Mission Guide: Google Mail

Your Mission: Use F-Response to access Google Mail

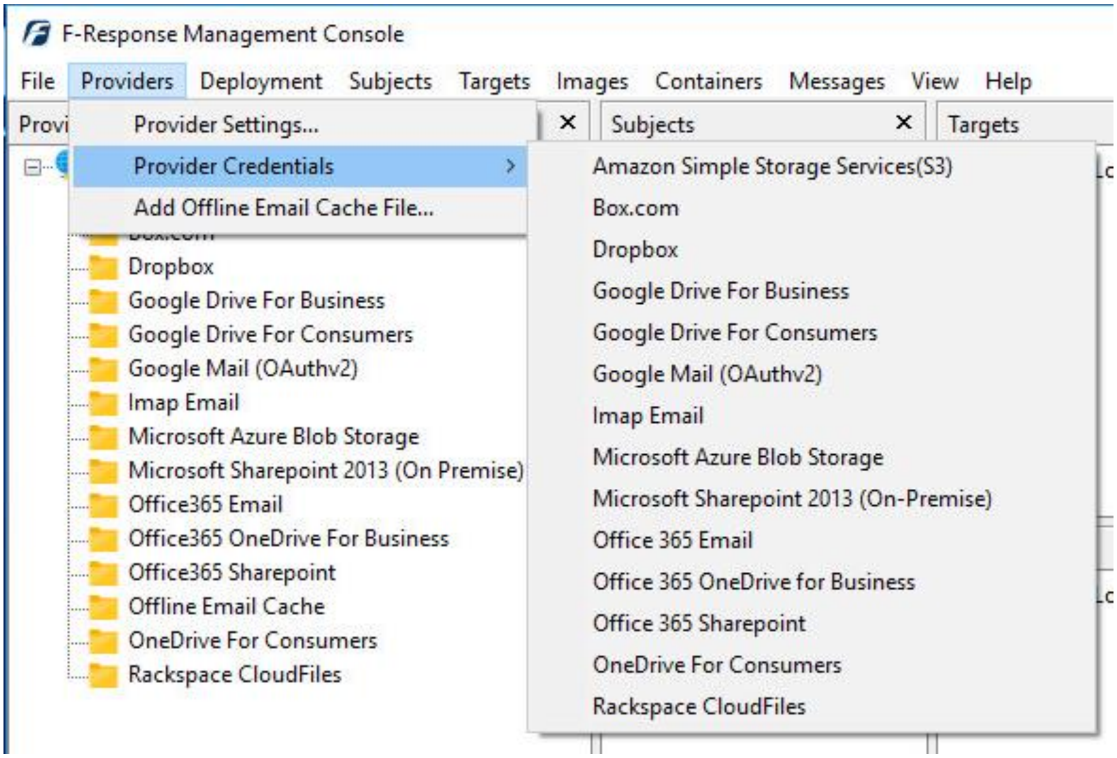
Using F-Response to connect to Google Mail and collect its contents

Important Note

Disclaimer: F-Response provide access to 3rd party data sources via Application Programming Interfaces (APIs) and internal structures presented by the provider. 3rd party provided data sources by their very nature are volatile. The afore mentioned F-Response products provide "best effort" for accessing and interacting with those 3rd party data sources however service disruptions, API changes, provider errors, network errors, as well as other communications issues may result in errors or incomplete data access. F-Response always recommends secondary validation of any 3rd party data collection.

Step 1: Open Google Mail Credential Configuration Window

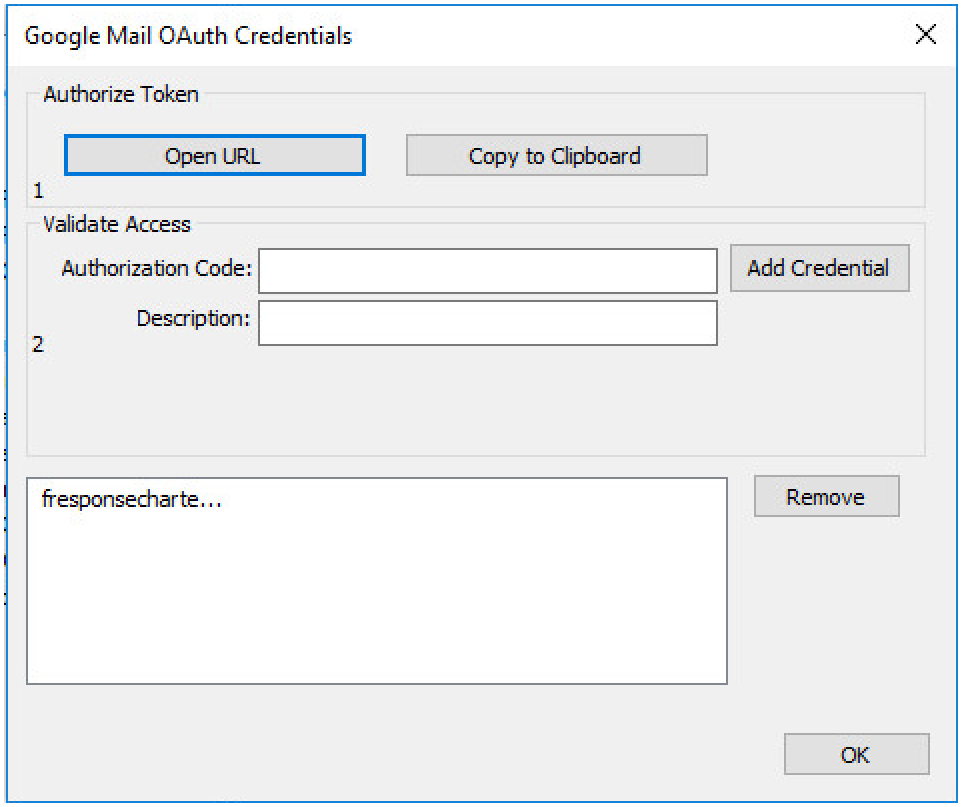
Open the F-Response Management Console and navigate to the Providers->Provider Credentials->Google Mail (OAuthv2) menu item.


F-Response Management Console
File
Providers
Deployment
Subjects
Targets
Images
Containers
Messages
View
Help
Provi
Provider Settings...
Provider Credentials
Add Offline Email Cache File...
Subjects
Targets
Amazon Simple Storage Services(S3)
Box.com
Dropbox
Google Drive For Business
Google Drive For Consumers
Google Mail (OAuthv2)
Imap Email
Microsoft Azure Blob Storage
Microsoft Sharepoint 2013 (On-Premise)
Office 365 Email
Office 365 OneDrive for Business
Office 365 Sharepoint
OneDrive For Consumers
Rackspace CloudFiles
Dropbox
Google Drive For Business
Google Drive For Consumers
Google Mail (OAuthv2)
Imap Email
Microsoft Azure Blob Storage
Microsoft Sharepoint 2013 (On Premise)
Office365 Email
Office365 OneDrive For Business
Office365 Sharepoint
Offline Email Cache
OneDrive For Consumers
Rackspace CloudFiles

F-Response Management Console

Step 2: Open URL or Copy to Clipboard

The first step in obtaining access to the Google Mail account is to request access either via the browser directly, or if you do not have access to the account in question, copying the request URL to the clipboard to be shared with the account holder via email, IM, etc.

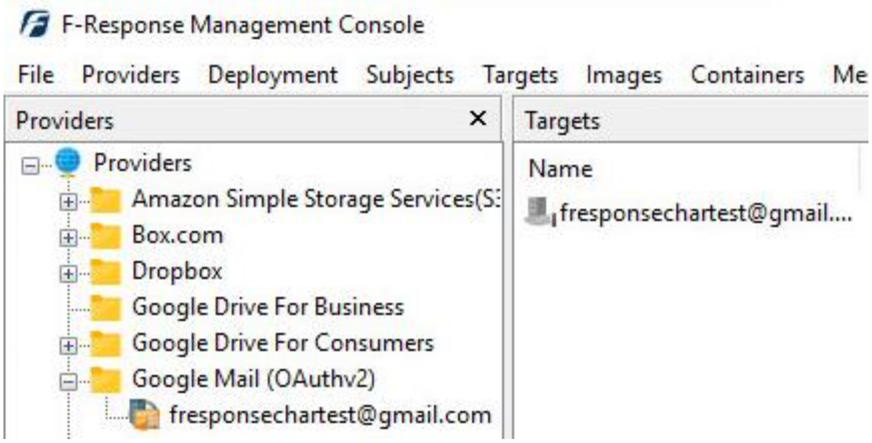


Google Mail Credentials Dialog

Regardless of the method chosen, the web browser user will be asked to login to Google Mail and authorize the F-Response Connector. Upon completion they will be redirected to the F-Response website where an Authorization code will be presented. This is the Google Mail Authorization Code, that code and a Description must be inputed into the credentials dialog window. Press Add Credential to verify and add this credential.

Step 3: Scan and Enumerate Google Mail accounts

Double click on the newly added Google Mail account under the Providers tree. This will scan the provider and result in a listing of available targets in the Targets window.



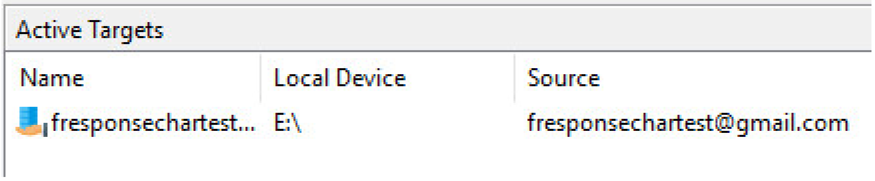
- Providers
  - Amazon Simple Storage Services(S:
  - Box.com
  - Dropbox
  - Google Drive For Business
  - Google Drive For Consumers
  - Google Mail (OAuthv2)
    - fresponsechartest@gmail.com

Name
fresponsechartest@gmail....

Listing Targets

Step 4: Login and Mount one or more Google Mail Targets

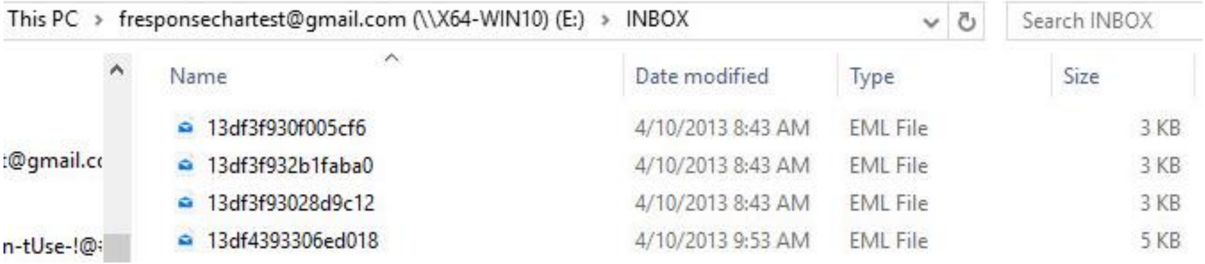
Double click on an individual target in the Targets window to begin the mounting process. Once attached the share will present a drive letter.



Name	Local Device	Source
fresponsechartest...	E:\	fresponsechartest@gmail.com

Attached Volume

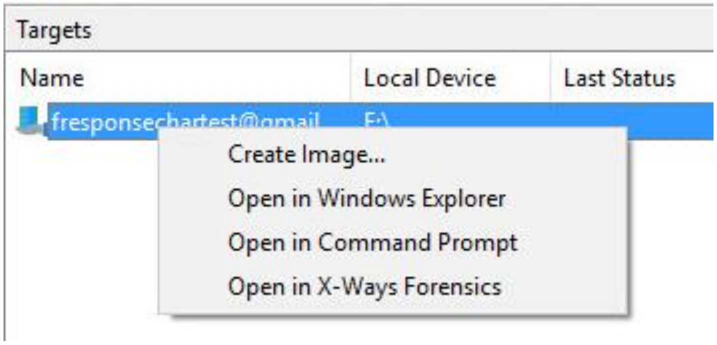
Gmail files are presented with Google's Unique Identifier in eml format:


This PC › fresponsechartest@gmail.com (\\X64-WIN10) (E:) › INBOX
Search INBOX
:@gmail.cc
n-tUse-!@

Name	Date modified	Type	Size
13df3f930f005cf6	4/10/2013 8:43 AM	EML File	3 KB
13df3f932b1faba0	4/10/2013 8:43 AM	EML File	3 KB
13df3f93028d9c12	4/10/2013 8:43 AM	EML File	3 KB
13df4393306ed018	4/10/2013 9:53 AM	EML File	5 KB

Step 5: Create Image of attached volume

Select the newly attached target and right click on the Local Device column. Use the "Create Image…" option to open the "Image" dialog to begin imaging the device.



Start Imaging Process…

Step 6: Complete Imaging Options…

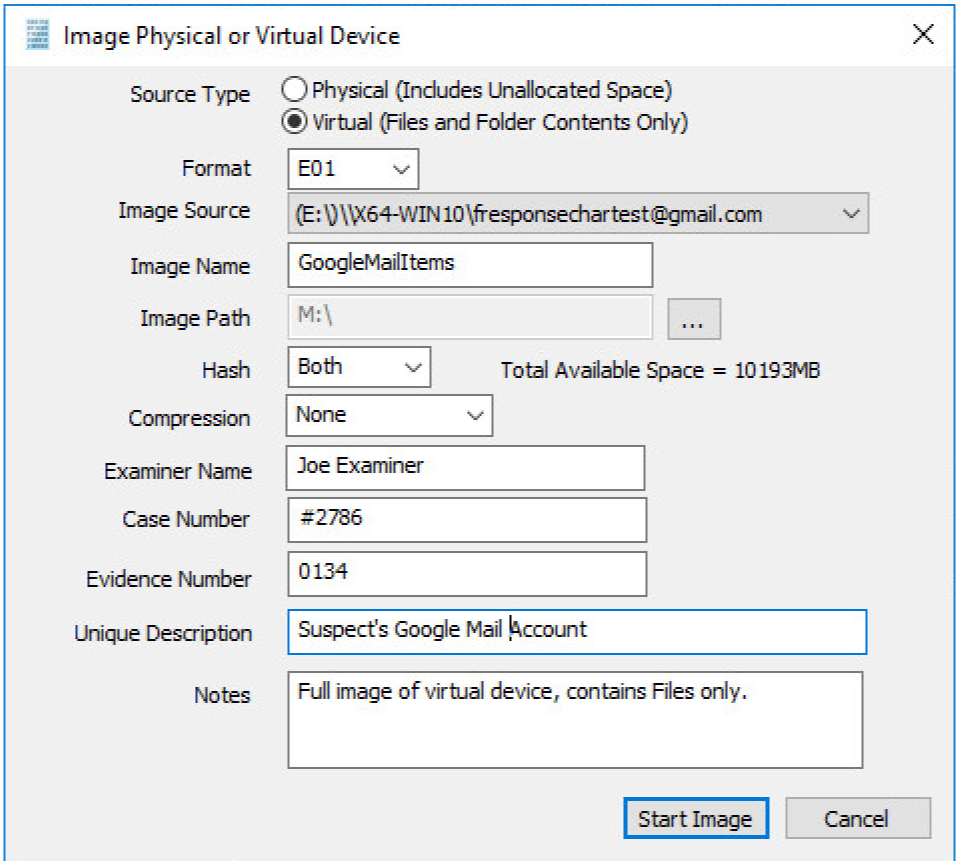


Image Physical or Virtual Device

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

Format: E01

Image Source: (E:\)\\X64-WIN10\fresponsechartest@gmail.com

Image Name: GoogleMailItems

Image Path: M:\

Hash: Both

Total Available Space = 10193MB

Compression: None

Examiner Name: Joe Examiner

Case Number: #2786

Evidence Number: 0134

Unique Description: Suspect's Google Mail Account

Notes: Full image of virtual device, contains Files only.

We'll work through this window from the top down. First, the **Source Type** is set to **Virtual** (by default) to be able to create an image of the connected virtual device data.

Next you can select the image **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.

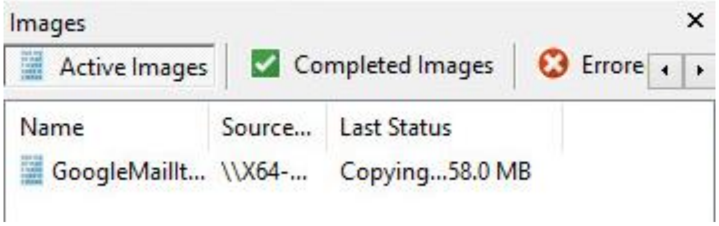
Image Source should be populated if we opened this window from Windows Explorer, just verify the drive letter is correct from Step 1. For **Image Path** we need to choose our destination drive—this must be a physical drive attached to our examiner machine (we cannot image to a network share).

Next we can choose 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 Image

Once started the dialog will close and you'll be able to monitor the image using the Active Images. When the Image completes you will see it move to Completed Images.

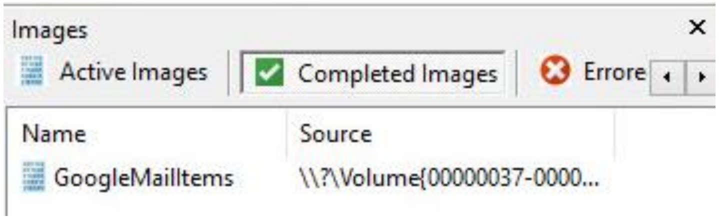


Name	Source...	Last Status
GoogleMailIt...	\\X64-...	Copying...58.0 MB

Imaging started and running…

Step 8: Review the Completed Image

Right click on the completed image to access the Image Path, Log, and File List. These logs and listings contain details about the image, the image itself, and a file listing of files collected.



Name	Source
GoogleMailItems	\\?\Volume{00000037-0000...

Reviewing the completed image.

Troubleshooting

I have an administrator account and I do not see the option to access the custodian accounts?

Correct, you need to enter the individual credentials for each account you wish to access.