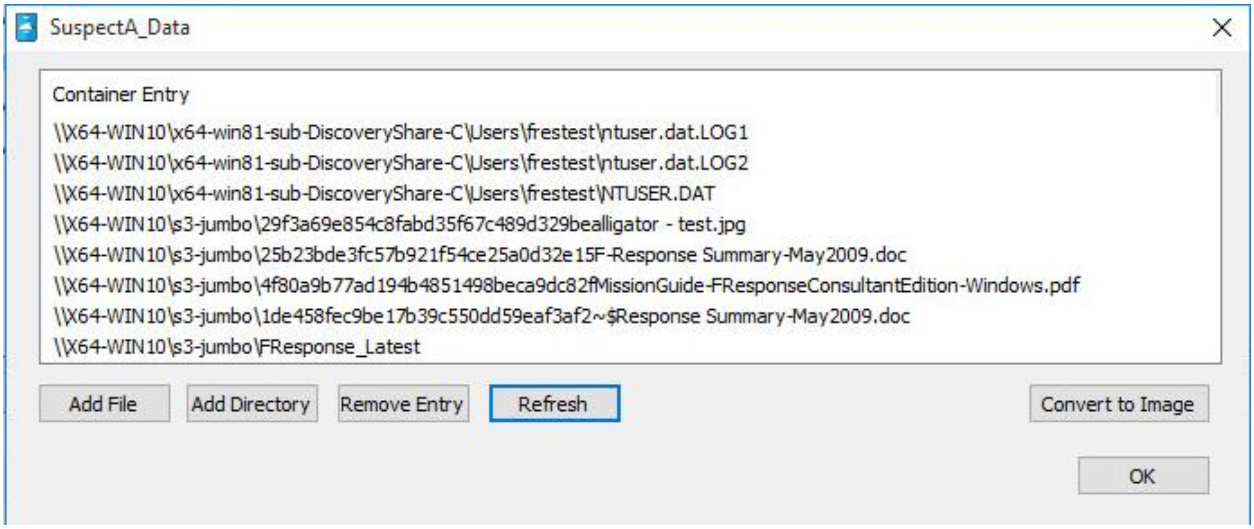
Email:support@f-response.com
Website:www.f-response.com
Phone: 1-800-317-5497

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:



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:

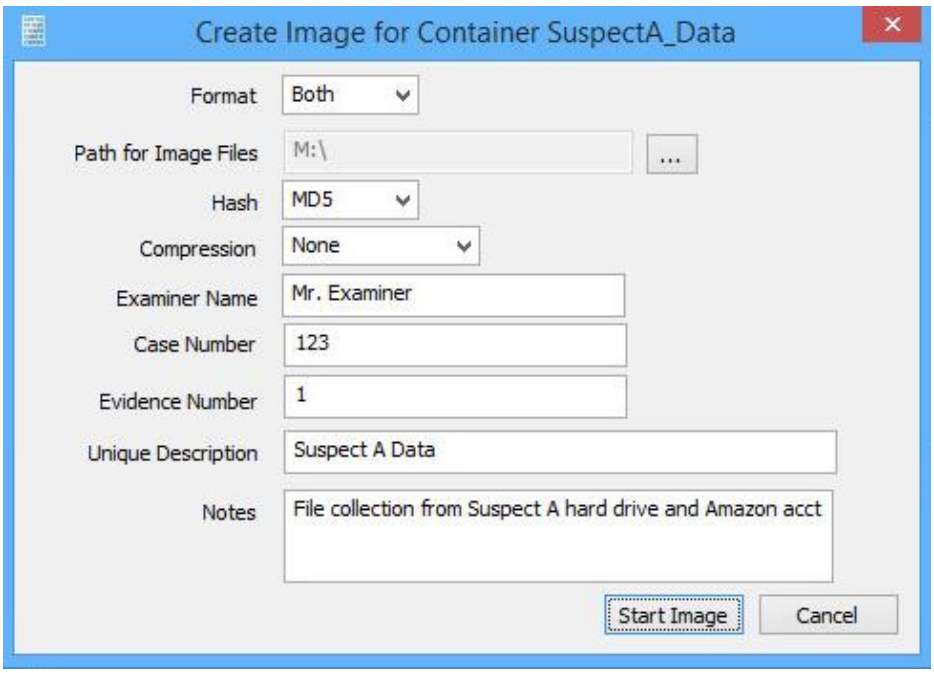


Here you can adjust the files/folders you are about to image from the various resources by adding or removing accordingly. Click **Refresh** to give it a final review and when you are happy with the results click the **Convert to Image** button.

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

STEP 5: CONVERT TO AN IMAGE

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



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.

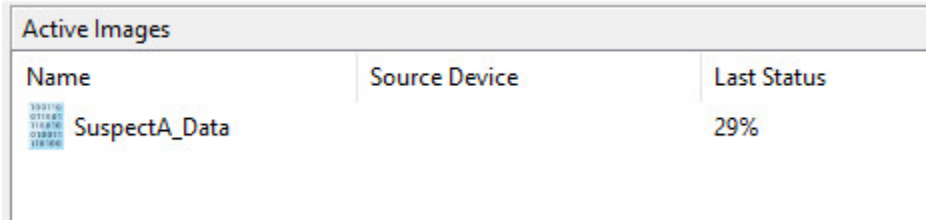
The **Path for Image Files** determines our destination drive—this must be a physical drive attached to our examiner machine (we cannot image to a network share).

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.

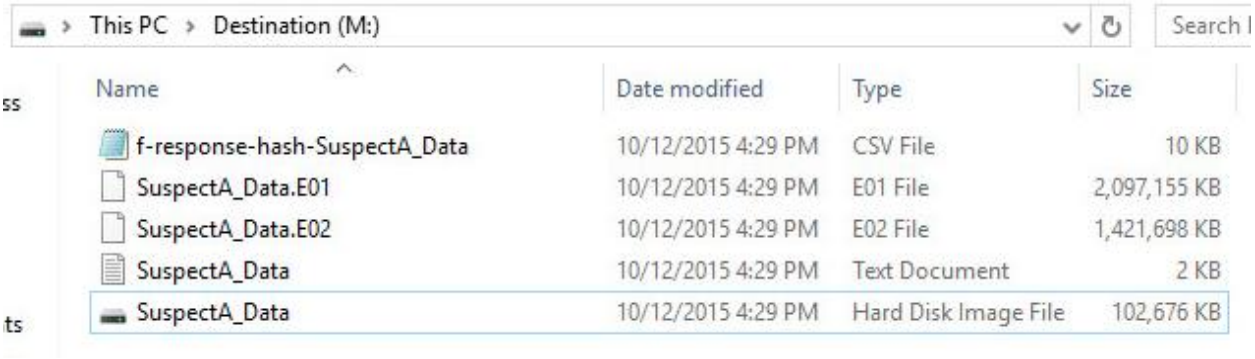
STEP 6: REVIEW

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



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.

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

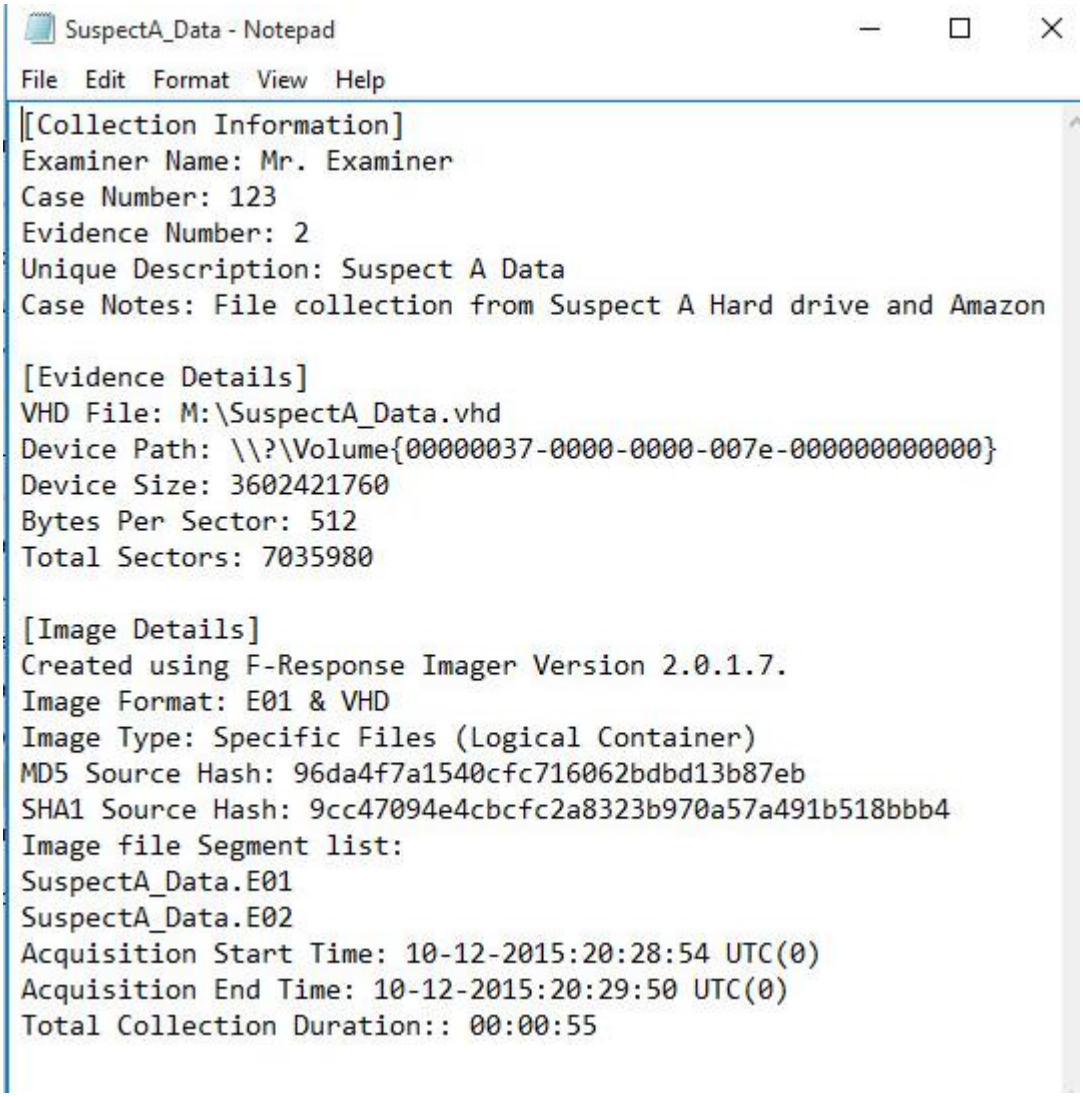


Here you will find your image files, a CSV listing of the collected files with their corresponding hashes, and text file report.

	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-FResponseEnterpri	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-FResponseEnterpri	76f6a8f0eeb70ae2d8c26f3170bc47be	74588bade88582a38f4a0352ca33e2d8635c4d1f

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

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



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.