

F-Response TACTICAL Manual

6.0.3.3

Provides a complete breakdown of leveraging F-Response TACTICAL Edition to perform expert remote computer forensics and incident response.

Table of Contents

Table of Contents	2
Welcome to F-Response TACTICAL	4
Supported Platforms	5
Prerequisites	6
F-Response TACTICAL License FOB Pair.....	7
Getting started with F-Response TACTICAL	8
Installing the F-Response TACTICAL Management Software (Optional, Recommended) ...	8
Managing F-Response TACTICAL.....	13
Backing up your F-Response TACTICAL Licenses	13
Restoring the F-Response TACTICAL Software	15
Restoring your F-Response TACTICAL Licenses.....	16
Download new F-Response TACTICAL Licenses.....	17
Using F-Response TACTICAL	18
Using F-Response TACTICAL Examiner for the first time on a Windows Vista or Windows 2008 Computer.	18
[OPTIONAL] Removing the F-Response TACTICAL Examiner driver from a Windows Vista, 2008, or 7 Computer.	20
Using F-Response TACTICAL to examine a Windows computer	21
Using F-Response TACTICAL to examine a Linux computer (Manual Method).....	22
Using F-Response TACTICAL to examine a Linux computer (Launcher Method)	23
Using F-Response TACTICAL to examine an Apple computer (Manual Method)	25
Using F-Response TACTICAL to examine an Apple computer (Launcher Method)Using the TACTICAL Examiner for Linux (Command Line).....	27
Using the TACTICAL Examiner for Linux (GUI)	31
F-Response Connector (Cloud Storage	35
Using the F-Response Connector for Cloud Storage Targets (TAC, CE, CE+C, and EE) ...	35
Configuring Cloud Storage Options.....	36
Configuring Cloud Storage Credentials	37
Scanning for Cloud Storage Targets.....	38
Connecting to Cloud Storage Targets.....	39
Disconnecting from Cloud Storage Targets	40
F-Response Connector (Database Objects).....	41

Using the F-Response Connector for Database Objects, Sharepoint 2010(TAC, CE, CE+C, and EE)	41
Configuring Database Server Credentials	42
Scanning for Database Object Targets	43
Connecting to Database Object Targets	44
Disconnecting from Database Object Targets	45
F-Response Connector (Email)	46
Using the F-Response Connector for Email (TAC, CE, CE+C, and EE).....	46
Configuring Connector Email Options	47
Configuring Email Credentials	48
Scanning for Email Account Targets	49
Connecting to Email Account Targets	50
Disconnecting from Email Account Targets.....	51
F-Response Flexdisk™	52
What is a F-Response Flexdisk™?	52
How do I access and use a F-Response Flexdisk™?.....	52
Frequently Asked Questions	54
Support.....	56
Appendix D - Master Software License Agreement.....	57
Appendix E - Legal Notices	62
Legal Notice	62
Trademarks	62
Statement of Rights	62
Disclaimer.....	62
Patents	62

Welcome to F-Response TACTICAL

Thank you for purchasing F-Response TACTICAL. You have now extended the capabilities of your existing arsenal of tools to enable them to work over an IP network. F-Response TACTICAL accomplishes this through the use of a Patented (US 7,899,882) process; a part of which includes leveraging the Internet Small Computer Systems Interface (iSCSI) protocol standard as defined in RFC 3720 (<http://www.ietf.org/rfc/rfc3720.txt>).

Supported Platforms

The F-Response TACTICAL Subject executable is capable of providing remote forensically sound read only physical hard drive connectivity on the following platforms:

Platforms supported by F-Response TACTICAL

- Windows XP (Home, Professional, Professional 64bit)
- Windows 2003 Server
- Windows Vista (32bit & 64bit)
- Windows 2008 (32bit & 64bit)
- Windows 7 (32bit & 64bit)¹
- Windows 8 (32bit & 64bit)
- Windows 2012 (32bit & 64bit)
- Linux (Glibc 2.3.5+)² (32bit and 64bit)
- Apple OS X (10.3, 10.4, 10.5, 10.6, 10.7, 10.8 Universal Binary)

F-Response Connector (TACTICAL Version)

Cloud Providers

- Amazon Web Services Simple Storage Service (S3)
- Windows Azure Blob Storage
- Rackspace Cloud Files (US and UK)
- HP Public Cloud
- Any Openstack³ based Cloud Storage (v1 series)
- Google Drive
- Dropbox
- Microsoft OneDrive

Email Providers

- Gmail (Google Apps and Gmail)
- Yahoo! Mail

¹ F-Response TACTICAL has received Windows 7 Compatibility validation from Microsoft.

² Linux glibc 2.3.5 includes Redhat, Suse, Ubuntu, Fedora, and many other distributions of Linux released during or after 2003.

³ More information on Openstack is available at www.openstack.org

- Most IMAP based Email providers

Database platforms

- Microsoft Sharepoint 2010, Microsoft SQL Server

Prerequisites

In order to use F-Response TACTICAL you will require the following:

1. A valid pair of F-Response TACTICAL License key FOBs (“TACTICAL FOBs”) which can be purchased from the F-Response Web site www.F-Response.com
2. Microsoft iSCSI initiator software, included by default with Windows Vista, Server 2008, and Windows 7 operating systems, and freely available for download from the Microsoft web site (**Only required on the Examiner computer**).

Note: The Microsoft iSCSI Software Initiator is available as a free download from <http://www.microsoft.com/downloads> for the following operating systems:

- Microsoft Windows Server 2003
- Microsoft Windows XP

This version should not be installed on the following operating systems:

- Windows Vista
- Windows Server 2008
- Windows 7
- Windows 8

The Microsoft iSCSI Software initiator is integrated into Windows Vista, Windows Server 2008, Windows 7, and Windows 8; therefore there is no need to install this package on those operating system versions.

The Microsoft iSCSI Software initiator configuration utility on Windows Vista and Windows Server 2008 can be accessed from the control panel in classic mode or from administrative tools in Windows Server 2008.

(Source: [Microsoft iSCSI Software Initiator 2.x User Guide](#), Nov 2007)

F-Response TACTICAL License FOB Pair

In order to use the F-Response TACTICAL application you must have a valid F-Response TACTICAL License FOB pair (“F-Response TACTICAL FOBs”), such as the ones shown below:



The F-Response TACTICAL Examiner License FOB (“Examiner”) must be inserted into the USB port of the analyst or investigator’s computer. The F-Response TACTICAL Subject License FOB (“Subject”) must be inserted into the USB port of the subject or target of inspection computer.

The F-Response TACTICAL License FOBs are USB Storage devices, they will be immediately recognized as USB Flash Storage disks on all supported platforms.

You will note that each FOB has a physical switch with designations for “locked” and “unlocked”. This is a physical write block feature that protects your USB device from being written to when the switch is in the “locked” position. We recommend using the subject FOB in its “locked” state, especially when being used on untrusted machines.

Getting started with F-Response TACTICAL

Installing the F-Response TACTICAL Management Software (Optional, Recommended)

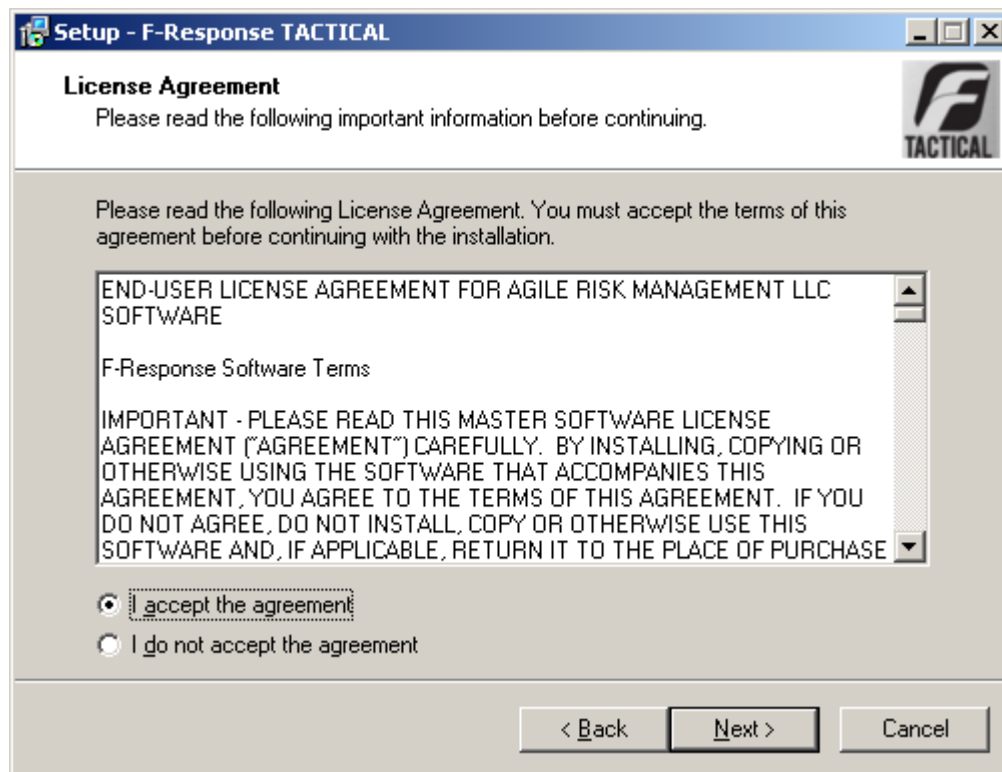
Download and install the F-Response TACTICAL Management software to your investigator or analyst computer. This installation contains a backup of all TACTICAL software deployed on the Examiner and Subject FOBs, in addition a management application that will allow you to backup and restore your F-Response TACTICAL licenses.⁴

The default installation is to Program Files -> F-Response. **Do not install this installation package on the machine to be analyzed.** The following screen captures show the steps involved in installing F-Response Enterprise Edition software on the analysis machine.

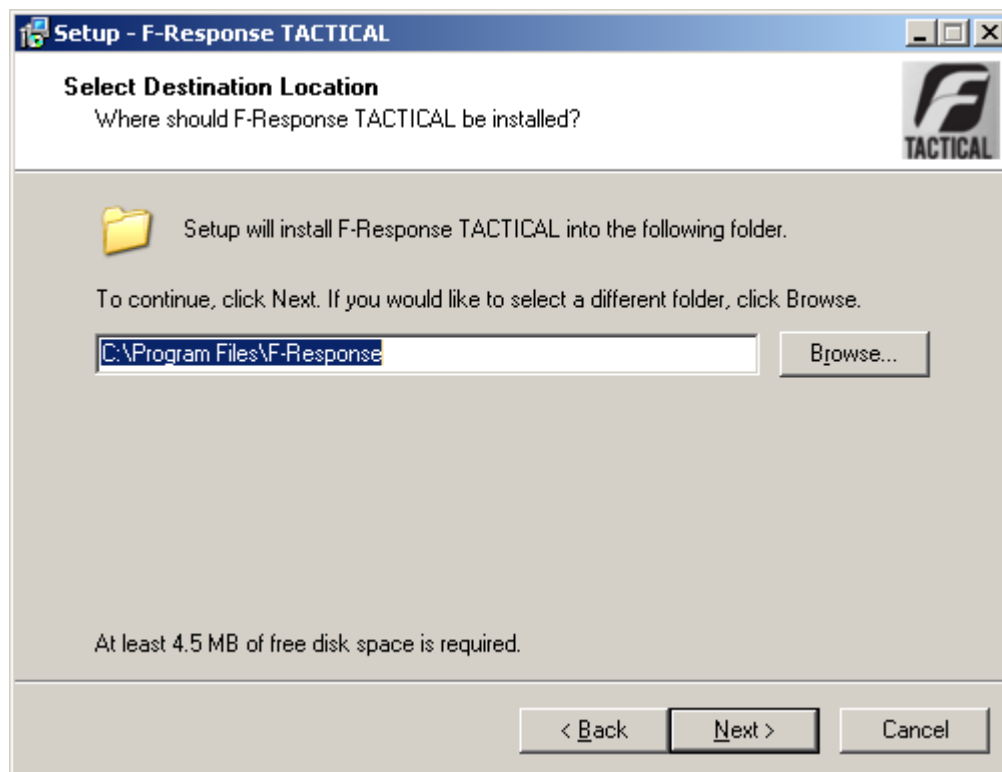


Initial Installation Window

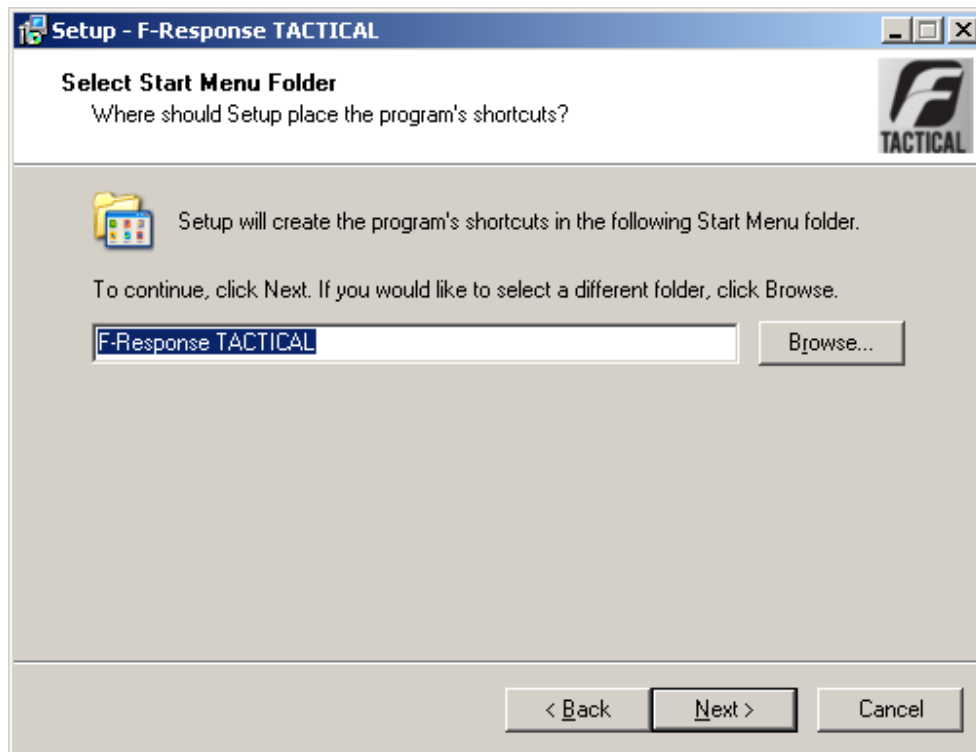
⁴ F-Response TACTICAL Manager will only backup one set of TACTICAL licenses, do not attempt to backup multiple licenses on one computer.



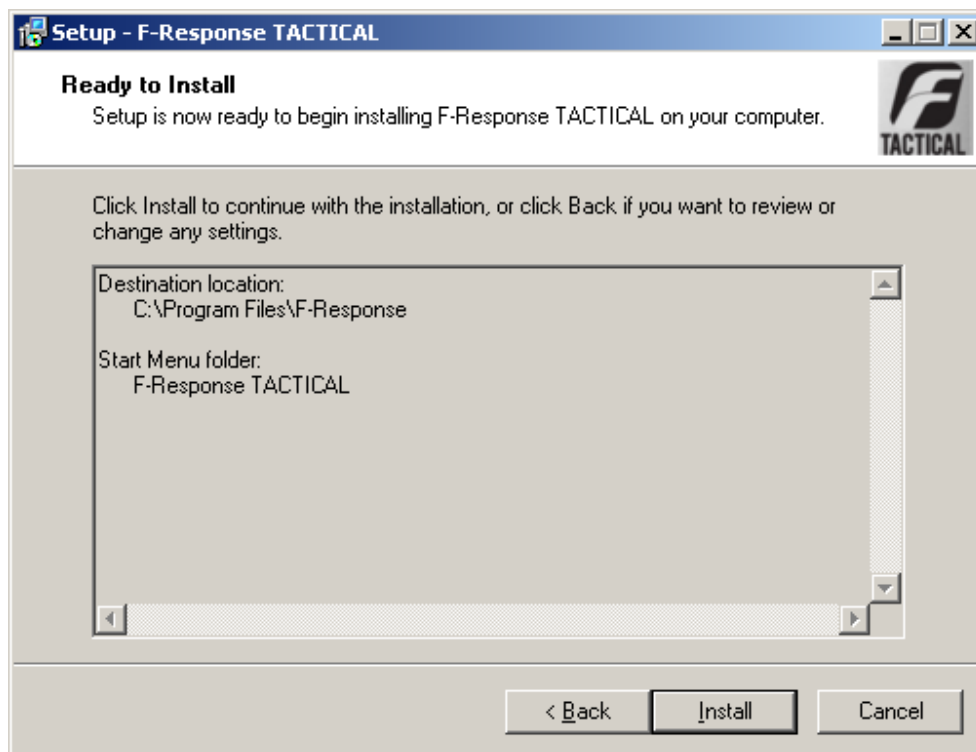
Standard Terms and Conditions



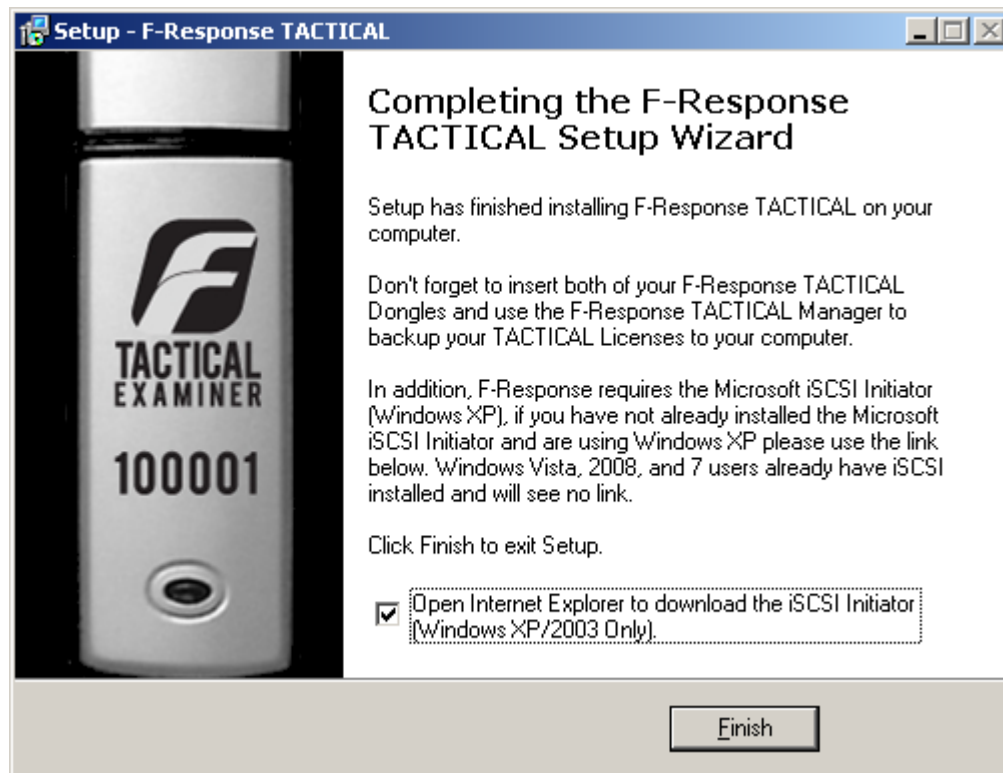
Select Destination Window



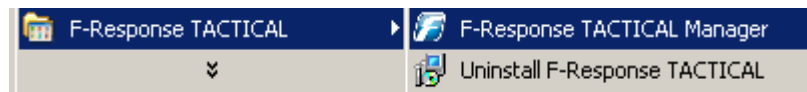
Select Start Menu Folder Window



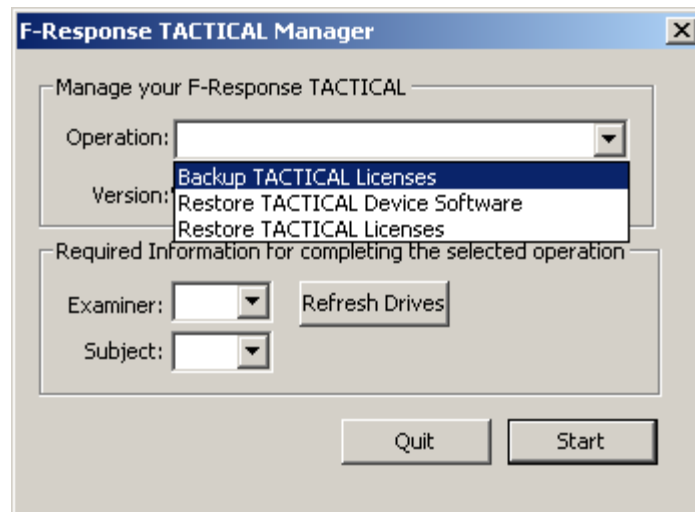
Confirm Installation Parameters Window



Installation Complete Window



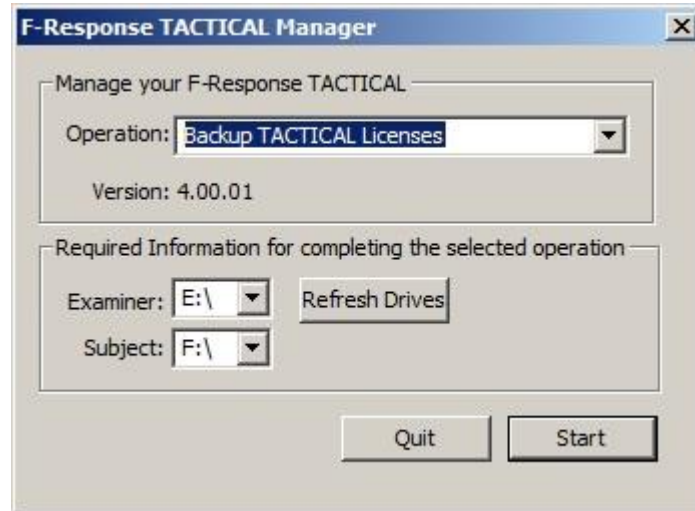
F-Response TACTICAL includes TACTICAL Manager



F-Response TACTICAL Manager Application

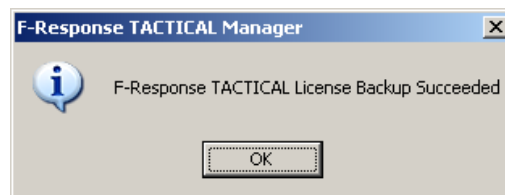
Managing F-Response TACTICAL

Backing up your F-Response TACTICAL Licenses

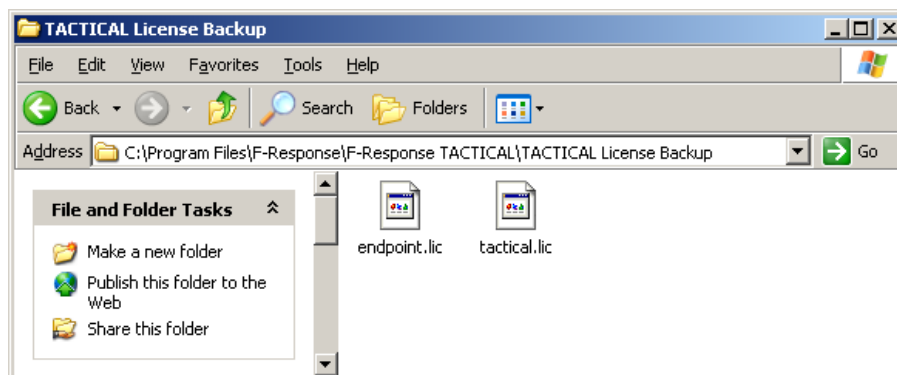


F-Response TACTICAL Manager “Backup TACTICAL Licenses”

We recommend using the F-Response TACTICAL Manager to backup your F-Response TACTICAL License files to your Analyst or Investigator’s computer prior to using F-Response TACTICAL for the first time. Insert both F-Response TACTICAL Fobs into your computer and select the appropriate drive letter for the Examiner and Subject device. If the drive letter is not listed, press “Refresh Drives” to re-populate the drop down listing of available devices. Press Start to begin the backup operation.

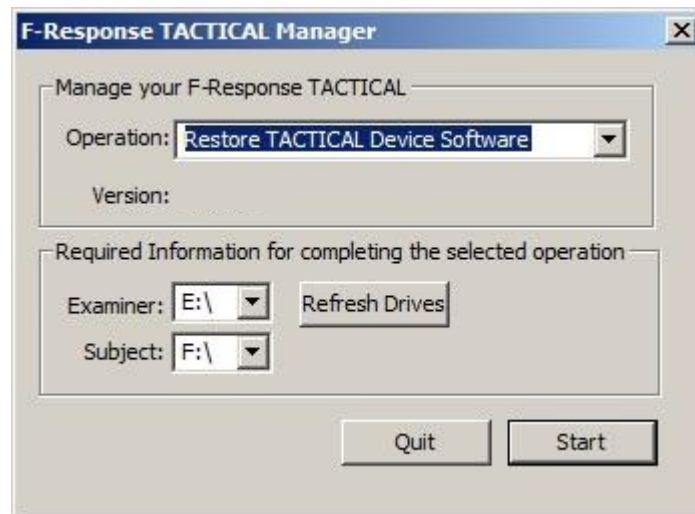


F-Response TACTICAL Manager “Backup TACTICAL Licenses” Completed Successfully



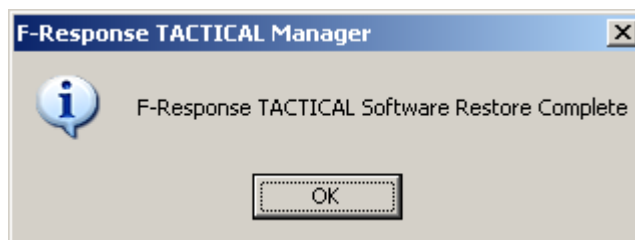
*TACTICAL License files are stored in C:\Program Files\F-Response\F-Response TACTICAL\Tactical
License Backup*

Restoring the F-Response TACTICAL Software



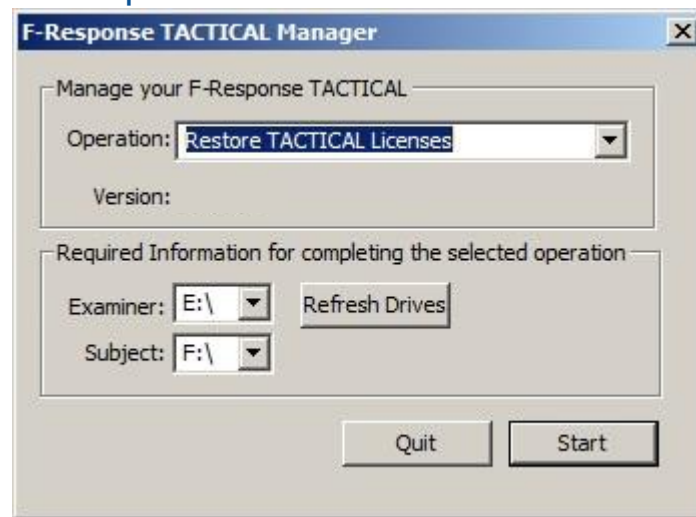
F-Response TACTICAL Manager "Restore TACTICAL Device Software"

Should the F-Response TACTICAL software ever be accidentally deleted, or if you have downloaded and installed a new version of F-Response TACTICAL, it will be necessary to update and restore the software to your F-Response TACTICAL Fobs. Insert both F-Response TACTICAL Fobs into your computer and select the appropriate drive letter for the Examiner and Subject device. If the drive letter is not listed, press "Refresh Drives" to re-populate the drop down listing of available devices. Press Start to begin the Restore/Update operation.



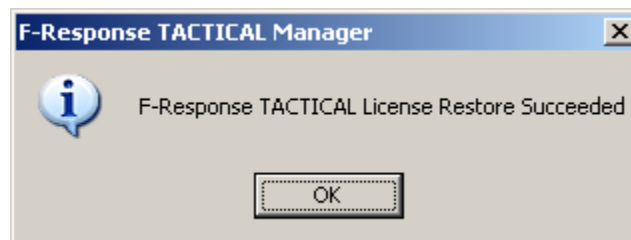
F-Response TACTICAL Manager "Restore TACTICAL Device Software" Completed Successfully

Restoring your F-Response TACTICAL Licenses



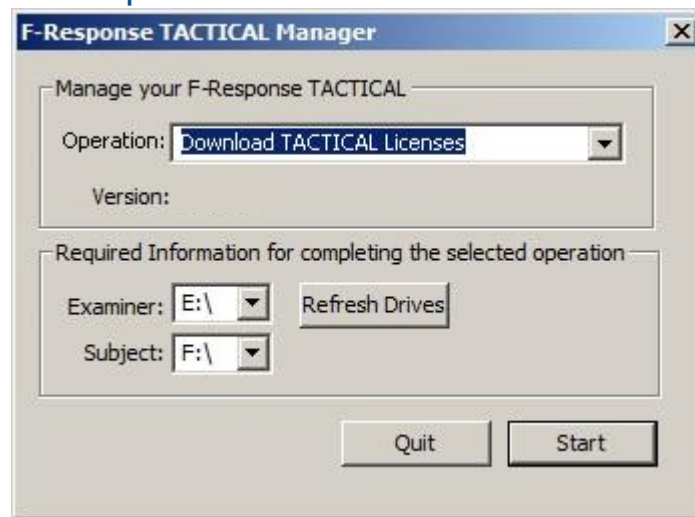
F-Response TACTICAL Manager "Restore TACTICAL Licenses"

Should the F-Response TACTICAL licenses ever be accidentally deleted, or if you have downloaded and copied new license files to your computer, it will be necessary to update and restore the licenses to your F-Response TACTICAL Fobs. Insert both F-Response TACTICAL Fobs into your computer and select the appropriate drive letter for the Examiner and Subject device. If the drive letter is not listed, press "Refresh Drives" to re-populate the drop down listing of available devices. Press Start to begin the Restore/Update operation.



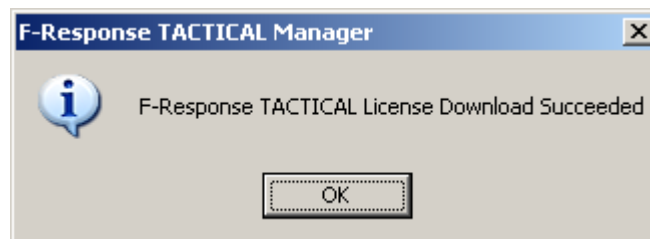
F-Response TACTICAL Manager "Restore TACTICAL Licenses" Completed Successfully

Download new F-Response TACTICAL Licenses



F-Response TACTICAL Manager "Download TACTICAL Licenses"

After renewing your F-Response TACTICAL you will be able to download replacement licenses directly from F-Response (Internet connection required). Insert both F-Response TACTICAL Fobs into your computer and select the appropriate drive letter for the Examiner and Subject device. If the drive letter is not listed, press "Refresh Drives" to re-populate the drop down listing of available devices. Press Start to begin the Download operation.



F-Response TACTICAL Manager "Download TACTICAL Licenses" Completed Successfully

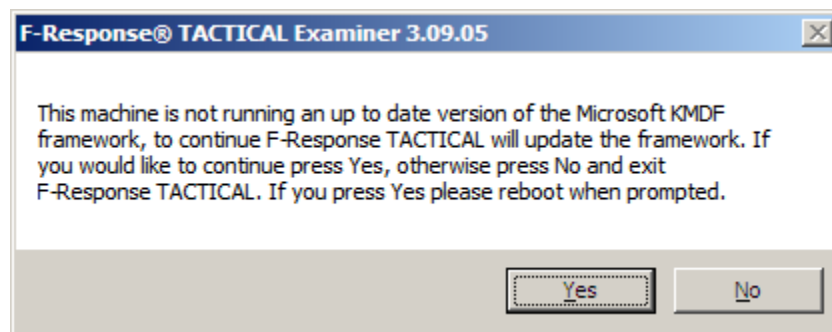
Using F-Response TACTICAL

Using F-Response TACTICAL Examiner for the first time on a Windows Vista or Windows 2008 Computer.

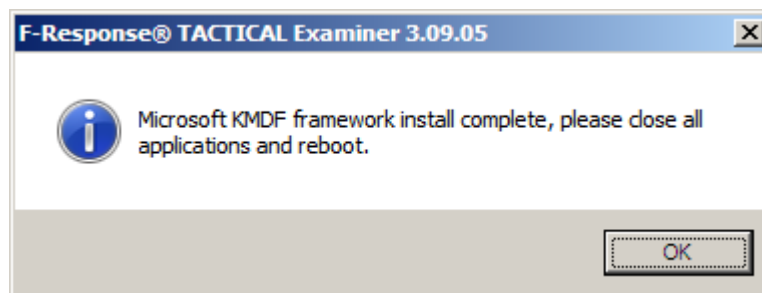
F-Response TACTICAL includes a special low-level operating system driver that needs to be deployed on the examiner computer prior to the first usage of F-Response TACTICAL Examiner.

Important note, this driver is only installed on the Examiner or Investigator computer and not the Subject computer.

In many cases the driver will install silently when you first open F-Response TACTICAL Examiner, however you may be prompted to upgrade the Microsoft KMDF Framework prior to continuing. By agreeing to the upgrade F-Response TACTICAL Examiner will initiate the upgrade process and prompt you when a reboot is required. You may elect not to upgrade the Microsoft KMDF and forgo using F-Response TACTICAL Examiner by selecting "No".



F-Response TACTICAL Microsoft KMDF Upgrade prompt



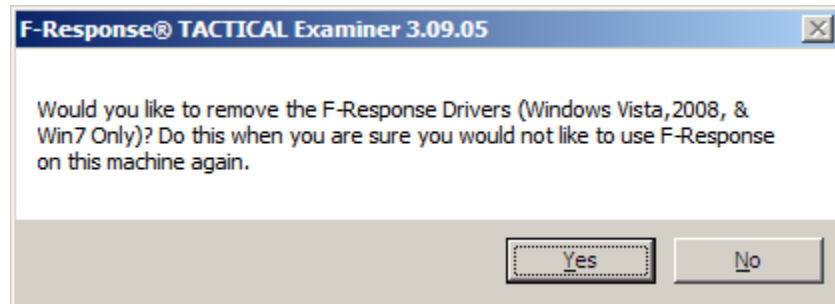
F-Response TACTICAL Reboot Prompt

Following a successful reboot you will be able to use F-Response TACTICAL Examiner without further driver prompting.

If you receive this warning on a Windows 7 or 8 computer this means you are not using the latest F-Response TACTICAL. Please make sure to download the latest F-Response TACTICAL Installer (<https://www.f-response.com/support/downloads>) and use the “Restore Device Software” option in the TACTICAL Manager.

[OPTIONAL] Removing the F-Response TACTICAL Examiner driver from a Windows Vista, 2008, or 7 Computer.

As indicated earlier, F-Response TACTICAL Examiner will install a low-level driver on Windows Vista, 2008, and Windows 7 computers prior to your first use. If at some future point you would like to completely remove that driver from the system you can do this by selecting “Help->Remove Drivers” in the F-Response TACTICAL Examiner menu.



F-Response TACTICAL Removal Prompt

You will have the option of removing drivers only on Windows Vista, 2008, and Windows 7 machines. If you elect to proceed, F-Response TACTICAL Examiner will remove the driver and close F-Response TACTICAL. At this point you can remove the F-Response TACTICAL Examiner dongle.

Using F-Response TACTICAL to examine a Windows computer

1

INSERT TACTICAL SUBJECT

Insert the F-Response TACTICAL Subject USB Dongle into the Suspect's Windows Computer. Locate the newly created Removable Disk and double-click on the f-response-tacsub.exe executable.



2

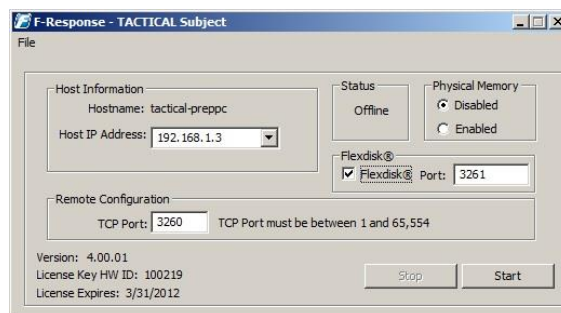
Press the START Button

Press the "START" button on the F-Response - TACTICAL Subject application window.

2

OPTIONAL, Hide the WINDOW, Enable FLeXdisk

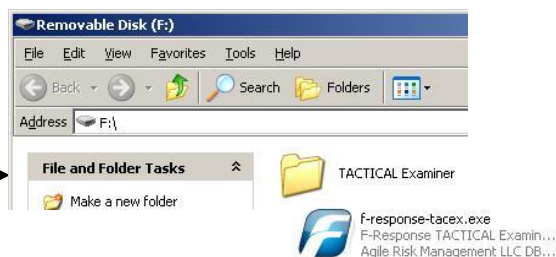
Press CTRL-ALT-F12 to hide the F-Response TACTICAL Subject Window. The same key sequence will restore the window. You can enable Flexdisk™ access by checking the Flexdisk™ box.



3

INSERT TACTICAL EXAMINER

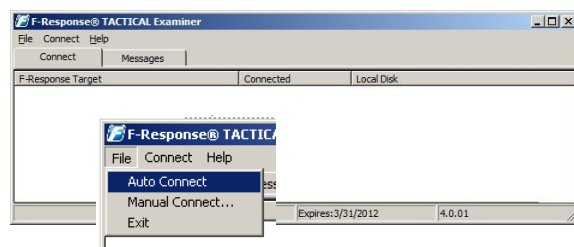
Insert the F-Response TACTICAL Examiner USB Dongle into the Analyst or Investigator's Windows Computer. Locate the newly created Removable Disk and double-click on the f-response-tacex.exe



4

Select File "Auto Connect"

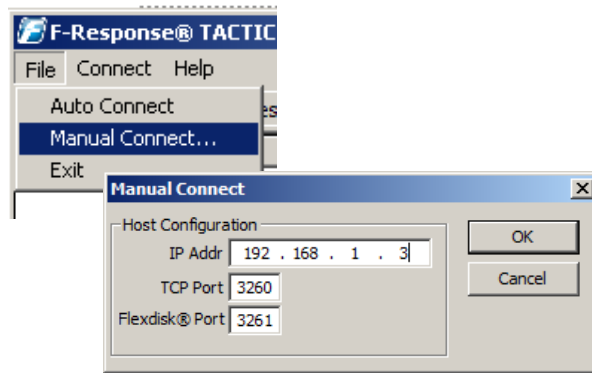
Select the File menu item "Auto Connect", this will tell the TACTICAL Examiner to begin searching the local network for the Subject.



4

(OPTIONAL) If Auto Connect does not work.

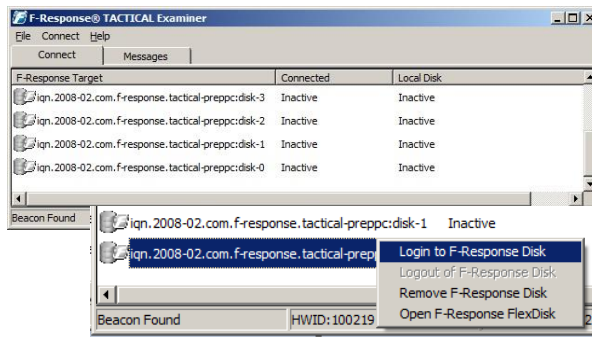
Select the File menu item "Manual Connect" and input the IP Address in the "Host IP Address" field on the TACTICAL Subject. See Above.



5

Login to the presented devices

Select one or more F-Response Targets, then right click and select "Login to F-Response Disk" to login to an F-Response Disk. Use the "Local Disk" column to identify the newly attached device on your



5

OPTIONAL

Select the Connect menu item "Open F-Response Flexdisk™" to launch the default browser and connect to the F-Response Flexdisk™ web viewer on the

Using F-Response TACTICAL to examine a Linux computer (Manual Method)

1

INSERT TACTICAL Subject

Insert the F-Response TACTICAL Subject USB Dongle into the Suspect's Linux Computer. Locate the newly created Removable Disk and open a Terminal Window.



2

Navigate to the USB Storage Device and execute the program

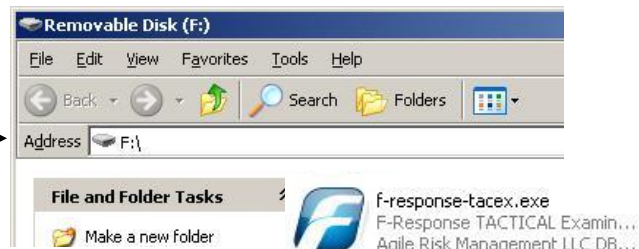
Navigate to the folder containing the F-Response TACTICAL Subject for Linux (f-response-tacsub-lin.exe or f-response-tacsub-lin-64.exe), in this instance that folder is /media/disk. Next execute the program as root or using sudo, (Root or account password will be required). The

```
root@mshannon-desktop: /media/disk/TACTICAL Subject
File Edit View Terminal Tabs Help
mshannon@mshannon-desktop:~$ sudo su
[sudo] password for mshannon:
root@mshannon-desktop:/home/mshannon# cd /media/disk/TACTICAL\ Subject/
root@mshannon-desktop:/media/disk/TACTICAL Subject# ./f-response-tacsub-lin
F-Response TACTICAL Subject (Linux Edition) Version 3.09.05
F-Response Disk: /dev/sda (16777216 sectors, 512 sector size)
8192 MB write blocked storage on F-Response Disk:sda
F-Response Disk: /dev/sdb (3891200 sectors, 512 sector size)
1900 MB write blocked storage on F-Response Disk:sdb
```

3

INSERT TACTICAL Examiner

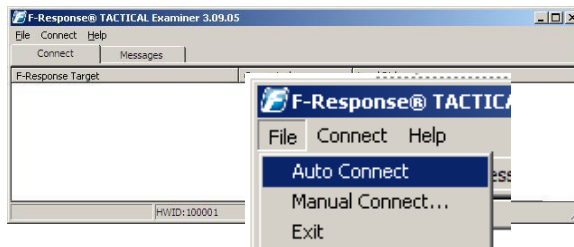
Insert the F-Response TACTICAL Examiner USB Dongle into the Analyst or Investigator's Windows Computer. Locate the newly created Removable Disk and double-click on the f-response-tacex.exe executable.



4

Select File "Auto Connect"

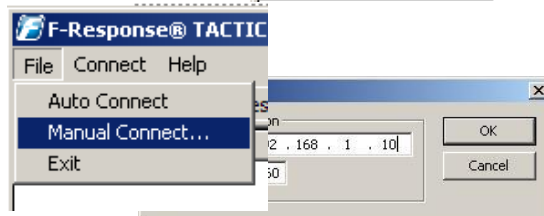
Select the File menu item "Auto Connect", this will tell the TACTICAL Examiner to begin searching the local network for the Subject.



4

(OPTIONAL) If Auto Connect does not work.

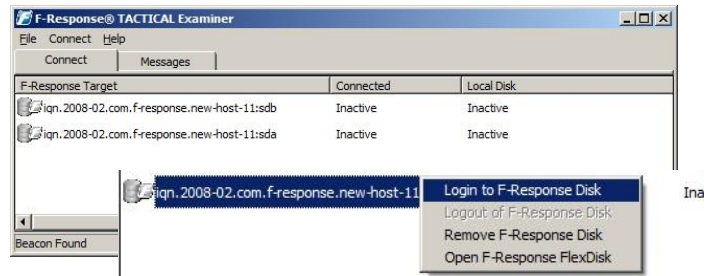
Select the File menu item "Manual Connect" and input the IP Address in the "Host IP Address" field on the TACTICAL Subject. See Above.



5

Login to the presented devices

Select one or more F-Response Targets, then right click and select "Login to F-Response Disk" to login to an F-Response Disk. Use the "Local Disk" column to identify the newly attached device on your



5

OPTIONAL



Select the Connect menu item "Open F-Response Flexdisk™" to launch the default browser and connect to the F-Response Flexdisk™ web viewer on the

Using F-Response TACTICAL to examine a Linux computer (Launcher Method)

- 1**

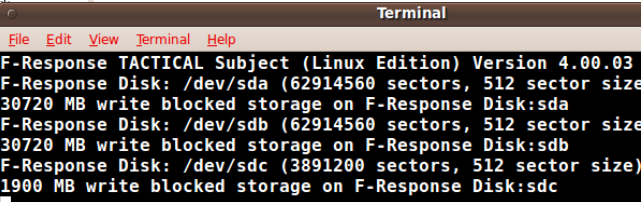
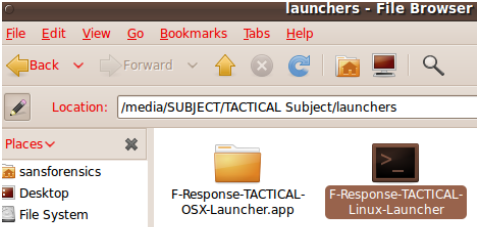
INSERT TACTICAL Subject

Insert the F-Response TACTICAL Subject USB Dongle into the Suspect's Linux Computer. Locate the newly created Removable Disk and double click to view contents.


- 2**



Navigate to the Launchers folder and double click on the appropriate launcher

Inside the TACTICAL Subject folder is a launchers folder. Inside the launchers folder you will find launchers for both the standard and 64bit versions of F-Response TACTICAL Subject for Linux. Double click on the appropriate launcher to execute TACTICAL.


- 3**

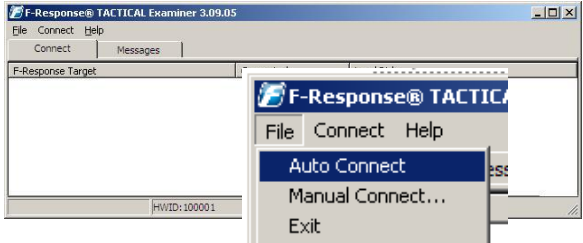
INSERT TACTICAL Examiner

Insert the F-Response TACTICAL Examiner USB Dongle into the Analyst or Investigator's Windows Computer. Locate the newly created Removable Disk and double-click on the f-response-tacex.exe executable.


- 4**

Select File "Auto Connect"

Select the File menu item "Auto Connect", this will tell the TACTICAL Examiner to begin searching the local network for the Subject.



- 4**

(OPTIONAL) If Auto Connect does not work.

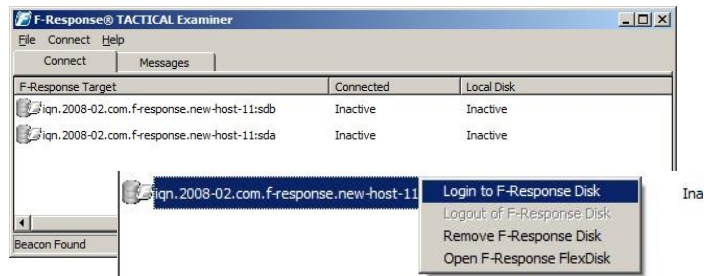
Select the File menu item "Manual Connect" and input the IP Address in the "Host IP Address" field on the TACTICAL Subject. See Above.



5

Login to the presented devices

Select one or more F-Response Targets, then right click and select "Login to F-Response Disk" to login to an F-Response Disk. Use the "Local Disk" column to identify the newly attached device on your



5

OPTIONAL

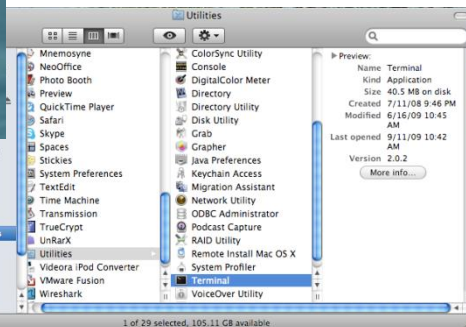
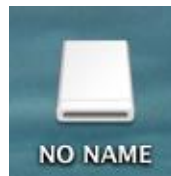
Select the Connect menu item "Open F-Response Flexdisk™" to launch the default browser and connect to the F-Response Flexdisk™ web viewer on the

Using F-Response TACTICAL to examine an Apple computer (Manual Method)

1

INSERT TACTICAL Subject

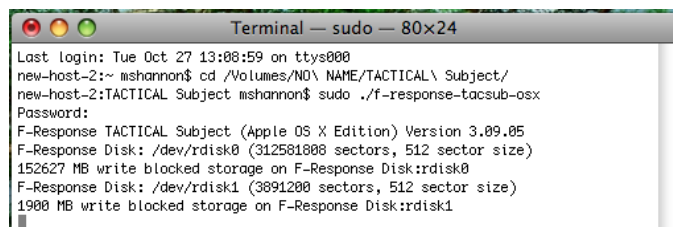
Insert the F-Response TACTICAL Subject USB Dongle into the Suspect's Apple OSX Computer. Locate the newly created Removable Disk and open a Terminal Window.



2

Navigate to the USB Storage Device and execute the program

Navigate to the folder containing the F-Response TACTICAL Subject for OSX (f-response-tacsub-osx), in this instance that folder is /Volumes/NO NAME. Next execute the program as root or using sudo, (admin or account password will be required). The command line is



3

INSERT TACTICAL Examiner

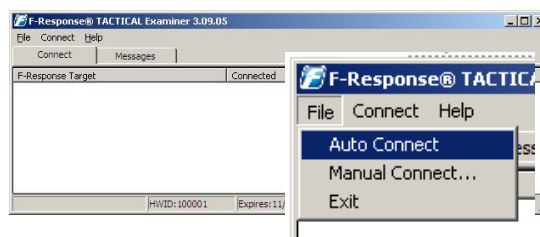
Insert the F-Response TACTICAL Examiner USB Dongle into the Analyst or Investigator's Windows Computer. Locate the newly created Removable Disk and double-click on the f-response-...



4

Select File "Auto Connect"

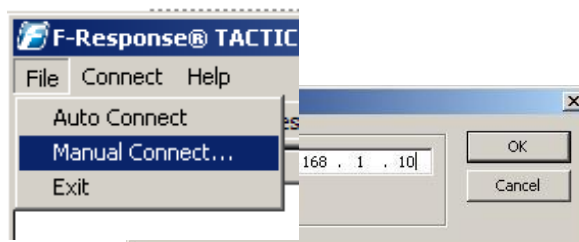
Select the File menu item "Auto Connect", this will tell the TACTICAL Examiner to begin searching the local network for the Subject.



4

(OPTIONAL) If Auto Connect does not work.

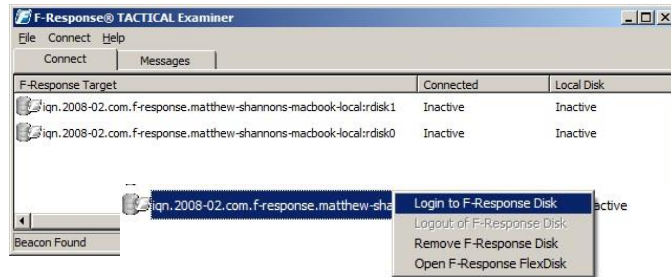
Select the File menu item "Manual Connect" and input the IP Address in the "Host IP Address" field on the TACTICAL Subject. See Above.



5

Login to the presented devices

Select one or more F-Response Targets, then right click and select "Login to F-Response Disk" to login to an F-Response Disk. Use the "Local Disk" column to identify the newly attached device on your



5

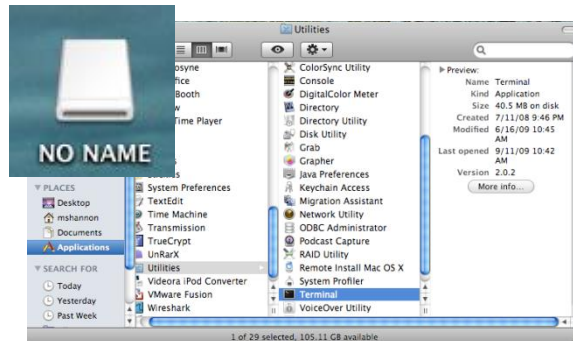
OPTIONAL

Select the Connect menu item "Open F-Response Flexdisk™" to launch the default browser and connect to the F-Response Flexdisk™ web viewer on the

Using F-Response TACTICAL to examine an Apple computer (Launcher Method)

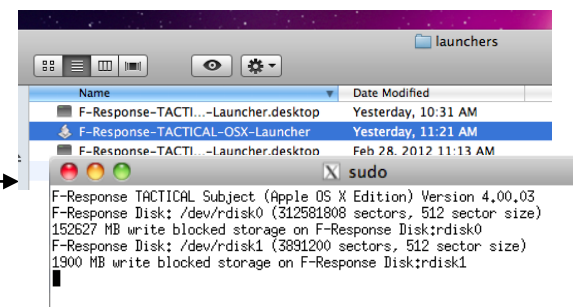
1 INSERT TACTICAL Subject

Insert the F-Response TACTICAL Subject USB Dongle into the Suspect's Apple OSX Computer. Locate the newly created Removable Disk and double click on it to view the contents.



2 Navigate to the Launchers folder and double click on the appropriate launcher

Inside the TACTICAL Subject folder is a launchers folder. Inside the launchers folder you will find launchers for F-Response TACTICAL for OSX, double click on the launcher to execute F-Response. You will be prompted for Administrative Access.



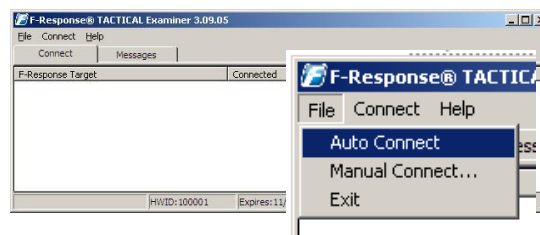
3 INSERT TACTICAL Examiner

Insert the F-Response TACTICAL Examiner USB Dongle into the Analyst or Investigator's Windows Computer. Locate the newly created Removable Disk and double click on the f-response-



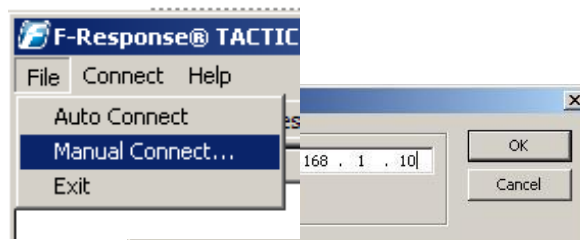
4 Select File "Auto Connect"

Select the File menu item "Auto Connect", this will tell the TACTICAL Examiner to begin searching the local network for the Subject.



4 (OPTIONAL) If Auto Connect does not work.

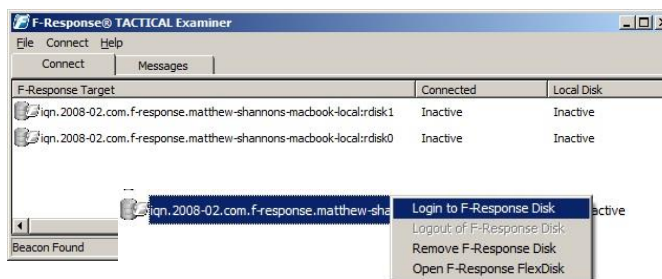
Select the File menu item "Manual Connect" and input the IP Address in the "Host IP Address" field on the TACTICAL Subject. See Above.



5

Login to the presented devices

Select one or more F-Response Targets, then right click and select "Login to F-Response Disk" to login to an F-Response Disk. Use the "Local Disk" column to identify the newly attached device on your



5

OPTIONAL

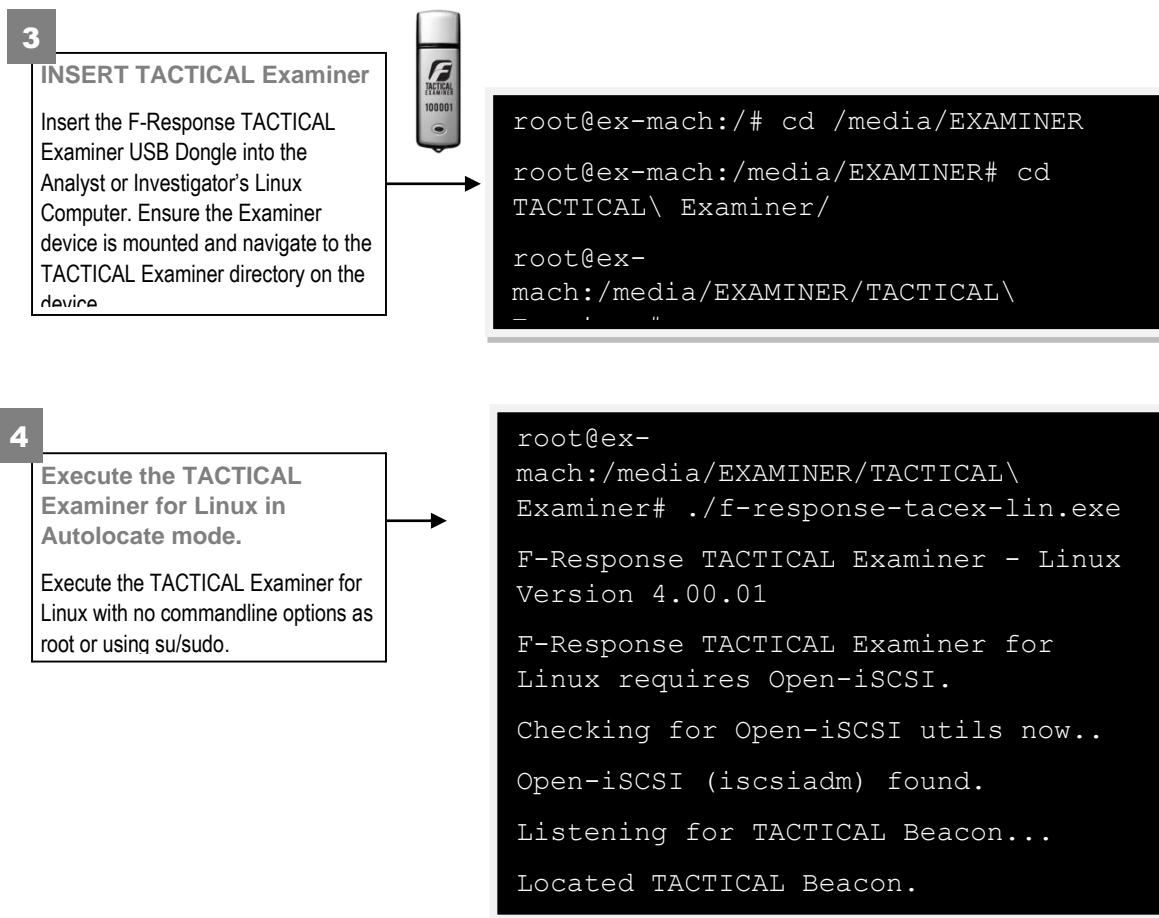
Select the Connect menu item "Open F-Response Flexdisk™" to launch the default browser and connect to the F-Response Flexdisk™ web viewer on the

Using the TACTICAL Examiner for Linux (Command Line)

F-Response TACTICAL Examiner includes a Linux based executable to allow for connections from Linux based machines to F-Response TACTICAL Subject targets. In order to effectively use the F-Response TACTICAL Examiner for Linux (f-response-tacex-lin.exe) you will need to meet the following requirements in order to use the Linux Examiner on your machine:

- Open-iSCSI
- Compatibility Libraries for 32bit Applications⁵
- Root access (native, or via SU/SUDO)

Please refer to the prior sections when using the TACTICAL Subject software, however starting on Step 3 you will refer to the following steps to properly use the TACTICAL Examiner for Linux.



⁵ Only required on 64bit Linux Examiner machines.

4

OPTIONAL Manual Connection

If the Auto-Locate option should fail use the following syntax to perform a manual connection: "f-response-tacex-lin -s <TARGETIP> -p <TARGET PORT>"



```
root@ex-
mach:/media/EXAMINER/TACTICAL\
Examiner# ./f-response-tacex-lin -s
192.168.1.5 -p 3260

F-Response TACTICAL Examiner - Linux
Version 4.00.01

F-Response TACTICAL Examiner for
Linux requires Open-iSCSI.

Checking for Open-iSCSI utils now..

Open-iSCSI (iscsiadm) found.

Discovery Results
```

5

Login to the presented devices

Use the resulting output to login to a target device, example login syntax is provided here



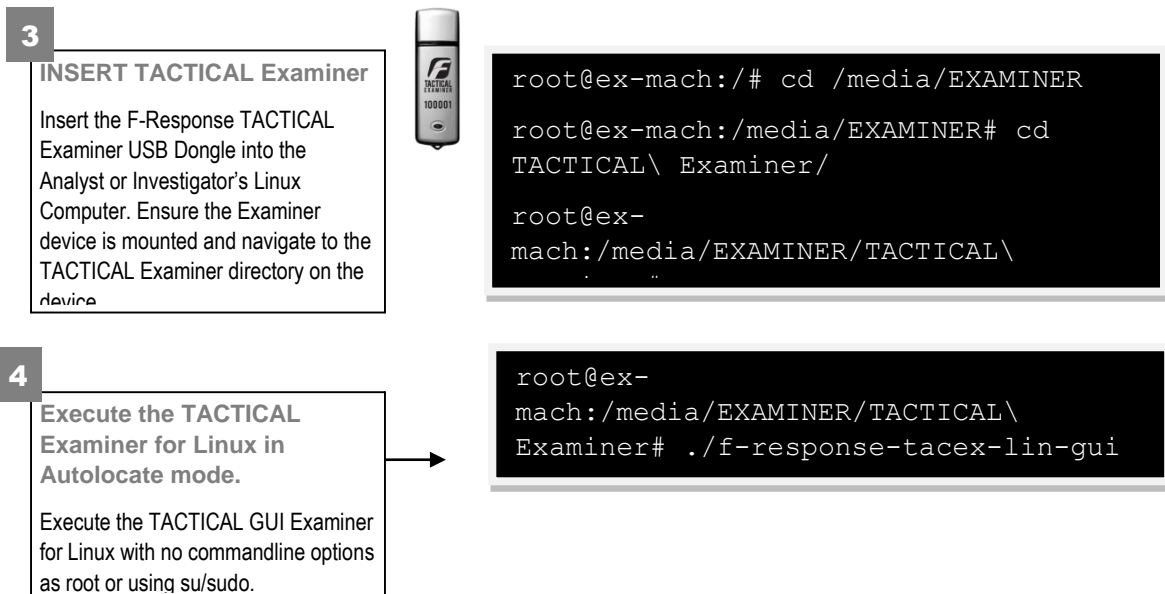
```
root@ex-mach:/media/EXAMINER/TACTICAL\
Examiner# iscsiadm -m node --
targetname=iqn.2008-02.com.f-
response.tactical-preppc:disk-0 --
login
```


Using the TACTICAL Examiner for Linux (GUI)

F-Response TACTICAL Examiner includes a GUI Linux based executable to allow for connections from Linux based machines to F-Response TACTICAL Subject targets. In order to effectively use the F-Response GUI TACTICAL Examiner for Linux (f-response-tacex-lin-gui) you will need to meet the following requirements in order to use the Linux Examiner on your machine:

- Open-iSCSI
- Compatibility Libraries for 32bit Applications⁶
- Root access (native, or via SU/SUDO)

Please refer to the prior sections when using the TACTICAL Subject software, however starting on Step 3 you will refer to the following steps to properly use the TACTICAL Examiner for Linux.

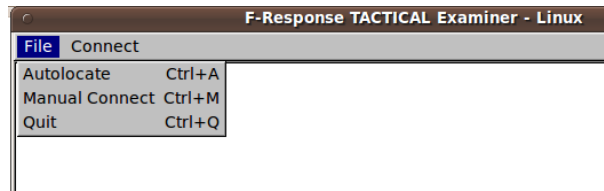


⁶ Only required on 64bit Linux Examiner machines.

4

Select Autolocate or Manual Connect

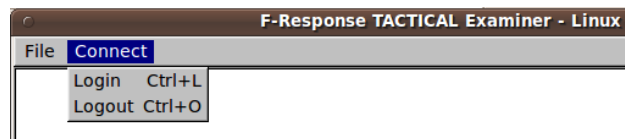
Use either the Autolocate or Manual Connect option to locate the remote Subject executable on the network.



5

Login to the presented devices

Select a returned device listing and use the Connect-> Login to login to the device then Connect->Logout to disconnect a device.



F-Response Connector (Cloud Storage)

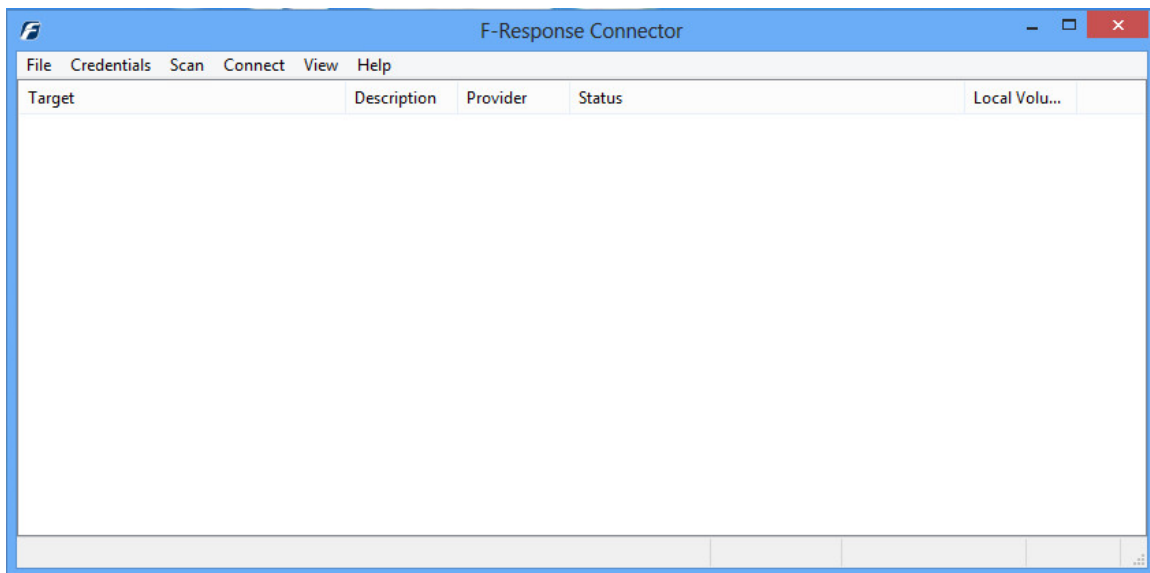
Using the F-Response Connector for Cloud Storage Targets (TAC, CE, CE+C, and EE)

Disclaimer: The F-Response Connector and legacy Connector products (F-Response Email Connector, Cloud Connector, and Database Object Connector) provide access to 3rd party data sources via Application Programming Interfaces (APIs) and internal structures presented by the provider. 3rd party provided data sources are by their very nature 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.

F-Response TACTICAL, Consultant, Consultant + Covert, and Enterprise edition includes a copy of the F-Response Connector (FC). The FC allows an examiner to mount remote Cloud Storage containers, Email Accounts, and Sharepoint Documents (Embedded Database Objects) as local read-only logical volumes or network shares.

The FC does not require executables or agents be deployed to remote systems.

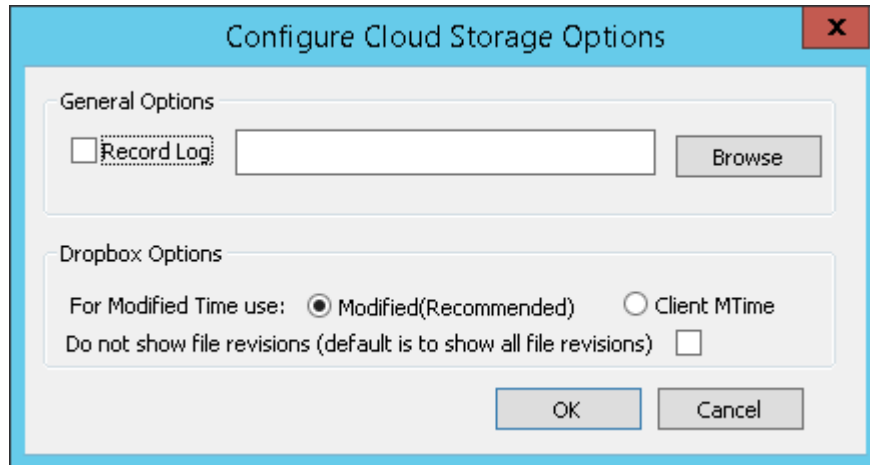
The FC does require a locally attached F-Response licensed dongle (TACTICAL, Consultant, or Consultant+Covert), or a remote Enterprise F-Response dongle connected via the F-Response License Manager at all times.



F-Response Connector

Configuring Cloud Storage Options

There are a number of options that can be configured when using the F-Response Connector to access Cloud Storage, these options include:

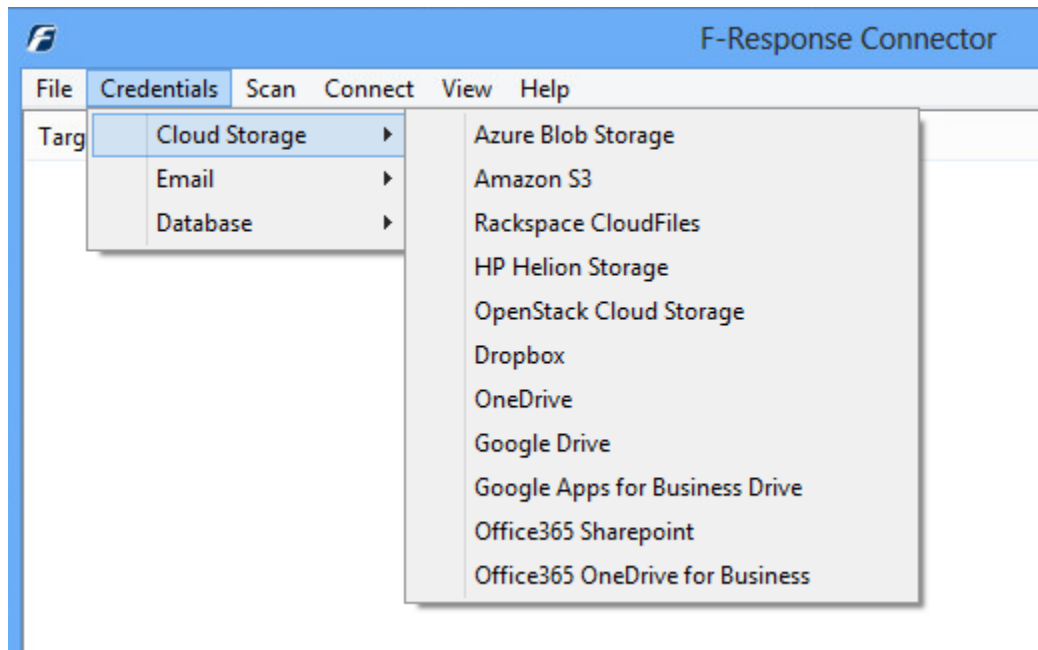


F-Response Connector Configure Cloud Storage Options

- **General Options**
 - **Record Log**
 - Will create a secondary CSV log file with the drive contents for each attached Cloud Storage device.
- **Dropbox Options**
 - **For Modified Time Use:**
 - Dropbox provides two different times that can be used as Modified Time for a given file. By default the Cloud Connector uses the Modified time as provided by the Dropbox Servers. Alternatively it is now possible to use the Client MTime, a non verified time that is assigned to the files when they are modified by a Dropbox Client tool. The Client MTime is not verified by Dropbox.
 - **Do not show file revisions (default is to show all file revisions)**
 - By default the connector will show all revisions for Dropbox items, checking this box will tell the Connector to not request multiple versions of items.

Configuring Cloud Storage Credentials

Before you can connect to Cloud Storage services you must first input valid credentials. While the credentials necessary vary by cloud storage provider, all credentials must be input using one of the Configure Credentials dialog boxes.

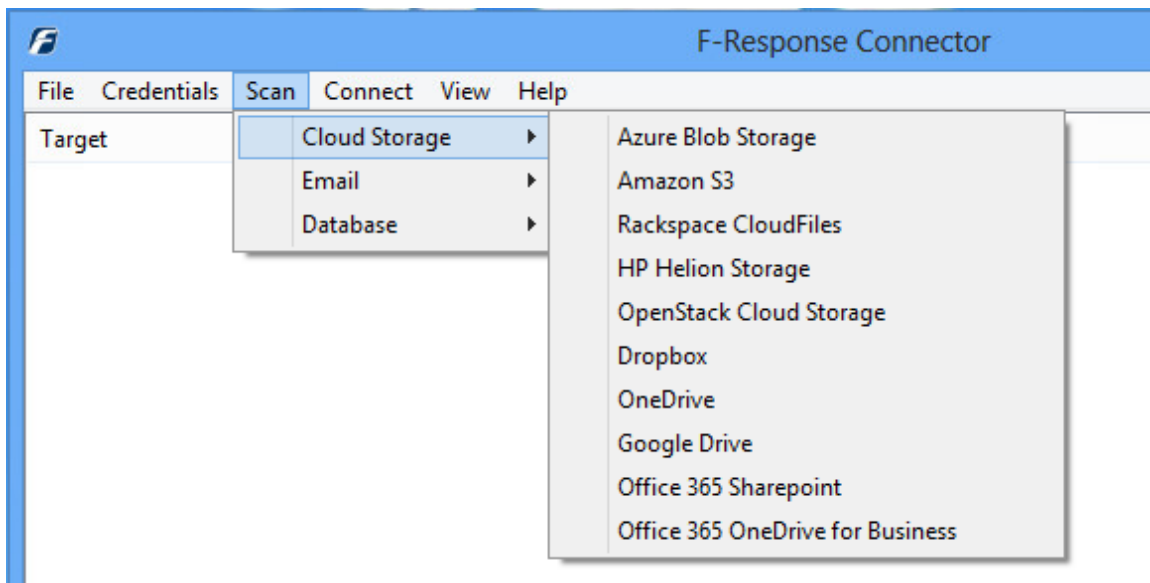


Credentials->Cloud Storage

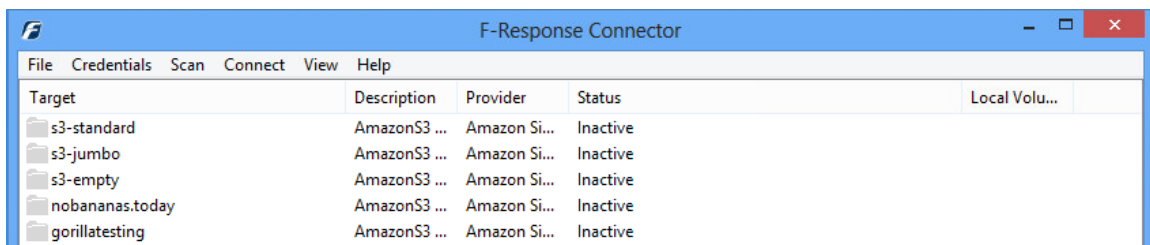
As the credential location and process for acquiring those credentials changes frequently for almost all cloud providers, including each one in this manual would quickly become obsolete. Please refer to the specific Mission Guide on the F-Response Website for details on cloud provider you are attempting to access. F-Response Mission Guides are available at <https://www.f-response.com/support/missionguides>

Scanning for Cloud Storage Targets

Use the Scan menu to enumerate cloud storage containers/buckets by service.



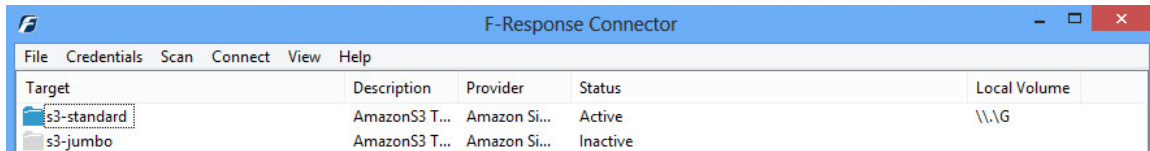
F-Response Connector Scan Cloud Storage menu



F-Response Connector scan results

Connecting to Cloud Storage Targets

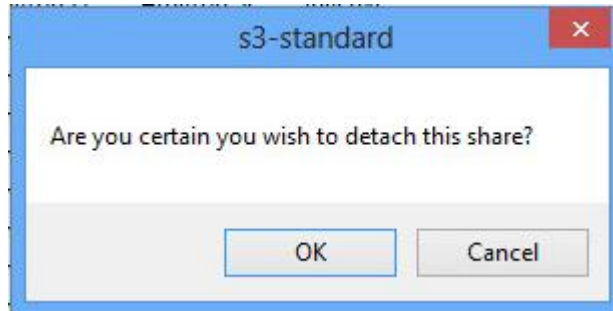
You can connect to one or more storage targets by simply double clicking on target. The newly attached volume will be assigned a drive letter and is now accessible via Windows Explorer.



Logged in Cloud Storage target assigned the G:\ drive letter

Disconnecting from Cloud Storage Targets

You can disconnect from one or more storage targets by simply double clicking on target.



Warning before detaching a connected share

F-Response Connector (Database Objects)

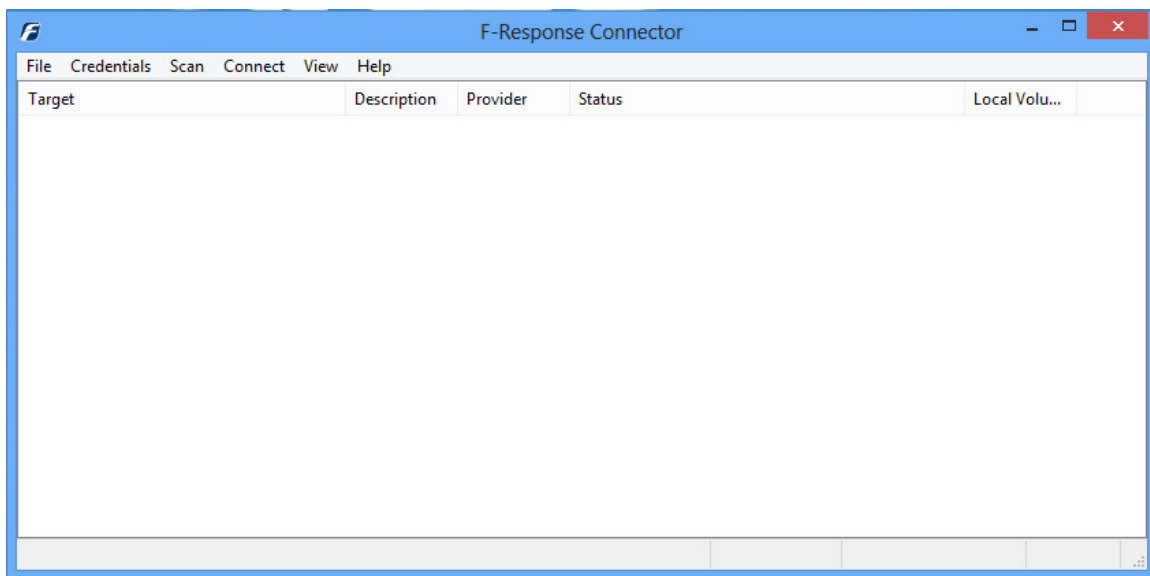
Using the F-Response Connector for Database Objects, Sharepoint 2010(TAC, CE, CE+C, and EE)

F-Response TACTICAL, Consultant, Consultant + Covert, and Enterprise edition includes a copy of the F-Response Connector (FC). The FC allows an examiner to mount remote Microsoft SQL Server Database Objects (Embedded Files, BLOBS, etc) as local read-only logical volumes or network shares.

The F-Response Connector supports Microsoft Sharepoint 2010 only at present.

The FC does not require executables or agents be deployed to the remote Microsoft SQL Server(s).

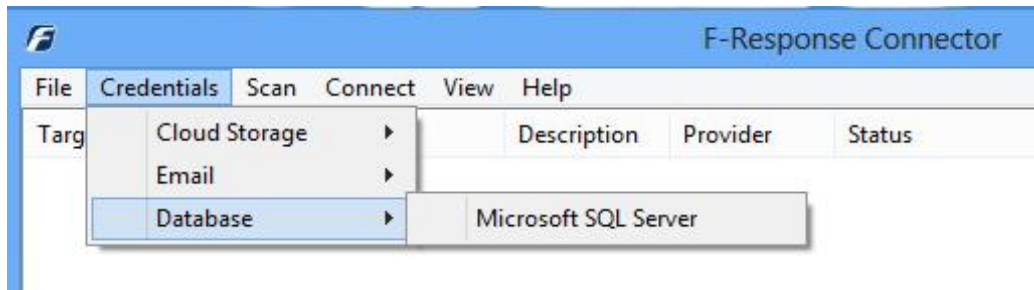
The FC does require a locally attached F-Response licensed dongle (TACTICAL, Consultant, or Consultant+Covert), or a remote Enterprise F-Response dongle connected via the F-Response License Manager at all times.



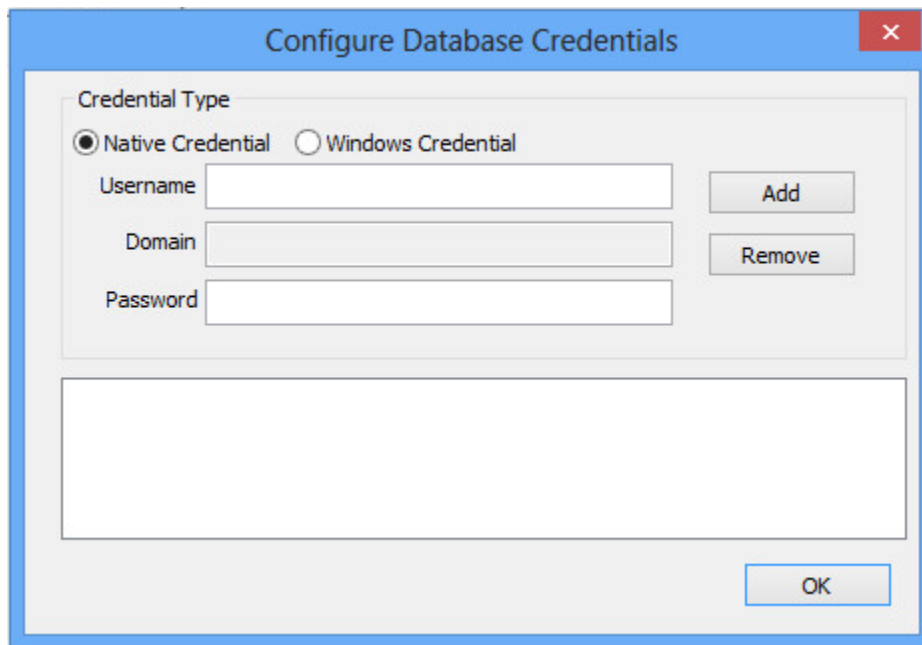
F-Response Connector

Configuring Database Server Credentials

Before you can connect to Database Server you must first input valid credentials. The current version of the FC supports Microsoft SQL Server 2010 only, however future versions will allow you to connect to other SQL based servers (including Oracle, etc). The Database Credentials dialog will allow you to enter one or more Database credentials, either Database Native Credentials (SQL Native) or Windows Domain Credentials. Database Credentials are ***not saved*** between executions of the FC.



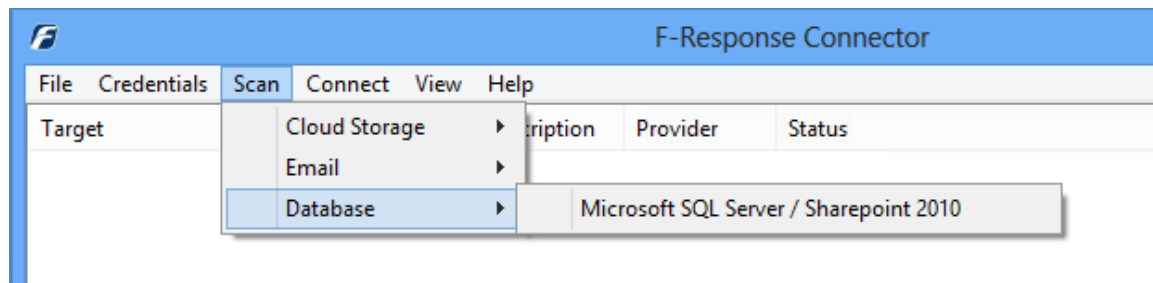
Credentials->Database...



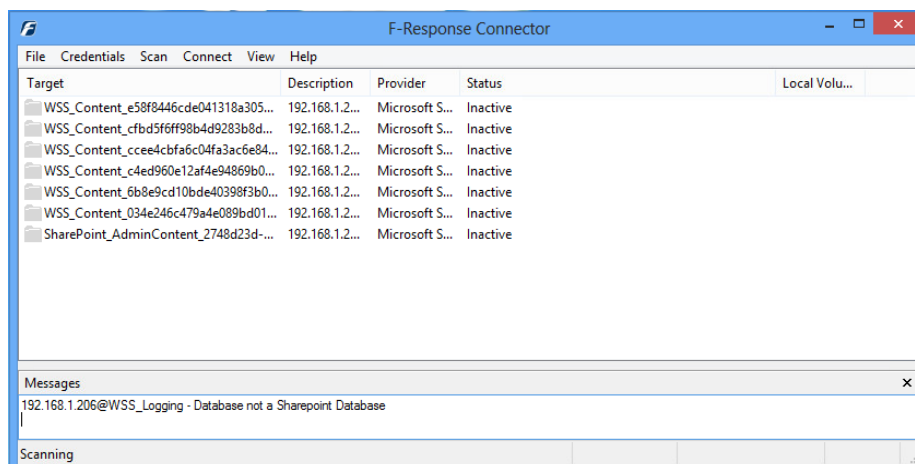
Database Credential dialog, Credentials can be either native credentials (Microsoft SQL Server Native Accounts) or Windows Credentials

Scanning for Database Object Targets

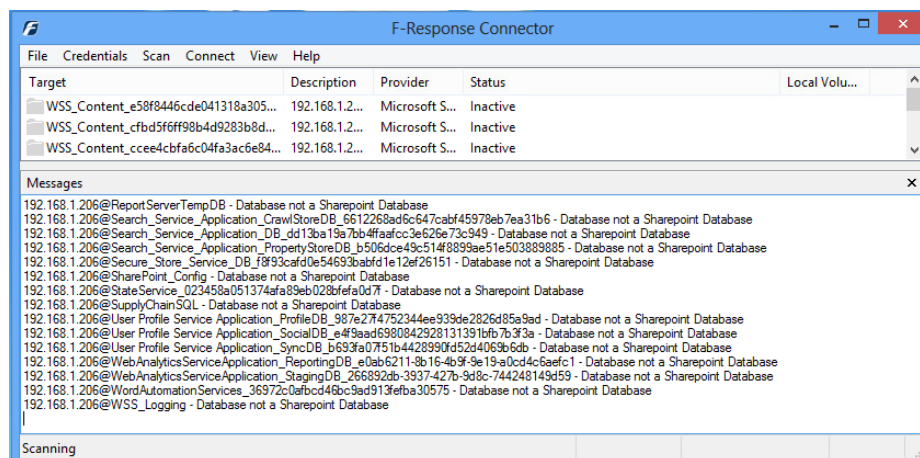
Use the Scan menu to enumerate Microsoft SQL Servers and Databases. The scanning process will use the local “plugins.xml” file to test database format and table structure. Periodically new “plugins.xml” files will be placed on the F-Response Website to add support for new Database formats and models.



Database Object Connector Scan menu



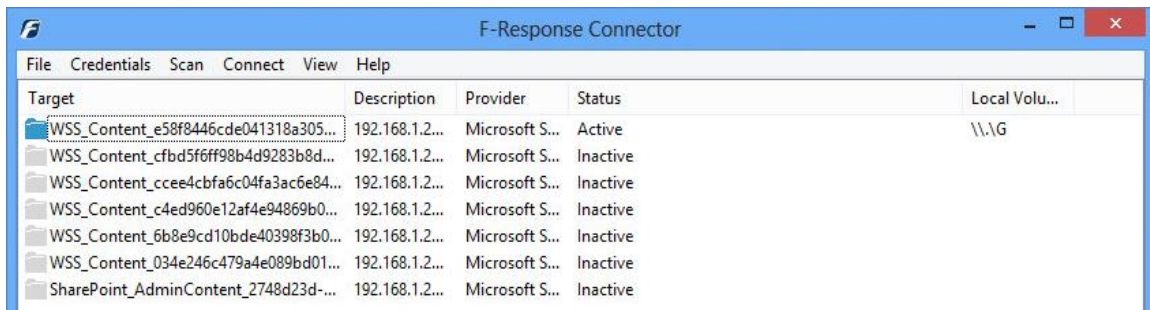
F-Response Connector scan results



Databases not recognized are listed on the Messages Panel

Connecting to Database Object Targets

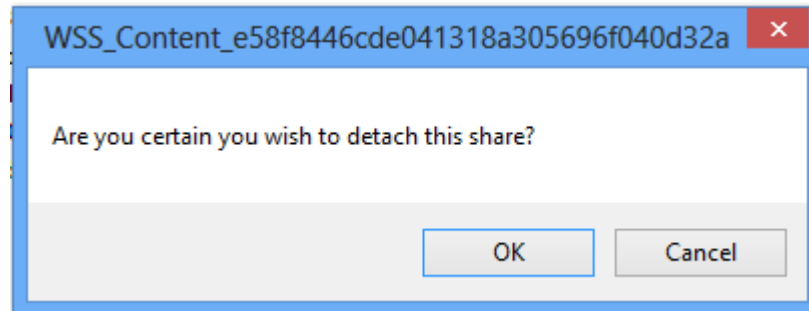
You can connect to one or more storage targets by simply double clicking on target. The newly attached volume will be assigned a drive letter and is now accessible via Windows Explorer.



Logged in Database Storage target assigned the G:\ drive letter

Disconnecting from Database Object Targets

You can disconnect from one or more storage targets by simply double clicking on target.



Warning before detaching a connected share

F-Response Connector (Email)

Using the F-Response Connector for Email (TAC, CE, CE+C, and EE)

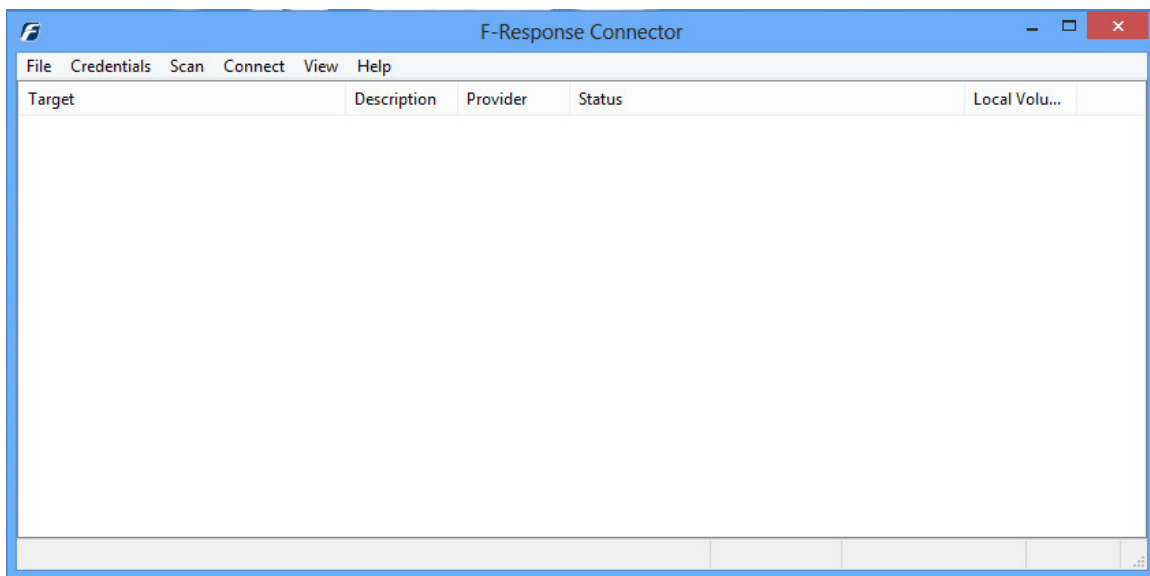
F-Response TACTICAL, Consultant, Enterprise and Consultant+Covert edition includes a copy of the F-Response Connector (FC). The FC allows an examiner to mount select remote mail items as local read-only logical volumes or network shares.

IMAP -> Individual Messages in “.eml” format, subject to provider throttling.

Office365 -> Individual Messages, Calendar Items, Contacts, and Tasks in native formats, subject to provider throttling. Additional Exchange “Distinguished Folders” are checked but may not be available under all accounts. (NOT AVAILABLE WITH TACTICAL)

The FC does not require executables or agents be deployed to the remote servers.

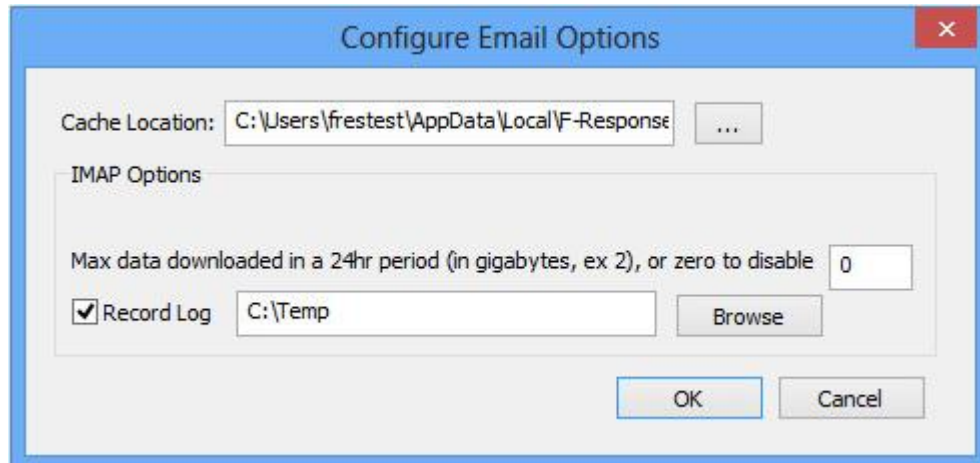
The FC does require a locally attached F-Response licensed dongle (TACTICAL, Consultant, or Consultant+Covert), or a remote Enterprise F-Response dongle connected via the F-Response License Manager at all times.



F-Response Connector

Configuring Connector Email Options

There are a number of options that can be configured when using the F-Response Connector to access Email accounts, these options include:



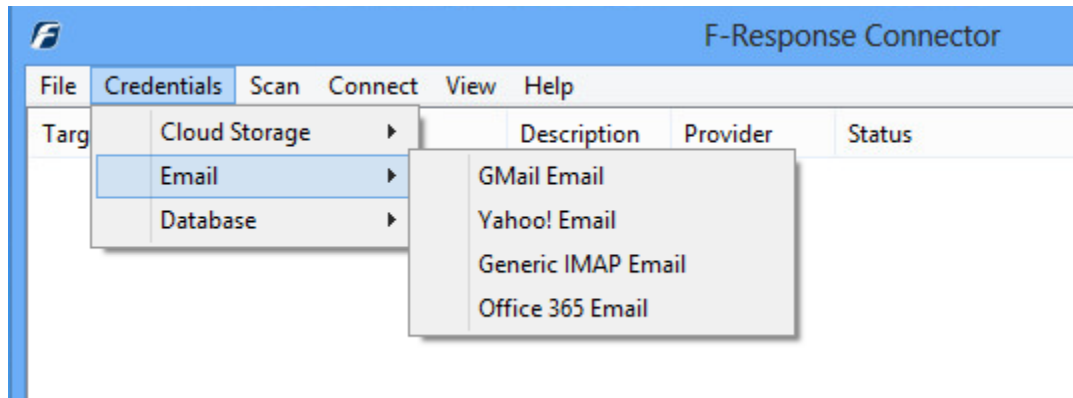
F-Response Email Connector Configure Options

- **Cache Location**
 - All Email content is cached locally, use this option to specify a location to store cache files.
- **IMAP Options**
 - **Max data downloaded in a 24hr period (in gigabytes, ex 2)**
 - Many providers restrict the total amount of data that can be downloaded in a 24hr period. For instance Google limits⁷ the total to 2.5 Gig/24hrs. By setting a limit here you enforce a soft throttle to limit the chances of account lockout. By setting this value to zero you enforce no limits and allow the data to be downloaded at the maximum possible speed.

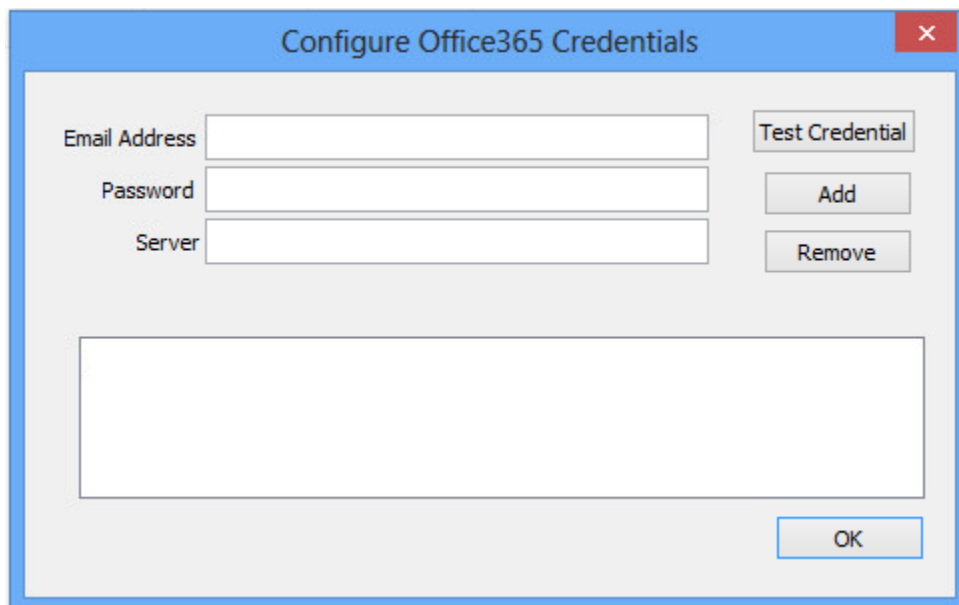
⁷ More on Google Limits can be found at <https://support.google.com/a/answer/1071518?hl=en>

Configuring Email Credentials

Before you can connect to Email service you must first input valid credentials. The FC provides access to Gmail, Yahoo! Mail, most generic IMAP servers, and Office 365 native Exchange Web Services(NOT AVAILABLE WITH TACTICAL). Credentials can be tested before they are added using the “Test Credential” button. Once the credential has been validated press the “Add” button to add them to the list of credentials to be used. Email credentials are **not saved** between executions of the FC.



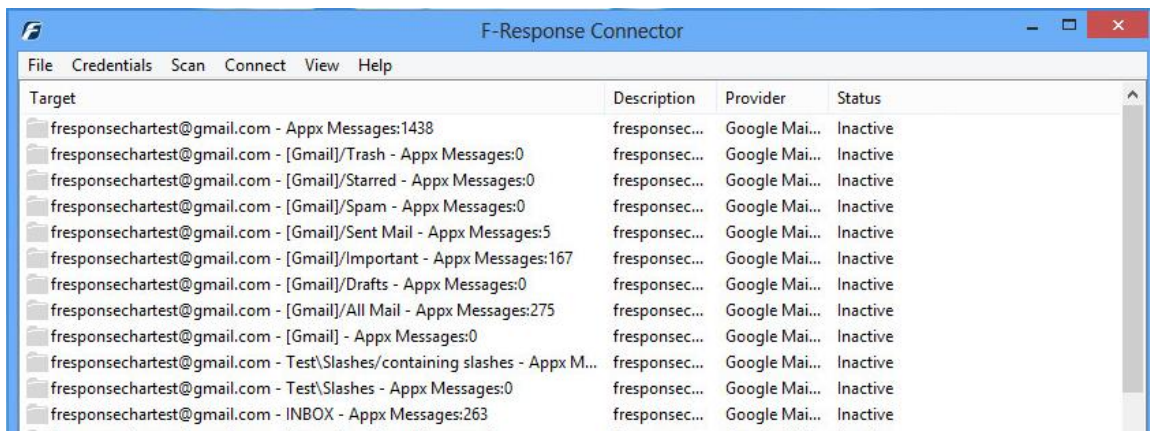
Credentials->Email...



Configure Gmail Credentials Dialog

Scanning for Email Account Targets

Use the Scan menu to enumerate Email accounts and IMAP Mailboxes.



The screenshot shows the F-Response Connector application window. The menu bar includes File, Credentials, Scan, Connect, View, and Help. The main area displays a table of scan results for the target email account fresponsechartest@gmail.com. The table has four columns: Target, Description, Provider, and Status. The results show various email folders and their approximate message counts, all with a status of Inactive.

Target	Description	Provider	Status
fresponsechartest@gmail.com - Appx Messages:1438	fresponsec...	Google Mai...	Inactive
fresponsechartest@gmail.com - [Gmail]/Trash - Appx Messages:0	fresponsec...	Google Mai...	Inactive
fresponsechartest@gmail.com - [Gmail]/Starred - Appx Messages:0	fresponsec...	Google Mai...	Inactive
fresponsechartest@gmail.com - [Gmail]/Spam - Appx Messages:0	fresponsec...	Google Mai...	Inactive
fresponsechartest@gmail.com - [Gmail]/Sent Mail - Appx Messages:5	fresponsec...	Google Mai...	Inactive
fresponsechartest@gmail.com - [Gmail]/Important - Appx Messages:167	fresponsec...	Google Mai...	Inactive
fresponsechartest@gmail.com - [Gmail]/Drafts - Appx Messages:0	fresponsec...	Google Mai...	Inactive
fresponsechartest@gmail.com - [Gmail]/All Mail - Appx Messages:275	fresponsec...	Google Mai...	Inactive
fresponsechartest@gmail.com - [Gmail] - Appx Messages:0	fresponsec...	Google Mai...	Inactive
fresponsechartest@gmail.com - Test\Slashes/containing slashes - Appx M...	fresponsec...	Google Mai...	Inactive
fresponsechartest@gmail.com - Test\Slashes - Appx Messages:0	fresponsec...	Google Mai...	Inactive
fresponsechartest@gmail.com - INBOX - Appx Messages:263	fresponsec...	Google Mai...	Inactive

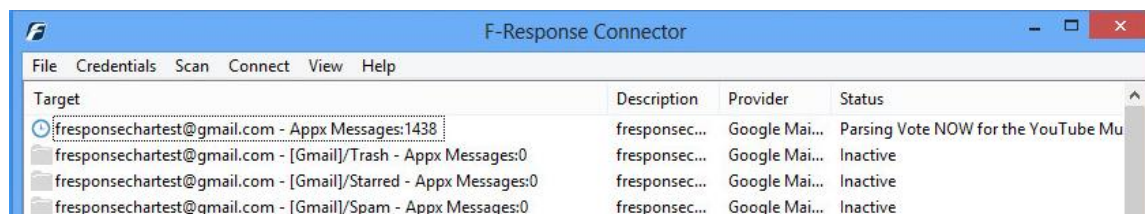
F-Response Connector scan results

Connecting to Email Account Targets

You can connect to one or more storage targets by simply double clicking on target. The newly attached volume will be assigned a drive letter and is now accessible via Windows Explorer.

The FC will begin processing the remote email and building a local cache. This process may be stopped at any time double clicking on the “clock icon”. Cancelled processes are restarted on the next “Login...” operation. The processing phase can take a considerable amount of time depending on the total number of messages, size of the messages, available bandwidth, and any throttling of performance done by the email provider. A running output of the message subjects will be shown in the Status column.

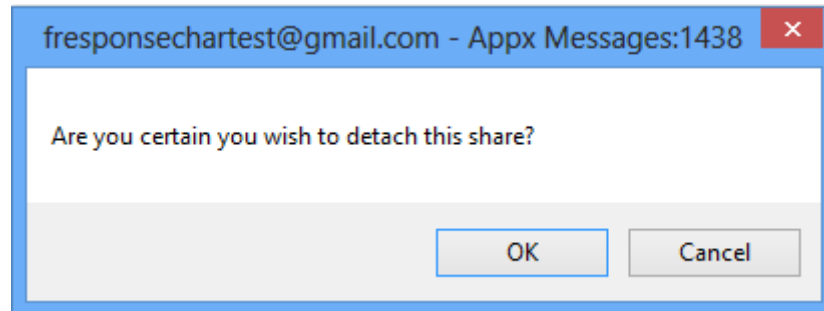
Once complete, the newly attached volume will be assigned a drive letter and is now accessible via Windows Explorer.



Processing email in an account

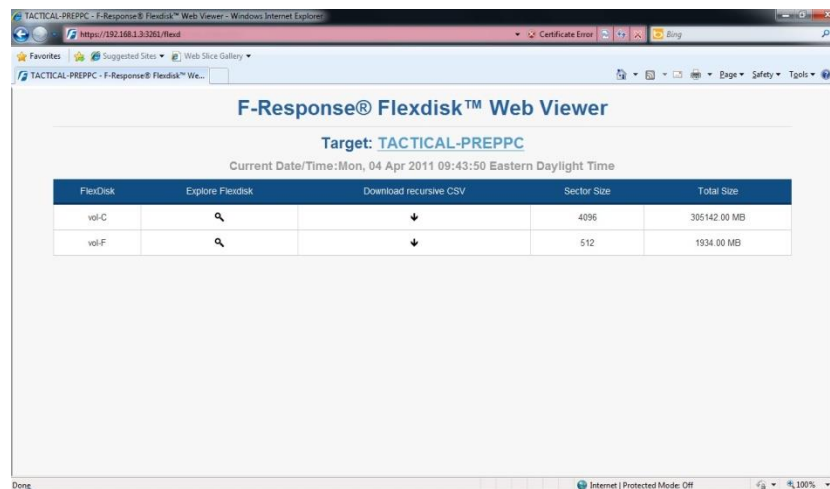
Disconnecting from Email Account Targets

You can disconnect from one or more storage targets by simply double clicking on target.



Warning before detaching a connected share

F-Response Flexdisk™



F-Response Flexdisk™ Web Viewer

What is a F-Response Flexdisk™?

The F-Response Flexdisk® (Patented) is a web based disk access and representation tool. The Flexdisk™ uses standard web technologies (HTTPS/REST⁸) to provide direct access to the remote target machines Logical and Physical targets in both raw and logical format. The Flexdisk™ can be accessed and used from any modern web browser and also exposes a feature rich and extensible application programming interface (API) accessible from any system capable of making and interpreting web queries and JSON⁹.

How do I access and use a F-Response Flexdisk™?

Using the F-Response Flexdisk™ is as easy as working with a web browser. The Flexdisk™ web viewer interface contains multiple icons as well as a clearly defined legend to cover their usage and meaning. A sample of that legend appears below:

Legend: Please review the following legend for resource states.

Download recursive CSV of directory contents	Allocated Directory	Allocated File
Download CSV of an individual file's metadata	Unallocated Directory	Unallocated File

⁸ REST or Representational State Transfer is a web services development model that uses simple HTTP verbs such as GET and POST.

⁹ JSON or Javascript Object Notation is a data formatting style considered smaller and easier to manipulate when compared to XML.

In addition to using the provided web viewer, the F-Response Flexdisk™ provides a rich and capable web services API that can be used to build mobile and web based applications that leverage F-Response Flexdisk™ provided content.

Frequently Asked Questions

1. [Q\) Do I change any data on the target computer by using F-Response?](#)
2. [Q\) I am connected via F-Response. I navigated to a file on the remote computer, hit delete, and it appears to be gone. Did I really delete the file?](#)
3. [Q\) I have a personal firewall running on my computers. Do I need to change firewall settings to use F-Response?](#)
4. [Q\) I have a remote user that accidentally deleted a file. Can I use F-Response to recover deleted files?](#)
5. [Q\) Is the F-Response iSCSI connection encrypted?](#)
6. [Q\) Does F-Response work as an agent?](#)
7. [Q\) I established an F-Response connection, tried to view the remote “Documents and Settings” folder and received a message that I don’t have permission to view that folder. Why don’t I have access?](#)

1. **Q) Do I change any data on the target computer by using F-Response?**

A) Once the F-Response Target code is executed and the network connection is established, the practitioner conducting the analysis cannot edit or alter data on the machine under inspection via the F-Response connection. Executing or starting the F-Response service does, of course, effect some change to the target computer, but the changes are about as minimal as they can be for analysis that is being conducted on a live machine.

2. **Q) I am connected via F-Response. I navigated to a file on the remote computer, hit delete, and it appears to be gone. Did I really delete the file?**

A) No, you didn’t delete the file. You cannot delete files, alter Meta data, or effect any other changes on the machine under inspection using F-Response. What you did do was fool your analysis machine into “believing” that the file is deleted and thus your analysis machine is no longer presenting the file to you as available.

3. **Q) I have a personal firewall running on my computers. Do I need to change firewall settings to use F-Response?**

A) Possibly, F-Response does create temporary exceptions in the Windows Firewall during execution. Furthermore these exceptions are removed when the application exits. However, if you are using a firewall other than the Microsoft Windows Firewall, you may need to set an exception. F-Response machines must be able to send and receive on port 3260 (this default is changeable). We recommend disabling the firewall for the duration of the session during ad hoc usage (e.g. temporary consultant use at a third party site), and tuning the firewall configurations to allow F-Response connectivity for planned enterprise deployment.

4. **Q)** I have a remote user that accidentally deleted a file. Can I use F-Response to recover deleted files?

A) F-Response will enable you to use your recovery tool of choice to recover the file(s) to a location other than the target machine. You cannot restore the file directly to the target machine via F-Response because you do not have write capability on that machine, but you can recover the file and make it available to the user via email , network share, etc.

5. **Q)** Is the F-Response iSCSI connection encrypted?

A) By default, no. However AES 256 bit Encryption is available in F-Response Enterprise edition. Alternatively, there are native methods to accomplish this, if needed. E.g. using Microsoft IPsec policy manager you can create a configuration to enforce an IPsec policy in your enterprise governing ports 3260, or whatever port you have elected to use with F-Response. This could be used to force F-Response to be used over an IPsec tunnel, and thus allow you to have the F-Response service start automatically with each boot. If F-Response is being used over the Internet and corporate policy dictates encryption over public networks, then the existing corporate VPN capability should satisfy the encryption policy.

6. **Q)** Does F-Response work as an agent?

A) No. It does not collect or store any data on the machine under inspection. It does not report to a management server. It does not have an inherent analysis or reporting capability.

7. **Q)** I established an F-Response connection, tried to view the remote “Documents and Settings” folder and received a message that I don’t have permission to view that folder. Why don’t I have access?

A) You have the access with the right tools. You probably used Windows Explorer or an equivalent tool that is subject to the file permission settings for those folders. If you use a forensics tool that can take advantage of your raw drive access, then you won’t have this issue.

Support

Didn't find what you're looking for in the manual? Many of our customers find that our growing selection of brief tutorial videos offers the information to meet their immediate needs:

<https://www.f-response.com/support/videos>

At the time of this writing, available tutorials include:

- Using F-Response TACTICAL for Windows
- Using F-Response TACTICAL for Apple
- Using F-Response TACTICAL for Linux

We take pride in providing prompt attention to your support needs, and will support your F-Response product for the period of your license term. F-Response support can be reached via

Email: support@f-response.com

Website: <https://www.f-response.com>

Software and documentation updates will be made available for download to registered users on the F-Response web site. E-mail support is available to licensed software users. We typically respond to your queries within 1 business day of receiving your request.

Appendix D - Master Software License Agreement

AGILE RISK MANAGEMENT LLC MASTER SOFTWARE LICENSE AGREEMENT

TERMS AND CONDITIONS

1. Scope of Agreement; Definitions. This Agreement covers the license and permitted use of the Agile Risk Management LLC (“Agile”) F-Response Software. Unless otherwise defined in this section, the capitalized terms used in this Agreement shall be defined in the context in which they are used. The following terms shall have the following meanings:

1.1. “Agile Software” or “Software” means any and all versions of Agile’s F-Response software.

1.2. “Customer” means the person or entity identified on the invoice and only such person or entity, Customer shall not mean any assigns, heirs, or related persons or entities or claimed third-party beneficiaries of the Customer.

1.3. “Documentation” means Agile release notes or other similar instructions in hard copy or machine readable form supplied by Agile to Customer that describes the functionality of the Agile Software

1.4. “License Term” means the term of the applicable license as specified on an invoice or as set forth in this Agreement.

2. Grant of Software License.

2.1. Enterprise License. Subject to the terms and conditions of this Agreement only, Agile grants Customer a non-exclusive, non-transferable license to install the Agile Software and to use the Agile Software during the License Term, in object code form only.

2.2. Third Party Software. Customer acknowledges that the Agile Software may include or require the use of software programs created by third parties, and the Customer acknowledges that its use of such third party software programs shall be governed exclusively by the third party’s applicable license agreement.

3. Software License Restrictions.

3.1. No Reverse Engineering; Other Restrictions. Customer shall not, directly or indirectly: (i) sell, license, sublicense, lease, redistribute or transfer any Agile Software; (ii) modify, translate, reverse engineer, decompile, disassemble, create derivative works based on, or distribute any Agile Software; (iii) rent or lease any rights in any Agile Software in any form to any entity; (iv) remove, alter or obscure any proprietary notice, labels or marks on any Agile Software. Customer is responsible for all use of the Software and for compliance with this Agreement and any applicable third party software license agreement.

3.2. Intellectual Property. Agile retains all title, patent, copyright and other intellectual proprietary rights in, and ownership of, the Agile Software regardless of the type of access or media upon which the original or any copy may be recorded or fixed. Unless otherwise expressly stated herein, this Agreement does not transfer to Customer any title, or other ownership right or interest in any Agile Software. Customer does not acquire any rights, express or implied, other than those expressly granted in this Agreement.

4. Ordering & Fulfillment. Pricing is set forth on the F-Response website and is subject to change at any time. Each order shall be subject to Agile’s reasonable acceptance. Delivery terms are FOB Agile’s shipping point.

5. Payments. Customer agrees to pay amounts invoiced by Agile for the license granted under this Agreement. If any authority imposes a duty, tax or similar levy (other than taxes based on Agile’s income), Customer agrees to pay, or to promptly reimburse Agile for, all such amounts. Unless otherwise indicated in an invoice, all Agile invoices are payable thirty (30) days from the date of the invoice. Agile reserves the right to charge and Customer agrees to pay Agile for every unauthorized copy or unauthorized year an amount equal to the cost per copy, per year, per computer, or per user, whichever is greater, as a late payment fee in the event Customer fails to remit payments when due or Customer otherwise violates the payment provisions of this Agreement. In addition to any other rights set forth in this Agreement, Agile may suspend performance or withhold fulfilling new Customer orders in the event Customer has failed to timely remit payment for outstanding and past due invoices.

6. Confidentiality.

6.1. Definition. “Confidential Information” means: (a) any non-public technical or business information of a party, including without limitation any information relating to a party’s techniques, algorithms, software, know-how, current and future products and services, research, engineering, vulnerabilities, designs, financial information,

procurement requirements, manufacturing, customer lists, business forecasts, marketing plans and information; (b) any other information of a party that is disclosed in writing and is conspicuously designated as “Confidential” at the time of disclosure or that is disclosed orally and is identified as “Confidential” at the time of disclosure; or (c) the specific terms and conditions of this Agreement.

6.2. Exclusions. Confidential Information shall not include information which: (i) is or becomes generally known to the public through no fault or breach of this Agreement by the receiving Party; (ii) the receiving Party can demonstrate by written evidence was rightfully in the receiving Party’s possession at the time of disclosure, without an obligation of confidentiality; (iii) is independently developed by the receiving Party without use of or access to the disclosing Party’s Confidential Information or otherwise in breach of this Agreement; (iv) the receiving Party rightfully obtains from a third party not under a duty of confidentiality and without restriction on use or disclosure, or (v) is required to be disclosed pursuant to, or by, any applicable laws, rules, regulatory authority, court order or other legal process to do so, provided that the Receiving Party shall, promptly upon learning that such disclosure is required, give written notice of such disclosure to the Disclosing Party.

6.3. Obligations. Each Party shall maintain in confidence all Confidential Information of the disclosing Party that is delivered to the receiving Party and will not use such Confidential Information except as expressly permitted herein. Each Party will take all reasonable measures to maintain the confidentiality of such Confidential Information, but in no event less than the measures it uses to protect its own Confidential Information. Each Party will limit the disclosure of such Confidential Information to those of its employees with a bona fide need to access such Confidential Information in order to exercise its rights and obligations under this Agreement provided that all such employees are bound by a written non-disclosure agreement that contains restrictions at least as protective as those set forth herein.

6.4. Injunctive Relief. Each Party understands and agrees that the other Party will suffer irreparable harm in the event that the receiving Party of Confidential Information breaches any of its obligations under this section and that monetary damages will be inadequate to compensate the non-breaching Party. In the event of a breach or threatened breach of any of the provisions of this section, the non-breaching Party, in addition to and not in limitation of any other rights, remedies or damages available to it at law or in equity, shall be entitled to a temporary restraining order, preliminary injunction and/or permanent injunction in order to prevent or to restrain any such breach by the other Party.

7. DISCLAIMER OF WARRANTIES. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, AGILE AND ITS SUPPLIERS PROVIDE THE SOFTWARE AND SUPPORT SERVICES (IF ANY) AS IS AND WITH ALL FAULTS, AND HEREBY DISCLAIM ALL OTHER WARRANTIES AND CONDITIONS, WHETHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING, BUT NOT LIMITED TO, ANY (IF ANY) IMPLIED WARRANTIES, DUTIES OR CONDITIONS OF MERCHANTABILITY, OF FITNESS FOR A PARTICULAR PURPOSE, OF RELIABILITY OR AVAILABILITY, OF ACCURACY OR COMPLETENESS OF RESPONSES, OF RESULTS, OF WORKMANLIKE EFFORT, OF LACK OF VIRUSES, AND OF LACK OF NEGLIGENCE, ALL WITH REGARD TO THE SOFTWARE, AND THE PROVISION OF OR FAILURE TO PROVIDE SUPPORT OR OTHER SERVICES, INFORMATION, SOFTWARE, AND RELATED CONTENT THROUGH THE SOFTWARE OR OTHERWISE ARISING OUT OF THE USE OF THE SOFTWARE. ALSO, THERE IS NO WARRANTY OR CONDITION OF TITLE, QUIET ENJOYMENT, QUIET POSSESSION, CORRESPONDENCE TO DESCRIPTION OR NON-INFRINGEMENT WITH REGARD TO THE SOFTWARE.

8. Limitations and Exclusions.

8.1. Limitation of Liability and Remedies. NOTWITHSTANDING ANY DAMAGES THAT YOU MIGHT INCUR FOR ANY REASON WHATSOEVER (INCLUDING, WITHOUT LIMITATION, ALL DAMAGES REFERENCED ABOVE AND ALL DIRECT OR GENERAL DAMAGES IN CONTRACT OR ANY OTHER THEORY IN LAW OR IN EQUITY), THE ENTIRE LIABILITY OF AGILE AND ANY OF ITS SUPPLIERS UNDER ANY PROVISION OF THIS AGREEMENT AND YOUR EXCLUSIVE REMEDY HEREUNDER SHALL BE LIMITED TO THE TOTAL AMOUNT PAID BY CUSTOMER FOR THE LICENSE. THE FOREGOING LIMITATIONS, EXCLUSIONS AND DISCLAIMERS SHALL APPLY TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, EVEN IF ANY REMEDY FAILS ITS ESSENTIAL PURPOSE.

8.2. Exclusion of Incidental, Consequential and Certain Other Damages. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL AGILE OR ITS SUPPLIERS BE LIABLE FOR ANY SPECIAL, INCIDENTAL, PUNITIVE, INDIRECT, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF PROFITS OR CONFIDENTIAL OR OTHER INFORMATION, FOR BUSINESS INTERRUPTION, FOR PERSONAL INJURY, FOR LOSS OF PRIVACY, FOR FAILURE TO MEET ANY DUTY INCLUDING OF GOOD FAITH OR OF REASONABLE CARE, FOR NEGLIGENCE, AND FOR ANY OTHER PECUNIARY OR OTHER LOSS WHATSOEVER) ARISING OUT OF OR IN ANY WAY RELATED TO THE USE OF OR INABILITY TO USE THE SOFTWARE, THE PROVISION OF OR FAILURE TO PROVIDE SUPPORT OR OTHER SERVICES, INFORMATION, SOFTWARE, AND RELATED CONTENT THROUGH THE SOFTWARE OR OTHERWISE ARISING OUT OF THE USE OF THE SOFTWARE, OR OTHERWISE UNDER OR IN CONNECTION WITH ANY PROVISION OF THIS AGREEMENT, EVEN IN THE EVENT OF THE FAULT, TORT (INCLUDING NEGLIGENCE), MISREPRESENTATION, STRICT LIABILITY, BREACH OF CONTRACT OR BREACH OF WARRANTY OF AGILE OR ANY SUPPLIER, AND EVEN IF AGILE OR ANY SUPPLIER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT WILL EITHER PARTY BE LIABLE TO THE OTHER PARTY OR TO ANY THIRD PARTY FOR ANY INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL, DAMAGES (INCLUDING WITHOUT LIMITATION,

LIABILITIES RELATED TO A LOSS OF USE, PROFITS, GOODWILL OR SAVINGS OR A LOSS OR DAMAGE TO ANY SYSTEMS, RECORDS OR DATA), WHETHER SUCH LIABILITY ARISES FROM ANY CLAIM BASED UPON CONTRACT, WARRANTY, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY OR OTHERWISE, EVEN IF ADVISED IN ADVANCE OR AWARE OF THE POSSIBILITY OF ANY SUCH LOSS OR DAMAGE.

9. Verification. Agile has the right to request Customer complete a self-audit questionnaire in a form provided by Agile. If an audit reveals unlicensed use of the Agile Software, Customer agrees to promptly order and pay for licenses to permit all past and ongoing usage.

10. Support Services

10.1. Rights and Obligations. This Agreement does not obligate Agile to provide any support services or to support any software provided as part of those services. If Agile does provide support services to you, use of any such support services is governed by the Agile policies and programs described in the user manual, in online documentation, on Agile's support webpage, or in other Agile-provided materials. Any software Agile may provide you as part of support services are governed by this Agreement, unless separate terms are provided.

10.2. Consent to Use of Data. You agree that Agile and its affiliates may collect and use technical information gathered as part of the support services provided to you, if any, related to the Software. Agile may use this information solely to improve our products or to provide customized services or technologies to you and will not disclose this information in a form that personally identifies you.

11. Miscellaneous.

11.1. Legal Compliance; Restricted Rights. Each Party agrees to comply with all applicable Laws. Without limiting the foregoing, Customer agrees to comply with all U.S. export Laws and applicable export Laws of its locality (if Customer is not located in the United States), and Customer agrees not to export any Software or other materials provided by Agile without first obtaining all required authorizations or licenses. In the event the Software is provided to the United States government it is provided with only "LIMITED RIGHTS" and "RESTRICTED RIGHTS" as defined in FAR 52.227-14 if the commercial terms are deemed not to apply.

11.2. Governing Law; Severability. This Agreement (including any addendum or amendment to this Agreement which is included with the Software) are the entire agreement between you and Agile relating to the Software and the support services (if any) and they supersede all prior or contemporaneous oral or written communications, proposals and representations with respect to the Software or any other subject matter covered by this Agreement. To the extent the terms of any Agile policies or programs for support services conflict with the terms of this Agreement, the terms of this Agreement shall control. This Agreement shall be governed by the laws of the State of Florida, USA, without regard to choice-of-law provisions. You and Agile agree to submit to the personal and exclusive jurisdiction of the Florida state court located in Tampa Florida and the United States District Court for the Middle District of Florida. If any provision of this Agreement is held to be illegal or unenforceable for any reason, then such provision shall be deemed to be restated so as to be enforceable to the maximum extent permissible under law, and the remainder of this Agreement shall remain in full force and effect. Customer and Agile agree that this Agreement shall not be governed by the U.N. Convention on Contracts for the International Sale of Goods.

11.3. Notices. Any notices under this Agreement will be personally delivered or sent by certified or registered mail, return receipt requested, or by nationally recognized overnight express courier, to the address specified herein or such other address as a Party may specify in writing. Such notices will be effective upon receipt, which may be shown by confirmation of delivery.

11.4. Assignment. Customer may not assign or otherwise transfer this Agreement without the Agile's prior written consent, which consent shall not be unreasonably withheld, conditioned or delayed. This Agreement shall be binding upon and inure to the benefit of the Parties' successors and permitted assigns, if any.

11.5. Force Majeure. Neither Party shall be liable for any delay or failure due to a force majeure event and other causes beyond its reasonable control. This provision shall not apply to any of Customer's payment obligations.

11.6. Redistribution Compliance.

(a) F-Response distributes software libraries developed by The Sleuth Kit ("TSK"). The license information and source code for TSK can be found at <http://www.sleuthkit.org/>. If any changes have been made by Agile to the TSK libraries distributed with the F-Response software, those changes can be found online at <http://www.f-response.com/TSKinfo>.

(b) A portion of the F-Response Software was derived using source code provided by Intel and Alistair Crooks (NetBSD), which requires the following notice be posted herein, and which applies only to the source code. F-Response code is distributed only in binary or object code form. F-Response source code, and any revised Intel and NetBSD code contained within the F-Response source code, is not available for distribution. The name of Intel Corporation and NetBSD are not being used to endorse or promote this product, nor is the name of the author being used to endorse or promote this product. This information is presented solely to comply with the required Intel and NetBSD license agreements which require reproduction of the following copyright notice, list of conditions and disclaimer:

Intel License Agreement

Copyright (c) 2000, Intel Corporation

All rights reserved.

- Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

- The name of Intel Corporation may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL INTEL OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright © 2006 Alistair Crooks. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

11.7. General. This Agreement, including its exhibits (all of which are incorporated herein), are collectively the Parties' complete agreement regarding its subject matter, superseding any prior oral or written communications. Amendments or changes to this Agreement must be in mutually executed writings to be effective. The Parties agree that, to the extent any Customer purchase or sales order contains terms or conditions that conflict with, or supplement, this Agreement, such terms and conditions shall be void and have no effect, and the provisions of this Agreement shall control. Unless otherwise expressly set forth in an exhibit that is executed by the Parties, this Agreement shall control in the event of any conflict with an exhibit. Sections 2, 3, 5, 7, 8, and 9, and all warranty disclaimers, use restrictions

and provisions relating to Agile's intellectual property ownership, shall survive the termination or expiration of this Agreement. The Parties are independent contractors for all purposes under this Agreement.

11.8. Changes to this agreement. Agile will only enter into changes to this agreement (Agile's MSLA) based on a one off administration fee of US\$8,000. The fee must be paid in advance of any changes. For purchases of over US\$100,000 this fee may be waived.

Appendix E - Legal Notices

Legal Notice

Copyright © 2015 Agile Risk Management, LLC. All rights reserved.

This document is protected by copyright with all rights reserved.

Trademarks

F-Response is a trademark of Agile Risk Management, LLC. All other product names or logos mentioned herein are used for identification purposes only, and are the trademarks of their respective owners.

Statement of Rights

Agile Risk Management, LLC products incorporate technology that is protected by U.S. patent and other intellectual property (IP) rights owned by Agile Risk Management LLC, and other rights owners. Use of these products constitutes your legal agreement to honor Agile Risk Management, LLC's IP rights as protected by applicable laws. Reverse engineering, de-compiling, or disassembly of Agile Risk Management, LLC products is strictly prohibited.

Disclaimer

While Agile Risk Management LLC has committed its best efforts to providing accurate information in this document, we assume no responsibility for any inaccuracies that may be contained herein, and we reserve the right to make changes to this document without notice.

Patents

F-Response is covered by United States Patent Numbers: 8,171,108; 7,899,882; and other Patents Pending.