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 Storage C	onnector - Premium Se	ervices		_ 🗆 🗵
<u>F</u> ile Scan Conne	ct <u>H</u> elp				
Connect	Messages	1			1
F-Response Cloud S	Storage Target	Description	Provider	Connected	Local Volume 🔺
🔯 s3-standard		test	Amazon S3	Connected	\\.V=:
s3-jumbo		test	Amazon S3	Inactive	
s3-empty		test	Amazon S3	Inactive	
nobananas.tod	lay	test	Amazon S3	Inactive	
Coorillatesting ▲		tart	Amazon \$3	Inactive	▼
			HWID:155519668	Expires: 4/17/2016	5.0.1

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.

Create and Attach Virtual Hard Disk	×
Specify the virtual hard disk location on the machine.	
Location:	
C:\example-container.vhd Browse	
Virtual hard disk size: 1000 MB	•
Virtual hard disk format O Dynamically expanding	
The size of this virtual hard disk expands to a fixed maximum size as data is saved to it. The disk size does not compact automatically when data is deleted.	
• <u>Fixed size (Recommended)</u>	
The virtual hard disk uses a fixed amount of space regardless of the amount of the data stored on it. Its default size is the maximum amount of space available on your physical hard disk.	
OK Cancel	

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-4ae7-96eeb18c4790cffd&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

-Ad	ninistr	ator	: C:W	windows's	SystemUtion	ulexe			1×
CINU	ndeu	ii 🗤	yzta	m32)Ba	becopy.ext	FIN EIN	/E /COP	VIDAT /DCOPVIT	-
ROBOCOPY :: Robust File Copy for Vindous									
Sta	urted		Nee	Sep 30	11+47+32	2813			
50	Dest		11						
1	liles								
Opt	ionz			NR NE	/COPY DAT	/\$C0P¥+T	/R11998	888 ×V138	
1001<		EXT	RA I Nou Nou	Dir Pile File	19 -1	F:\ E:\\$RECY 162 162	LE.BIN	"SResponse Connery-May2009.doc "SResponse Unite paper_202008.d	
1005 1005 1005×		5.200 S		File File File File		88296 328425 368 65.8 m		alligator — test.jpy CDSplach.ong ceratesmellfiles.psi Episode 32 - The Mecca for Digi	
1000	h3.	4	Neu	Pile Pile		195984 213584		P-Response Sunnary-May2009.doc P-Response White paper_202000.do	
1.689		1	New	File.		16862		Freeponse uhttepaper changes.de-	
100x 100x 100x 100x			Neu Neu Neu	File File File File		2.5 m 1.1 m 388 558878		P-ResponseGuides.zip Hoadshot.JPG MakeSmallFiles.ps1 MG_ConnectToRndyoidTaegetsEE.pd	
1980			Neu	File		512534		MissionGalde-FResponseConsultan	
198<	n-H	ind ppl	eus. Neu e093	.µdf File €.pdf		613287		MissionGaide-FRespecseEnterpris	

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.

ingenier 🕶 Durn					a • 🖬 🛙
👷 Pavorites	Nome +	Date modified	Type	Size	
Downloads	Skesponse Summery-May2009.doc	8/27/2012 10:29 AM	DOC File	1 KB	
3 Recent Places	-\$Response White paper_2Q2008.doc	B/27/2012 10:29 AM	DOC File	1KB	
Cesktop	🔛 eligator - test	8/27/2012 10:29 AM	JPEG mage	79 KB	
Ka SkyDrive	CDSplash	8/27/2012 10:29 AM	PNG mage	313 KB	
	Createsnalfiles	8/27/2012 10:29 AM	Windows PowerShel	188	
ubraries	Episode 32 - The Merca for Digital F.mp3	B/27/2012 10:29 AM	MP3 File	66,653 KB	
Documents	F-Response Summary-May2009.doc	8/27/2012 10:29 AM	DOCIFILE	104KB	
Musc	F-Response White paper _202008.doc	B/27/2012 10:29 AM	DOC File	209 KB	
Pictures	fresponse whitepaper changes	8/27/2012 10:29 AM	Office Open XML Do	16 KB	
a vicio	F-ResponseGuides	8/27/2012 10:29 AM	Compressed (zope	2,658 KB	
Computer	= Headshot	8/27/2012 10:29 AM	JPEG image	1,207 KB	
Local Disk (C1)	42] MakeSmallPiles	8/27/2012 10:29 AM	Windows PowerShel	1158	
EXContainer (E:)	MG_ConnectToAndroidTargetsEE	8/27/2012 10:29 AM	Adobe Acrobat Doc	538 KB	
🚍 is3-standard (\\ANALYST) (Fr)	MassonGude-PResponseConsultantEdition-W	6/27/2012 10:29 AM	Adobe Acrobat Doc	501 KB	
	MasionGuide -FResponseEnterpriseEdition-Ap	8/27/2012 10:29 AM	Adobe Acrobat Doc	599 KB	
🐺 Network	MissionGuide-FResponseEnterpriseEdition-Linux	8/27/2012 10:29 AM	Adobe Acrobat Doc	64430	
	MasionQuide -FRasponseEnterpriseEdition-Wi	B/27/2012 10:29 AM	Adobe Acrohat Doc	561.KB	
	MassonGuides	B/27/2012 10:29 AM	Compressed (sppe	2.658 KB	
		A.M.M.M. 10, 10, 101	+11 + 1.14	A 40 100	

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

Computer + EXConta	ner (El) +		* (23) Se	arch EXContainer (E)	2
Organize = Include in library = S	hare with Burn New folder			() ()	- 11 0
-	Norre =	Date modified	Type	See	
a Downloads	-\$Response Summary May2009.doc	8/27/2012 10:29 AM	DOC File	148	
Sill Recent Places	-SResponse White paper_202008.doc	8/27/2012 10:29 AM	DOC Nie	3 KB	
E Desktop	🔜 aligator - test	8/27/2012 10:29 AM	JPEG image	79 KB	
SkyDrive	Sector CDSpleet	8/27/2012 10:29 AM	PNG image	313 K8	
	(42) createsmalifies	8/27/2012 10:29 AM	Windows PowerShel	1KB	
Libraries	Episode 32 - The Mecca for Digital F.mp3	8/27/2012 10:29 AM	MP3 File	66,653 KB	
Documents	F-Response Summary-May2009.doc	8/27/2012 10:29 AM	DOC File	304 KB	
🗄 🌒 Music	F-Response White paper_302008.doc	8/27/2012 10:29 AM	DOC File	209 KB	
Pictures	fresponse whitepaper changes	8/27/2012 10:29 AM	Office Open XML Do	16 KB	
III. 📷 Videos	I F-ResponseGuides	8/27/2012 10:29 AM	Compressed (zppe	2,658 KB	
	C Headshot	8/27/2012 10:29 AM	JPEG image	1,207 KB	
Computer	di) MakeSmalFiles	8/27/2012 10:29 AM	Windows PowerShel	11/3	
Den ElCantaner (El)	MG_ConnectFoAndroidTargetsEE	8/27/2012 10:29 AM	Adabe Acrobat Doc	538 KB	
H === s3-standard (VANALYST) (Fr)	MasonGuide FResponseConsultantEdition-Windows	8/27/2012 10:29 AM	Adobe Acrobat Doc	501 KB	
	MassonGuide-FResponseEnterpriseEdition-Apple/05X	8/27/2012 10:29 AM	Adobe Acrobat Ooc	599 KB	
Stetwork	MasionQuide -FRasponseEnterpriseEdition-Linux	8/27/2012 10:29 AM	Adobe Acrobat Doc	644 KB	
NATION IN CONTRACTOR	MissionGuide #ResponseEnterpriseEdition-Windows	8/27/2012 10:29 AM	Adobe Acrobat Doc.	561 KB	
	MexicorGuides	8/27/2012 10:29 AM	Compressed Grope	2,658 KB	
	SupportSudeLEBoverEthemetv3	8/27/2012 10:29 AM	Adobe Acrobat Dec	446 KB	
20 items	A CONTRACTOR OF			0.00	

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".

<u> ا ا ا ا ا ا ا ا ا ا ا ا ا ا ا ا ا ا ا</u>	New Spanned Volume New Striped Volume New Mirrored Volume New RAID-5 Volume	
Disk 0 Basic	Convert to Dynamic Disk Convert to GPT Disk	(C:)
Online	Offline Detach VHD	i Healthy (Boot, Page File, Crash Dump, P
Disk 1	Properties	
999 MB Online	Help Healthy (Primary Partition)	

Detach VHD is available in the VHD's context menu

Detach Virtual Hard Disk
Detaching a virtual hard disk will make it unavailable until it is attached again. Virtual hard disk file location:
C:\example-container.vhd
Delete the virtual hard disk file after removing the disk.
Deleting the virtual hard disk file will cause all data stored on disk to be permanently lost.
OK Cancel

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.







Attach Virtual Hard Disk	×
Specify the virtual hard disk location on the computer.	
Location:	
C:\example-container.vhd	Browse
Read-only.	
ОК	Cancel

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

Computer • ExContain	er (tt.) •		• (3) 54	nch EXContainer (E:)	
rganize + 🏹 Open + Burn)册 •	
Pevantes Downloads Recent Places Desktop Storbure	Name * Summary way 2009.doc Sefeesponse White paper_202008.doc Sefeesponse White paper_202008.doc Sefeesponse White paper_202008.doc	Date modified 8/27/2012 10:29 AM 8/27/2012 10:29 AM 8/27/2012 10:29 AM 8/27/2012 10:29 AM 8/27/2012 10:29 AM	Type DOC File JPEG mage PNG mage	5/28 1 KB 79 KB 313 KB	
Ubraries Documents Music Pictures Videos	Createsmalifies Episode 32 – The Mesca for Digital F.rep3 F-Response Summary-May2009.doc F-Response White paper_202008.doc tesponse whitepaper changes	8/27/2012 10:29 AM 8/27/2012 10:29 AM 0/27/2012 10:29 AM 8/27/2012 10:29 AM 8/27/2012 10:29 AM	Windows PowerShel MP3 File DOC File DOC File Office Open XM. Do	1 KB 66,653 KB 104 KB 209 KB 16 KB	
Computer	Headshot MakeSmallFiles	8/27/2012 10:29 AM 8/27/2012 10:29 AM (Type: Compressed (zpped) F	JPEG Image alder pws PowerShel	1,207 KB	
도 EXCantainer 준:) 모 s3-standard (\\ANALYST) (Fi) 에 Network	MS_ConnectToAndroidTargetsEE MssionGuide FResponseConsultantEdition-Windows MssionGuide FResponseEnterpriseEdition-AppleOSX MssionGuide FResponseEnterpriseEdition-Unix	B/27/2012 10:29 AM B/27/2012 10:29 AM B/27/2012 10:29 AM B/27/2012 10:29 AM B/27/2012 10:29 AM	29 AM e Acrobat Doc Adobe Acrobat Doc Adobe Acrobat Doc Adobe Acrobat Doc	538 KB 501 KB 599 KB 644 KB	
	MissionQuide -FResponseEnterpriseEdition-Windows MissionQuides SupportQuideUSBoverEthernetv3	8/27/2012 10:29 AM 8/27/2012 10:29 AM 8/27/2012 10:29 AM	Adobe Acrobat Doc Compressed (zippe Adobe Acrobat Doc	561 KB 2,658 KB 446 KB	

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

