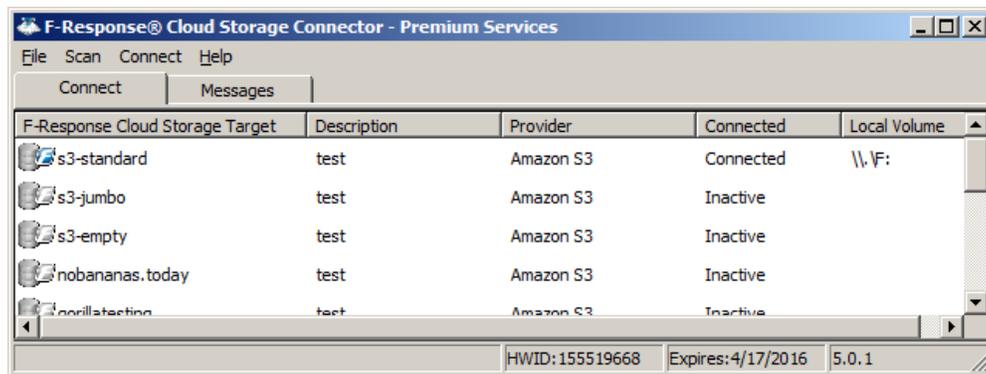


Your Mission: Use the F-Response Cloud Connector , Robocopy, and Virtual Hard Disk(s) to create simple read-only cloud evidence collections

Note: This guide assumes you have started the F-Response Cloud Connector (FCLDC), and are using a version of Windows that supports creating and attaching VHD(Windows 7+). For more information, please reference the F-Response User Manual.

Step 1: Connect to the Cloud Storage container

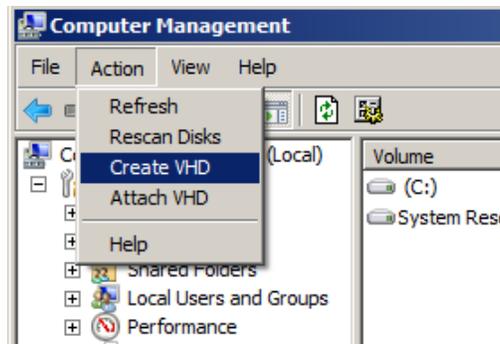
This guide assumes you have already connected to one of more Cloud Storage containers using the F-Response Cloud Connector. Should you have questions on how to do that, please refer to the F-Response Cloud Connector Mission Guide specific to the cloud environment you are looking to access, or the F-Response User Manual.



F-Response Cloud Connector attached to an Amazon S3 Bucket

Step 2: Create a VHD and attach it to your Examiner machine

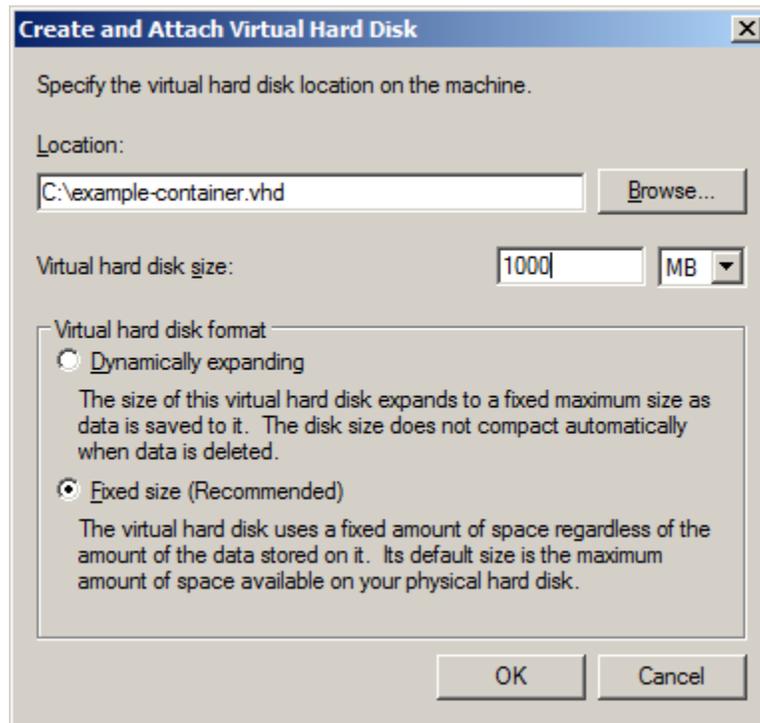
In order to collect the contents of the newly attached F:\ drive we must create a Virtual Hard Disk using the Computer Management snap-in available in Control Panel -> Administrative Tools. Once the Computer Management snap is open you will find Create VHD¹ in the Action Menu.



¹ VHD or Virtual Hard Disk is a file format which represents a virtual hard disk drive. (http://en.wikipedia.org/wiki/VHD_%28file_format%29)

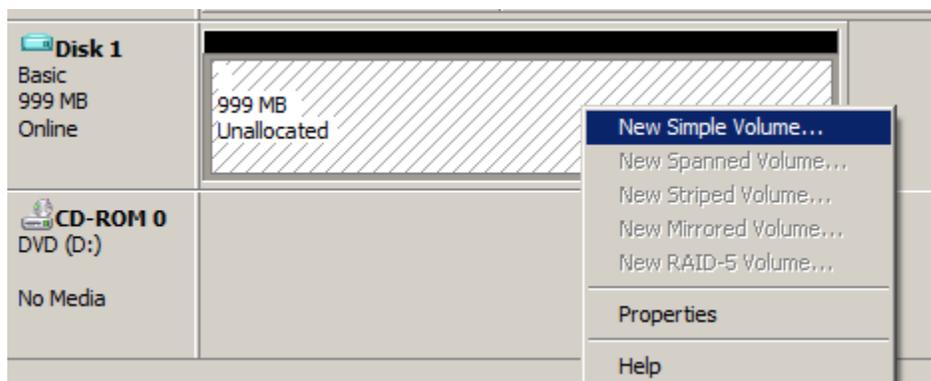
Create a new Virtual Hard Disk (VHD)

The first step in creating a VHD is selecting a location to store the VHD file and selecting either a dynamic or static VHD. In this example we chose a static VHD due to limited resources in our virtual machine.

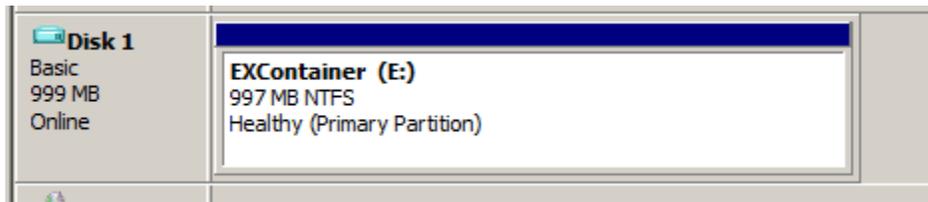


Creating a VHD

Once a VHD is created it must be Initialized using the context menu, then a new Simple Volume must be applied to the VHD.



Applying a new simple volume to the VHD



After the volume has been created the VHD is mounted and available for use.

Step 3: Install Microsoft Robocopy

Skip this step if you already have Microsoft Robocopy installed. However, if not, it is available as part of the Microsoft Windows Server 2003 Resource Kit. You will want to download and install this resource kit from the following link.

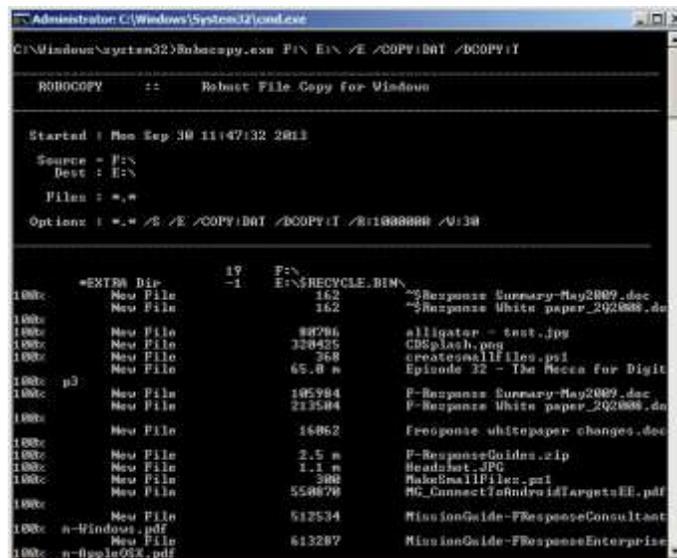
<http://www.microsoft.com/downloads/details.aspx?familyid=9d467a69-57ff-4ae7-96ee-b18c4790cfd&displaylang=en>

Step 4: Use Robocopy to duplicate the contents of the Cloud Connector share

Robocopy is a reasonably straight forward command line copy tool, but, it does possess a very large number of potential flag options. We have included a number of those options below, however this document should not be considered a replacement for any Robocopy usage guidelines presented elsewhere.

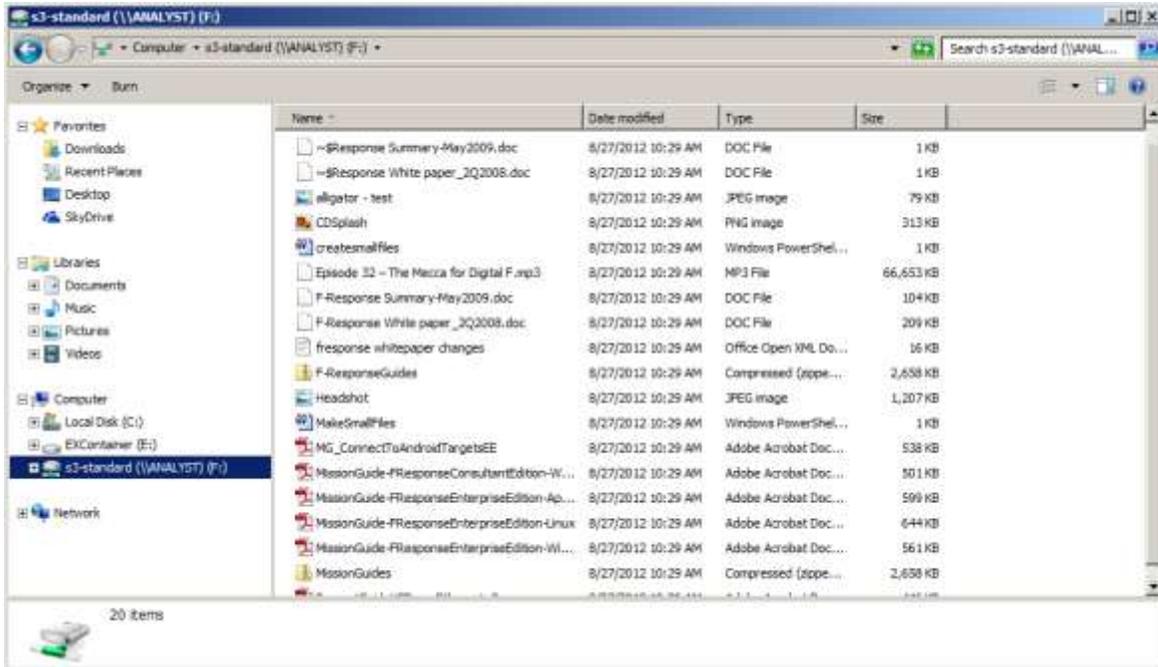
In order to instruct Robocopy to perform a simple copy of the data presented by the Cloud Connector, and preserve any file/folder metadata the following command was used.

Robocopy.exe F:\ E:\ /E /COPY:DAT /DCOPY:T

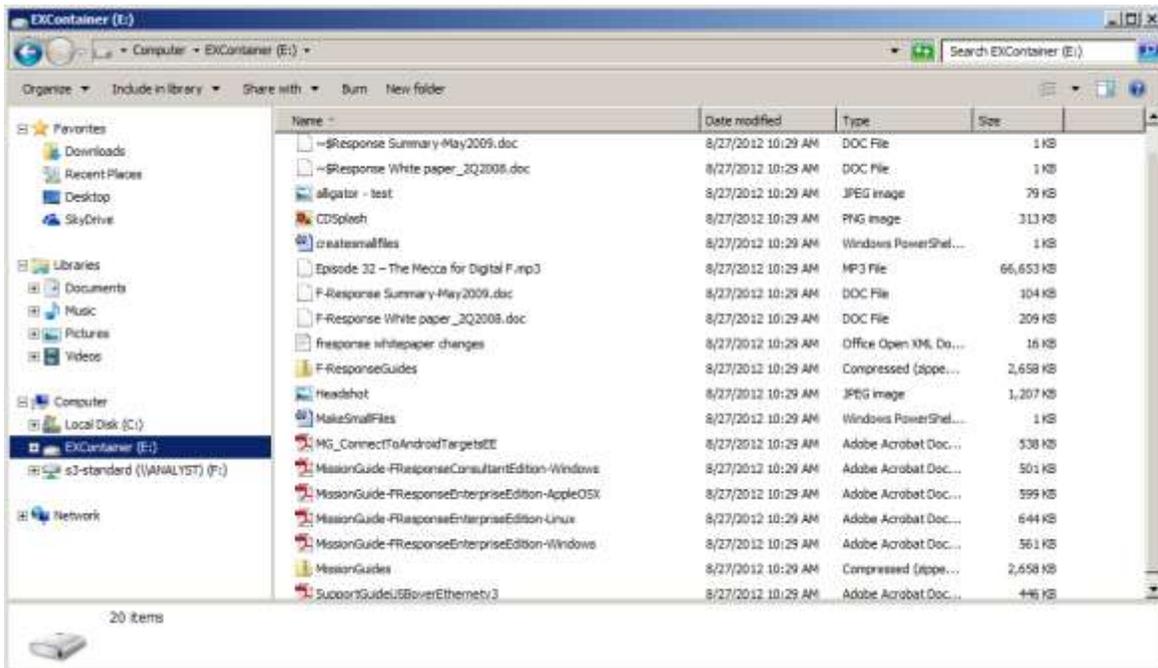


Using Robocopy with basic commands to duplicate the data in the Cloud Connected Volume

Once complete we can verify the resulting data visually by reviewing the source share and destination VHD.



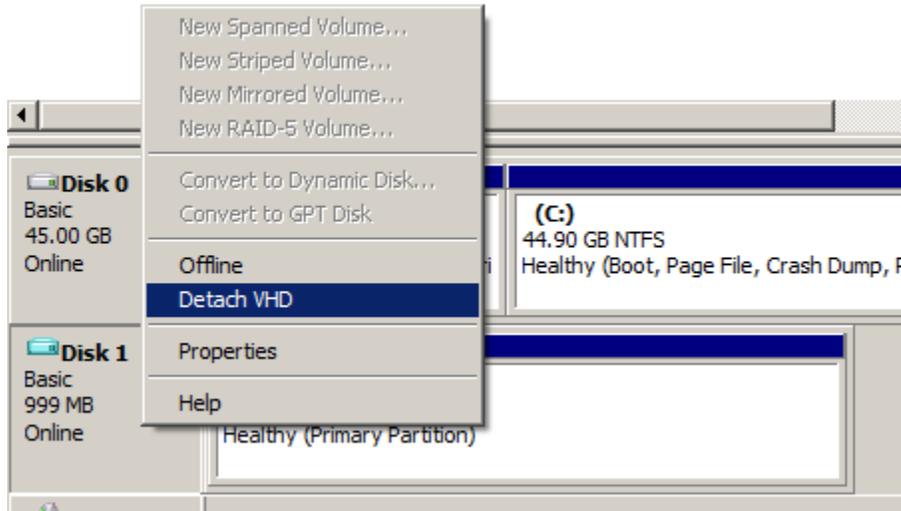
Amazon S3 hosted storage data presented by the F-Response Cloud Connector



VHD containing preserved content from the Cloud Connector share

Step 5: Detach the newly minted VHD and optionally re-attach it read-only

Once the data has been copied to the VHD it can be detached using the Computer Management snap-in (Control Panel->Administrative Tools->Computer Management). Simply select the VHD and right click on it, in the resulting context menu select “Detach VHD”.

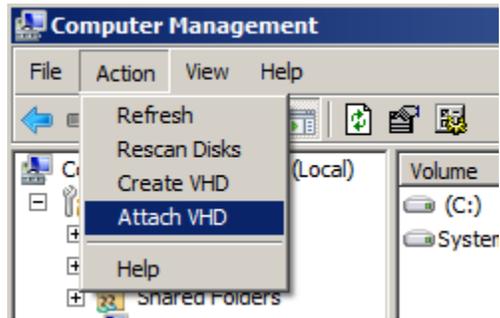


Detach VHD is available in the VHD's context menu



Be sure to not check the “Delete the virtual hard disk file..” option when detaching the VHD

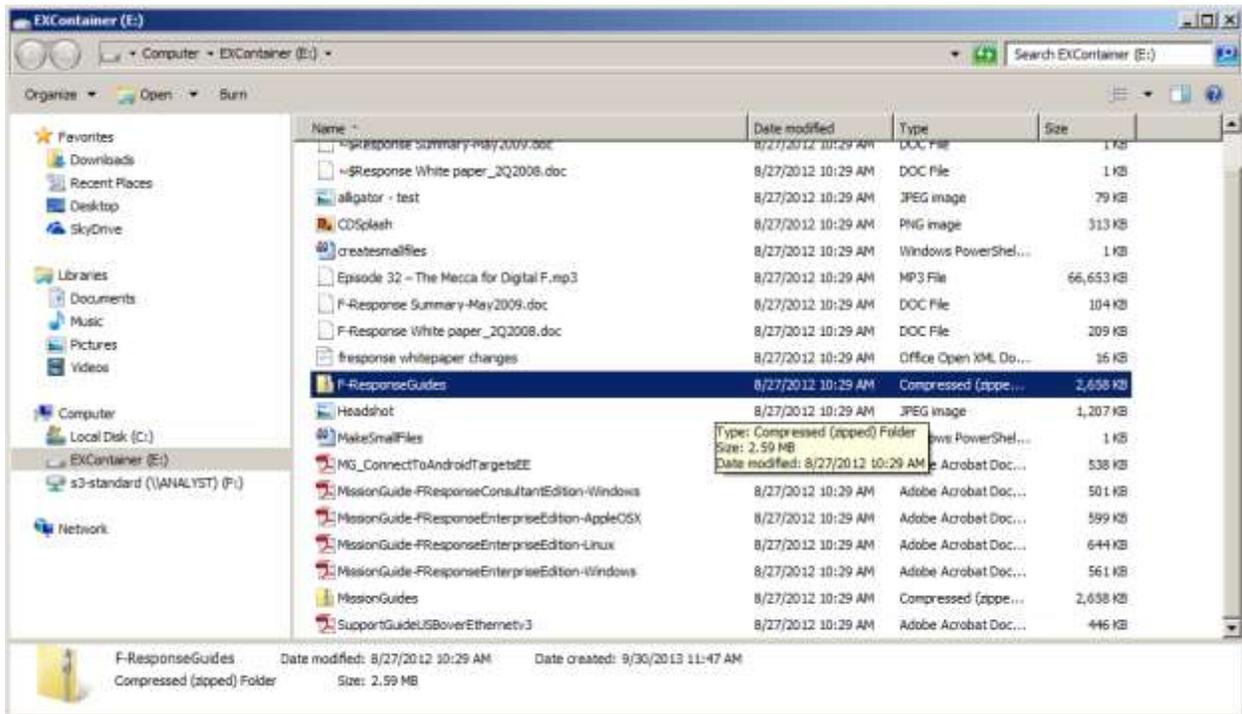
Once detached a VHD can be reattached to any Windows 7+ system, furthermore it can be re-attached read-only, allowing additional review via other tools without concern for potential modification.



Computer Management Action Menu, Attach VHD



Be sure to check the "Read-only" option when attaching the VHD



Review the new attached VHD content using any forensic or e-discovery tools.