F-Response Mission Guide
Connecting to Linux target(s) using F-Response Consultant Edition
Rev 1.0
January 8, 2014

Email:support@f-response.com
Website:www.f-response.com

Phone: 1-800-317-5497

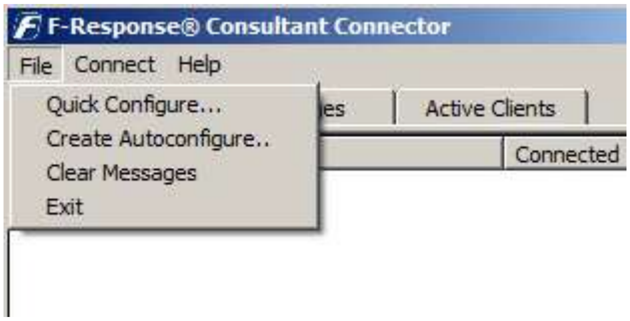
Your Mission: Connect to a remote Linux target(s) disk using F-Response Consultant Edition.

Note: This guide assumes you have installed F-Response Consultant Edition, your F-Response licensing dongle is plugged into your analyst machine, the F-Response License Manager Monitor is installed and running, and the F-Response Consultant Connector (FCC) has been started. For more information, please reference the F-Response User Manual or the F-Response Consultant Edition Training Video on the F-Response Website.

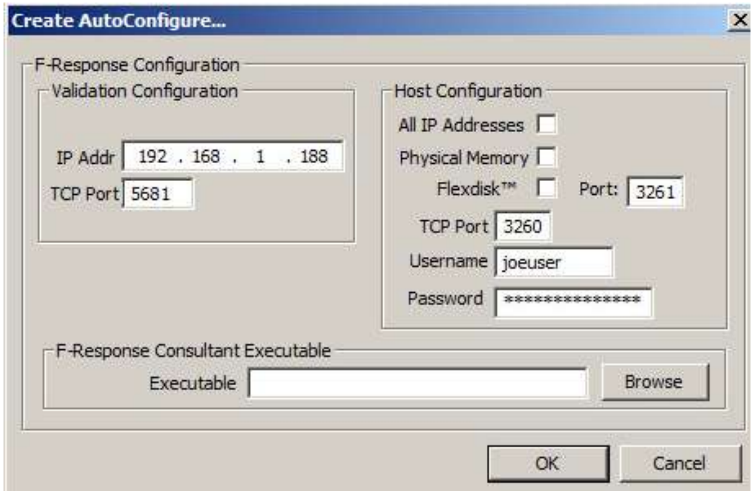
F-Response supports Linux glibc 2.3.5+ Intel/i386

Step 1: Create a Bundle

There are a few ways to deploy F-Response to a Linux target machine(s), but for our mission we'll use the option to create an autoconfiguration bundle. Start the F-Response Consultant Connector on your examiner machine and go to File- Create Autoconfigure..



The Automatic Configuration window will appear:



IP Addr 192 . 168 . 1 . 188
TCP Port 5681

All IP Addresses □
Physical Memory □
Flexdisk™ □ Port: 3261
TCP Port 3260
Username joeuser
Password ***************

Executable

Under Validation Configuration, verify the IP address of your analyst machine (where the F-Response license dongle is plugged in and the Licensing Manager is running) and leave the default port at 5681.

Next, under Host Configuration, Create an F-Response username and password—go ahead, make it anything you would like. Again, leave the default port at 3260.

There are three check box options here as well. None of them are really applicable to what we are looking to accomplish here, so they can be ignored. Click OK to save the resulting autoconfiguration file (fresponse.ini).

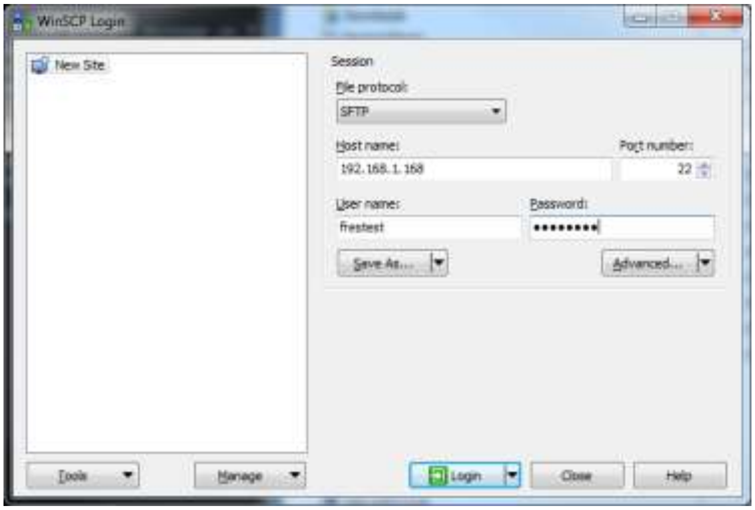
Lastly, we'll need to choose the F-Response Consultant executable "f-response-ce". If you installed F-Response with the default settings this file can be found in the Program Files\F-Response\F-Response Consultant Edition directory.

Step 2: Distribute the bundle

Once you have finished creating the fresponse.ini file, you'll want to couple it with the Linux 'f-response-ce-e-lin' executable (note there is a 64 bit version for x64 target machines: f-response-ce-e-lin-64, both are located in the default directory for F-Response Consultant Edition, see above) and make it available to your Linux target machine(s). You can do this however you would like by copying both files to a CD, USB thumb drive or network share as an example of some the most common options.

However, working from the comfort of our chair, we are going to use a free tool called WinSCP to distribute the file to our Linux target(s) over the network. If you don't have WinSCP installed, you can download and install it from here.

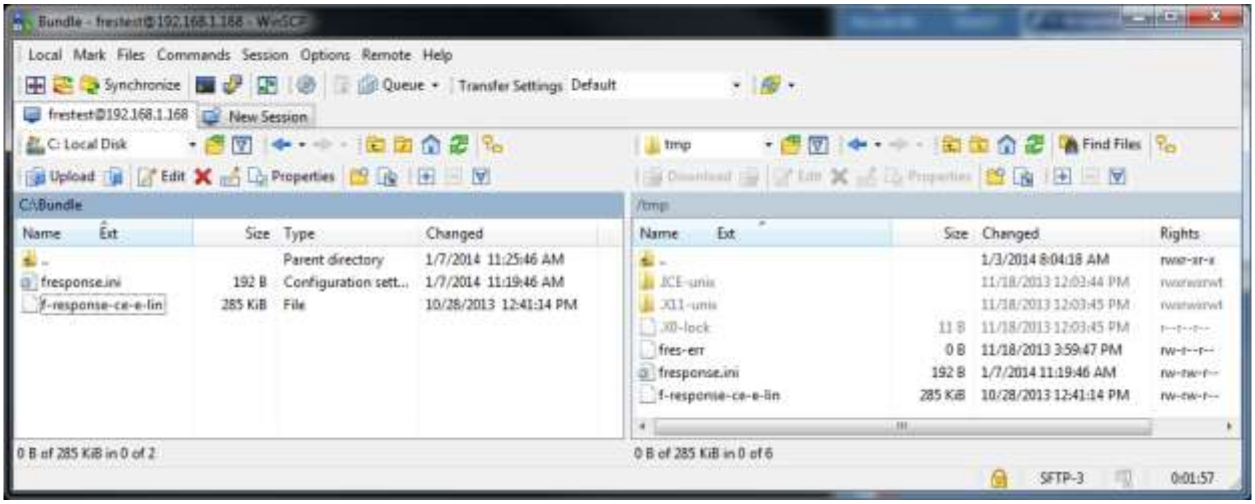
Start up WinSCP and you will be greeted with a Login Window:



File protocol: SFTP
Host name: 192.168.1.168
Port number: 22
User name: frestest
Password: •••••••••

Here you can enter the IP or Host name for the Linux target machine into the Host name field. Fill in the login and password for your target machine and click the Login button.

After connecting you'll be greeted with a file copy dialog that resembles the Windows Explorer interface.


Bundle - frestest@192.168.1.168 - WinSCP
Local Mark Files Commands Session Options Remote Help
Synchronize
Queue
Transfer Settings Default
frestest@192.168.1.168
New Session
C: Local Disk
tmp
Find Files
Upload
Edit
Properties
Download
SFTP-3
0:01:57

C:\Bundle

Name	Ext	Size	Type	Changed
..			Parent directory	1/7/2014 11:25:46 AM
fresponse.ini		192 B	Configuration sett...	1/7/2014 11:19:46 AM
f-response-ce-e-lin		285 KiB	File	10/28/2013 12:41:14 PM

0 B of 285 KiB in 0 of 2

/tmp

Name	Ext	Size	Changed	Rights
..			1/3/2014 8:04:18 AM	rwxr-xr-x
.ICE-unix			11/18/2013 12:03:44 PM	rwxrwxrwt
.X11-unix			11/18/2013 12:03:45 PM	rwxrwxrwt
.X0-lock		11 B	11/18/2013 12:03:45 PM	r--r--r--
fres-err		0 B	11/18/2013 3:59:47 PM	rw-r--r--
fresponse.ini		192 B	1/7/2014 11:19:46 AM	rw-rw-r--
f-response-ce-e-lin		285 KiB	10/28/2013 12:41:14 PM	rw-rw-r--

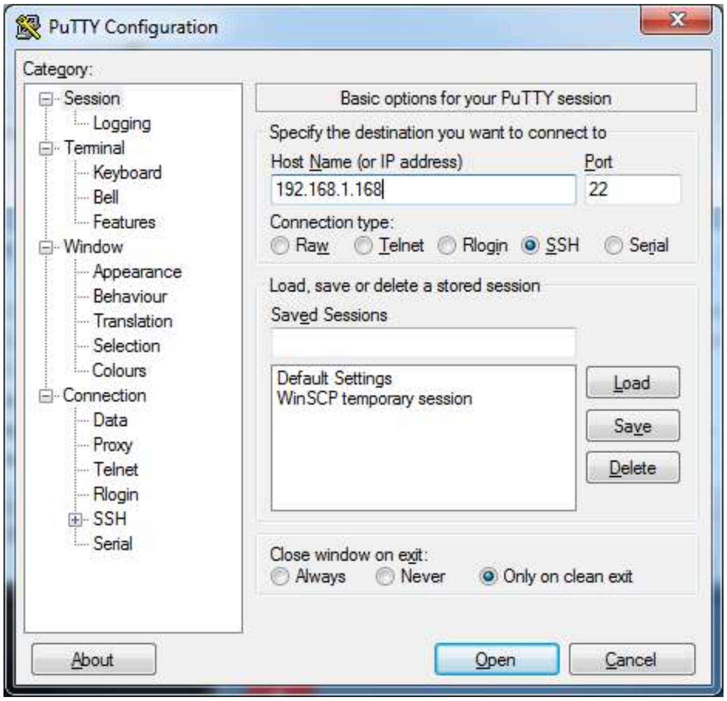
0 B of 285 KiB in 0 of 6

In the left pane you can browse to the location where you saved the F-Response files, in this case the C:\Bundle directory. Then we'll copy the files to the /<root> /tmp directory on the Linux target by browsing to the folder, then highlighting and dragging the files into the right pane.

Step 3: Fire it up!

Let's use another nice free easy tool to start F-Response on the Linux target(s). If you don't already have it installed, download a copy of puTTY.

Start puTTY and you are greeted with the following window:



Host Name (or IP address): 192.168.1.168
Port: 22

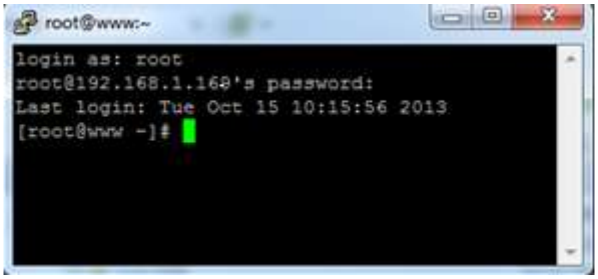
Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Saved Sessions:
Default Settings
WinSCP temporary session

Close window on exit: ○ Always ○ Never ● Only on clean exit

Simply enter the Linux target name or IP address into the Host Name field and click the Open button (leave everything else at the default setting).

Putty will start the connection and then prompt you for a Username and Password. Generally there are two types of Linux accounts for our purposes: the all powerful administrator "root" account, and a general user account that can assume root privileges for a time.



```
login as: root
root@192.168.1.168's password:
Last login: Tue Oct 15 10:15:56 2013
[root@www ~]#
```

To log into the Linux target with the root account, type 'root' for the login, and enter the password when prompted. You will see the prompt change to a # sign.

Given the power of the root account, it is more likely you will be using a general user account that will assume root privileges. The two possibilities for accomplishing this with your user account are su and sudo but first you'll need to login with your user account by entering your login and password at the prompt.

Once you are logged in, you recall copying the F-Response files to the /tmp directory. You can change to this directory by typing the command **cd /tmp** and hitting enter. Because the files were copied locally, the executable file needs to be defined as an executable, which is done by the command:

chmod a+x f-response-ce-e-lin

Now, to start F-Response:

If you logged in as root, you will type:

./f-response-ce-e-lin –c fresponse.ini [ENTER]

Again, you will probably be using a general user account to execute the F-Response code with root privileges via sudo or su. Let's take a look at these two possibilities:

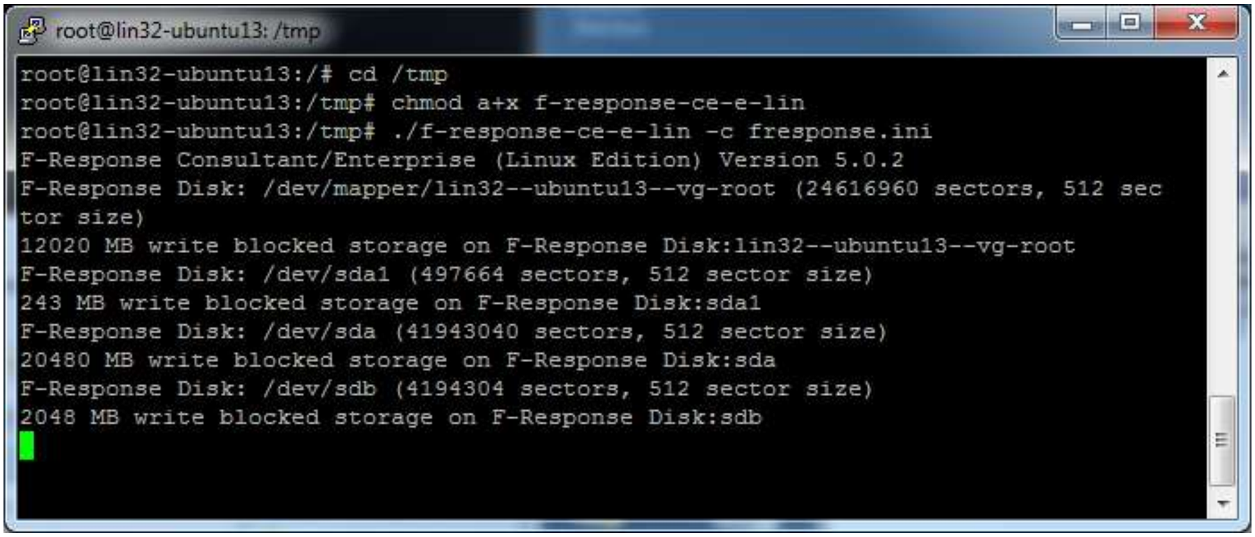
Sudo, or "SuperUser Do", is used to execute a command as root. The command to start F-Response using sudo is:

sudo ./f-response-ce-e-lin –c fresponse.ini [ENTER]

su can be used to assume root privileges. Once we have assumed root, the command to start F-Response is the same as if we are logged in with the root account. To start F-Response using su, type:

su [ENTER]
Type the root password [ENTER]
./f-response-ce-e-lin –c fresponse.ini [ENTER]

In this example we logged in using the root account. Then we changed to the temp directory where the F-Response files have been copied. We then modified F-Response as an executable. Finally we typed the command to start F-Response.



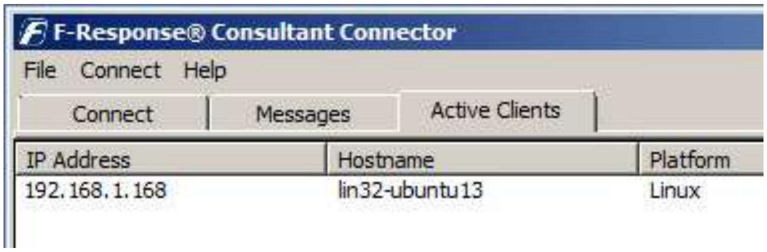
```
root@lin32-ubuntu13:/# cd /tmp
root@lin32-ubuntu13:/tmp# chmod a+x f-response-ce-e-lin
root@lin32-ubuntu13:/tmp# ./f-response-ce-e-lin -c fresponse.ini
F-Response Consultant/Enterprise (Linux Edition) Version 5.0.2
F-Response Disk: /dev/mapper/lin32--ubuntu13--vg-root (24616960 sectors, 512 sec
tor size)
12020 MB write blocked storage on F-Response Disk:lin32--ubuntu13--vg-root
F-Response Disk: /dev/sda1 (497664 sectors, 512 sector size)
243 MB write blocked storage on F-Response Disk:sda1
F-Response Disk: /dev/sda (41943040 sectors, 512 sector size)
20480 MB write blocked storage on F-Response Disk:sda
F-Response Disk: /dev/sdb (4194304 sectors, 512 sector size)
2048 MB write blocked storage on F-Response Disk:sdb
```

F-Response will then run and use the bundled information contained in the fresponse.ini file to locate the licensing server (your analyst machine). Once your analyst machine has been successfully located, F-Response will list each available write-blocked disk on the Linux target in the terminal window. These targets can then be seen on your analyst machine in the F-Response Consultant Connector.

Repeat Steps 2 and 3 for each Linux target machine you would like to view in the FCC on your analyst machine.

Step 4: Viewing your Target Disk(s)

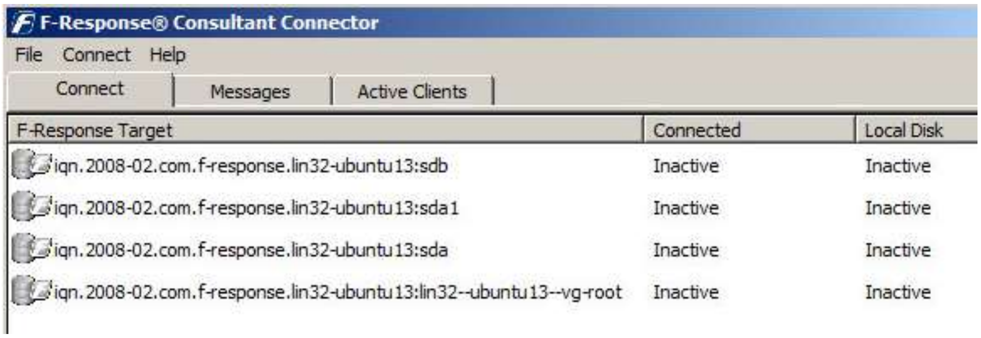
In the FCC on your analyst machine, look at the active clients tab for a list of Linux target machines.



IP Address	Hostname	Platform
192.168.1.168	lin32-ubuntu13	Linux

Here we can find potential target disks on the Linux targets by highlighting the machine(s) and selecting Issue Discovery Request from the Connect drop down or right click menus.

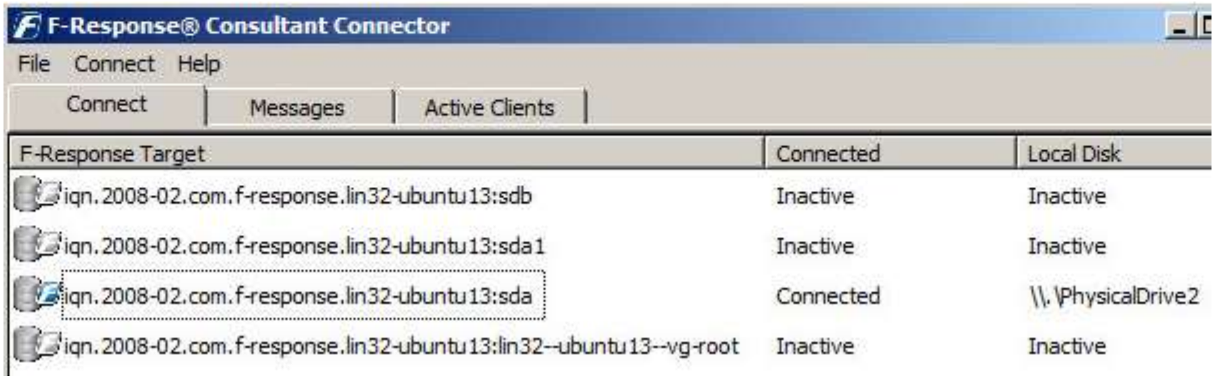
Once you've issued a discovery request, move on over to the Connect tab to see the results.



F-Response Target	Connected	Local Disk
iqn.2008-02.com.f-response.lin32-ubuntu13:sdb	Inactive	Inactive
iqn.2008-02.com.f-response.lin32-ubuntu13:sda1	Inactive	Inactive
iqn.2008-02.com.f-response.lin32-ubuntu13:sda	Inactive	Inactive
iqn.2008-02.com.f-response.lin32-ubuntu13:lin32--ubuntu13--vg-root	Inactive	Inactive

Under the Connect tab you can pick what disk(s) to connect to by highlighting and choosing Login to F-Response Disk from the Connect drop down or right click menus.

Once you log into the target disk the F-Response badge icon will change from gray to blue and the Connected status column will show as Connected.



F-Response Target	Connected	Local Disk
iqn.2008-02.com.f-response.lin32-ubuntu13:sdb	Inactive	Inactive
iqn.2008-02.com.f-response.lin32-ubuntu13:sda1	Inactive	Inactive
iqn.2008-02.com.f-response.lin32-ubuntu13:sda	Connected	\\.\PhysicalDrive2
iqn.2008-02.com.f-response.lin32-ubuntu13:lin32--ubuntu13--vg-root	Inactive	Inactive

Step 5: Fire up the tool of your choice!

F-Response is a vendor neutral product. Once F-Response presents the remote target disk as a write blocked local connection, we step out of your way so that you can select the right tool to get your job done. At this point, you can reach into your toolbox and apply the tool of your choice to the target disk(s).

Understanding F-Response Disk Naming

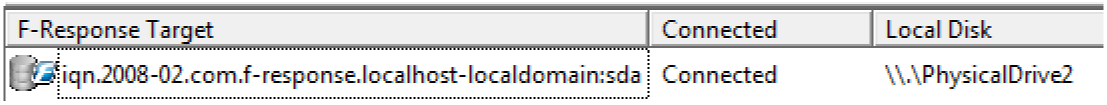
F-Response uses the following naming convention for target disks:

iqn.2008-02.com.f-response.HOSTNAME.O/S disk name

We are only concerned with the "HOSTNAME.O/S disk name" portion of the name.

HOSTNAME is the name of your Linux target machine. If you only know the IP address a quick glance back at the Active Clients tab will help you tie the hostname to the address.

For the "O/S disk name," Linux identifies hard disks using the format hdx or sdx. An "hd" prefix tells us this is a IDE or PATA disk and an "sd"prefix is used for SCSI, SATA, or USB drives. The 'x' portion is a letter, starting with 'a', representing the order the Linux O/S added the drive. For example:



F-Response Target	Connected	Local Disk
iqn.2008-02.com.f-response.localhost-localdomain:sda	Connected	\\.\PhysicalDrive2

This target is the first SCSI,SATA,or USB drive on the machine named 'localhost-localdomain'. If the last part of the name said "sdb" or "sdc" it would be the second or third physical disk on the 'localhost-localdomain' machine.

Troubleshooting

I cannot seem to connect to the linux target with WinSCP or puTTY? *These tools require SSH and SFTP to be running the on Linux target. To start ssh, from the command prompt on the Linux target type:* ***cd /etc/rd.d/init.d****, then* ***sh sshd start*** *to start the service.*

When I try to start F-Response on the target I get an error telling me it could not connect to Validation server? *Check your license manager is bound to the correct local IP address on your analyst machine. You may also check inside the fresponse.ini file to see the IP address matches your F-Response license manager.*

I have copied the F-Response files to the Linux machine and I have root level permissions, but when I try to start F-Response from the command line it tells me "Permission Denied"? *You may need to assign execute permission to the newly copied file. Type 'chmod +x f-response-ce-e-lin' (minus the quotes) at the command line.*

F-Response says I'm connected to the remote disk, yet I cannot see it in Explorer? *Correct, while your Windows analysis machine can only read FAT and NTFS, Linux can use these file systems and more. Most likely the target disk is using the one of the Linux standard ext2 or ext3 file system formats. To view the disk you will need use one of your third party tools.*

When I try to execute the "sudo" command and enter my password I get "Access Denied", why? *In the Linux OS environment your account can be either a user account or an admin account. Make sure your user account is set as an admin account and try executing sudo again.*

F-Response Consultant Edition works well, but I'd like to know if there's a way to hide the deployment or perhaps access it in a more covert manner. Does such an option exist? *F-Response Consultant Edition was not designed with covert deployment in mind. For more covert deployment and access options see F-Response Enterprise Edition.*

If you are having issues not covered in this guide. *Please don't hesitate to contact us directly either on the web (www.f-response.com) or via email (support@f-response.com), or via IM (YahooIM fresponse_s).*