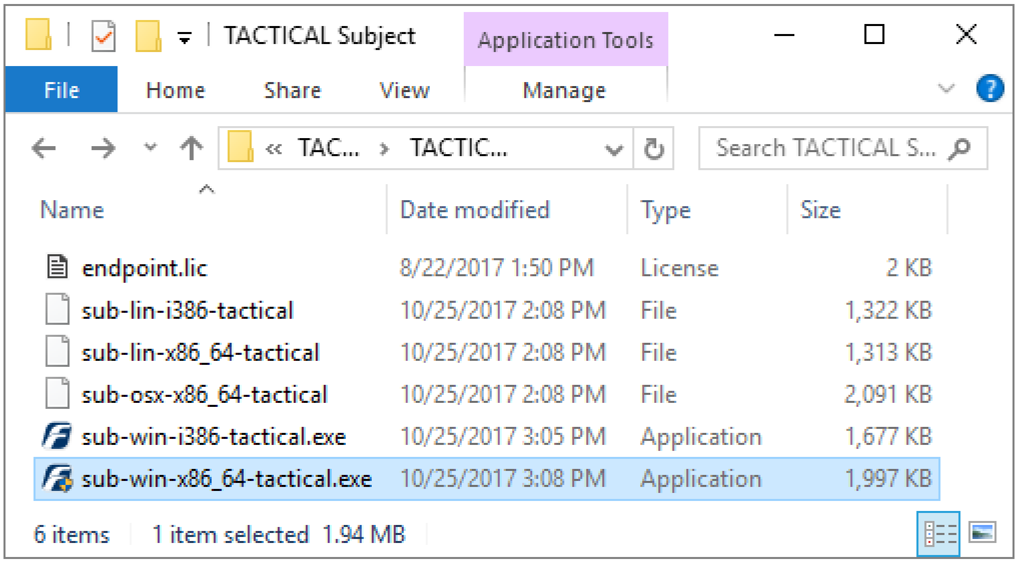
Mission Guide: TACTICAL v7

Connecting to a Tactical Subject Using The F-Response Accelerator on Linux

Overview

Step 1: Start the Tactical Subject

Insert the tactical subject USB into the subject's computer. The tactical subject USB contains a license file and subject executables. Then select a subject executable based on the platform and architecture of the subject's computer.

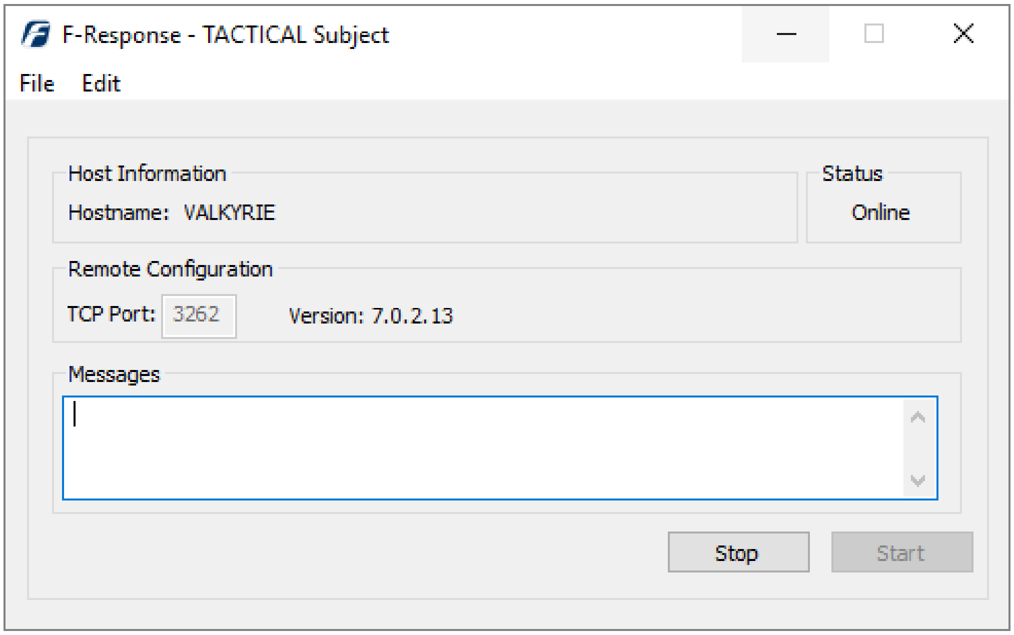


Name	Date modified	Type	Size
endpoint.lic	8/22/2017 1:50 PM	License	2 KB
sub-lin-i386-tactical	10/25/2017 2:08 PM	File	1,322 KB
sub-lin-x86_64-tactical	10/25/2017 2:08 PM	File	1,313 KB
sub-osx-x86_64-tactical	10/25/2017 2:08 PM	File	2,091 KB
sub-win-i386-tactical.exe	10/25/2017 3:05 PM	Application	1,677 KB
sub-win-x86_64-tactical.exe	10/25/2017 3:08 PM	Application	1,997 KB

6 items 1 item selected 1.94 MB

Figure 1: An example view of the tactical subject USB.

In this example, the subject's computer is running Windows 10 on a x86-64 processor, which matches the subject executable named sub-win-x86_64-tactical.exe.



Host Information
Hostname: VALKYRIE

Status
Online

Remote Configuration
TCP Port: 3262
Version: 7.0.2.13

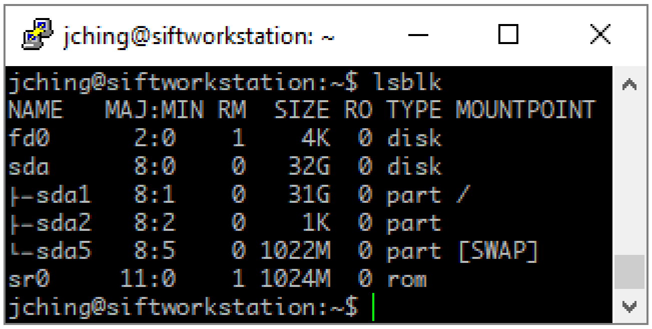
Messages

Figure 2: An example view of the sub-win-x86_64-tactical.exe.

Step 2: Mount the Tactical Examiner USB

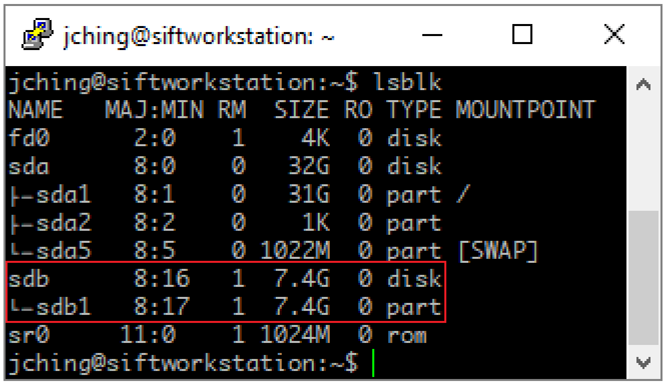
The tactical examiner USB is a block device and the `lsblk` command prints a list of block devices. The following procedure identifies the tactical examiner USB.

1. Run the `lsblk` command **before** inserting the tactical examiner USB.



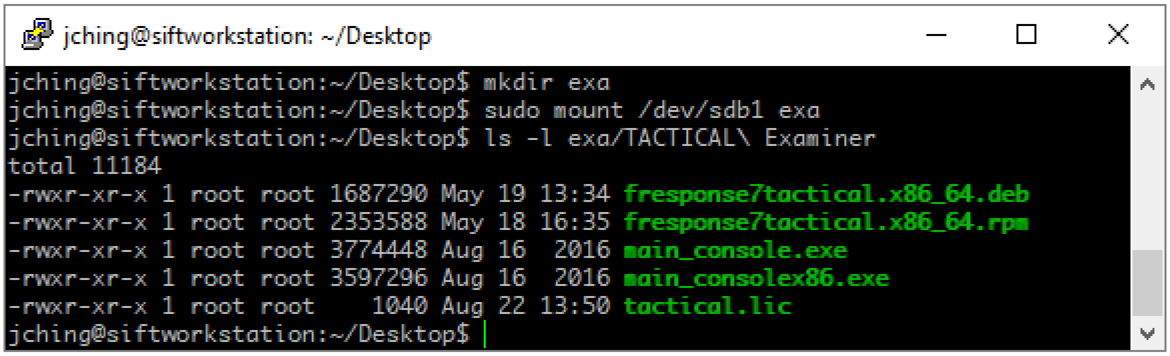
```
jching@siftworkstation:~$ lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
fd0      2:0    1    4K  0 disk
sda      8:0    0   32G  0 disk
├─sda1   8:1    0   31G  0 part /
├─sda2   8:2    0    1K  0 part
└─sda5   8:5    0 1022M  0 part [SWAP]
sr0     11:0    1 1024M  0 rom
jching@siftworkstation:~$
```

2. Insert the tactical examiner USB and run the `lsblk` command again.



```
jching@siftworkstation:~$ lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
fd0      2:0    1    4K  0 disk
sda      8:0    0   32G  0 disk
├─sda1   8:1    0   31G  0 part /
├─sda2   8:2    0    1K  0 part
└─sda5   8:5    0 1022M  0 part [SWAP]
sdb      8:16   1  7.4G  0 disk
└─sdb1   8:17   1  7.4G  0 part
sr0     11:0    1 1024M  0 rom
jching@siftworkstation:~$
```

In this example, the tactical examiner USB has one partition, which contains a vfat filesystem. To mount the vfat filesystem, run the `mount` command on the device file of the partition and a directory for mounting the filesystem.



```
jching@siftworkstation:~/Desktop$ mkdir exa
jching@siftworkstation:~/Desktop$ sudo mount /dev/sdb1 exa
jching@siftworkstation:~/Desktop$ ls -l exa/TACTICAL\ Examiner
total 11184
-rwxr-xr-x 1 root root 1687290 May 19 13:34 fresponse7tactical.x86_64.deb
-rwxr-xr-x 1 root root 2353588 May 18 16:35 fresponse7tactical.x86_64.rpm
-rwxr-xr-x 1 root root 3774448 Aug 16  2016 main_console.exe
-rwxr-xr-x 1 root root 3597296 Aug 16  2016 main_consolex86.exe
-rwxr-xr-x 1 root root    1040 Aug 22 13:50 tactical.lic
jching@siftworkstation:~/Desktop$
```

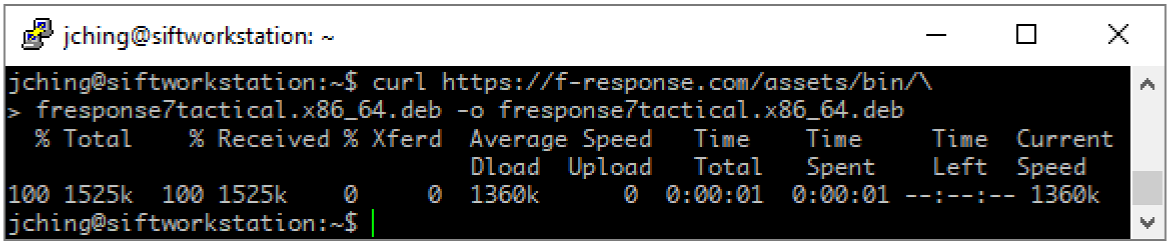
Figure 3: An example mount procedure.

Step 3: Install the F-Response Accelerator

The RPM and Debian packages for the F-Response Accelerator are available through the following link: https://f-response.com/support/downloads.

In this example, the SIFT workstation is running Ubuntu 16.04 LTS, which uses the Debian package manager. The following procedure downloads and installs the Debian package for the F-Response Accelerator.

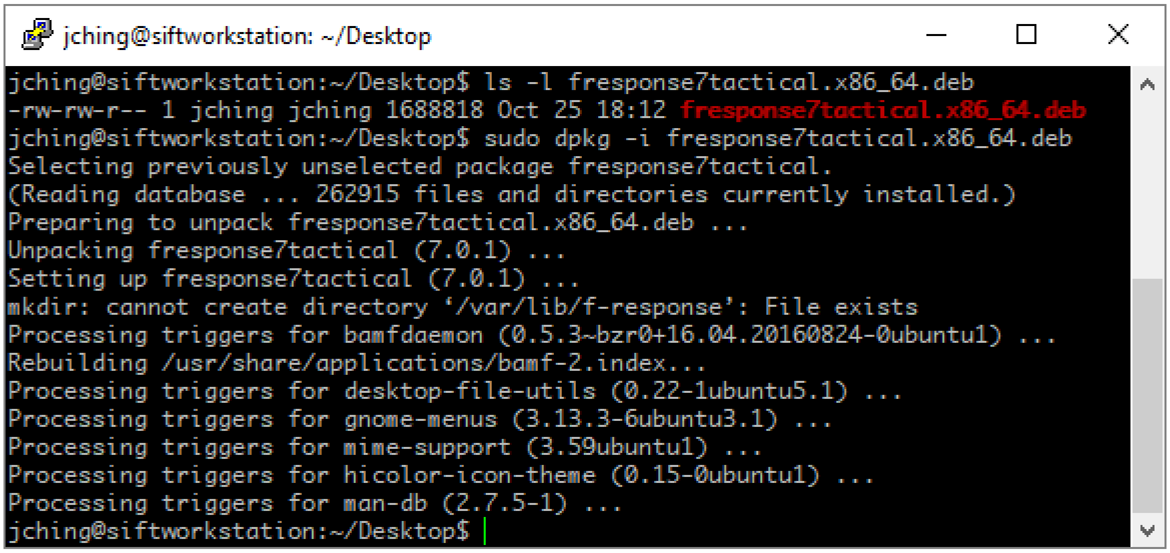
1. Download the Debian package using `curl`.



```
jching@siftworkstation:~$ curl https://f-response.com/assets/bin/\
> fresponse7tactical.x86_64.deb -o fresponse7tactical.x86_64.deb
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 1525k  100 1525k    0     0  1360k      0  0:00:01  0:00:01 --:--:-- 1360k
jching@siftworkstation:~$
```

Figure 4: Downloading the Debian package from the F-Response webserver.

2. Install the Debian package using dpkg.



```
jching@siftworkstation:~/Desktop$ ls -l fresponse7tactical.x86_64.deb
-rw-rw-r-- 1 jching jching 1688818 Oct 25 18:12 fresponse7tactical.x86_64.deb
jching@siftworkstation:~/Desktop$ sudo dpkg -i fresponse7tactical.x86_64.deb
Selecting previously unselected package fresponse7tactical.
(Reading database ... 262915 files and directories currently installed.)
Preparing to unpack fresponse7tactical.x86_64.deb ...
Unpacking fresponse7tactical (7.0.1) ...
Setting up fresponse7tactical (7.0.1) ...
mkdir: cannot create directory '/var/lib/f-response': File exists
Processing triggers for bamfdaemon (0.5.3~bzr0+16.04.20160824-0ubuntu1) ...
Rebuilding /usr/share/applications/bamf-2.index...
Processing triggers for desktop-file-utils (0.22-1ubuntu5.1) ...
Processing triggers for gnome-menus (3.13.3-6ubuntu3.1) ...
Processing triggers for mime-support (3.59ubuntu1) ...
Processing triggers for hicolor-icon-theme (0.15-0ubuntu1) ...
Processing triggers for man-db (2.7.5-1) ...
jching@siftworkstation:~/Desktop$
```

Figure 5: Installing the Debian package for F-Response Accelerator.

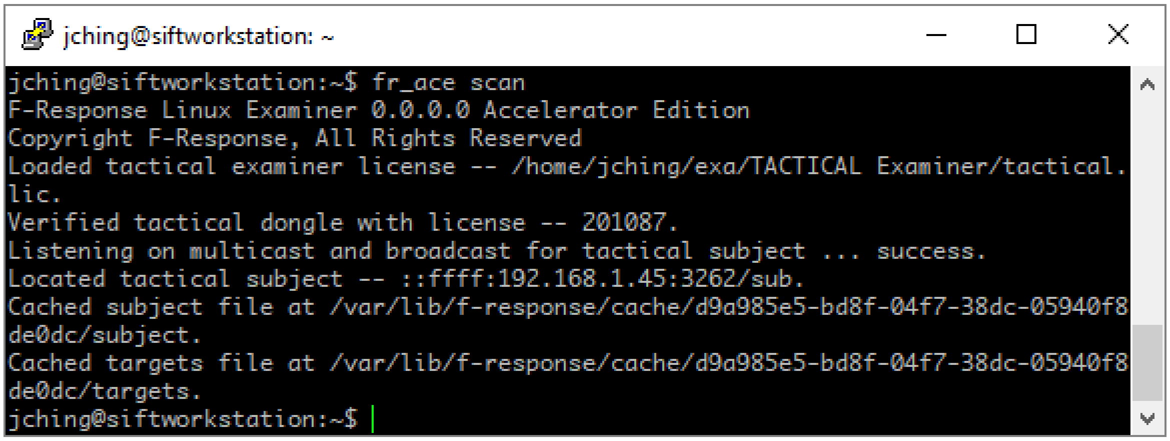
3. Run the `` `sudo apt-get install -f` `` to resolved missing dependencies.

Step 4: Listen for the Tactical Subject

The tactical subject emits broadcast and/or multi-cast traffic and the tactical examiner listens for the traffic on the local network.

Command Line Interface using `fr_ace`

To listen for the tactical subject, run the `` `fr_ace scan` `` command.

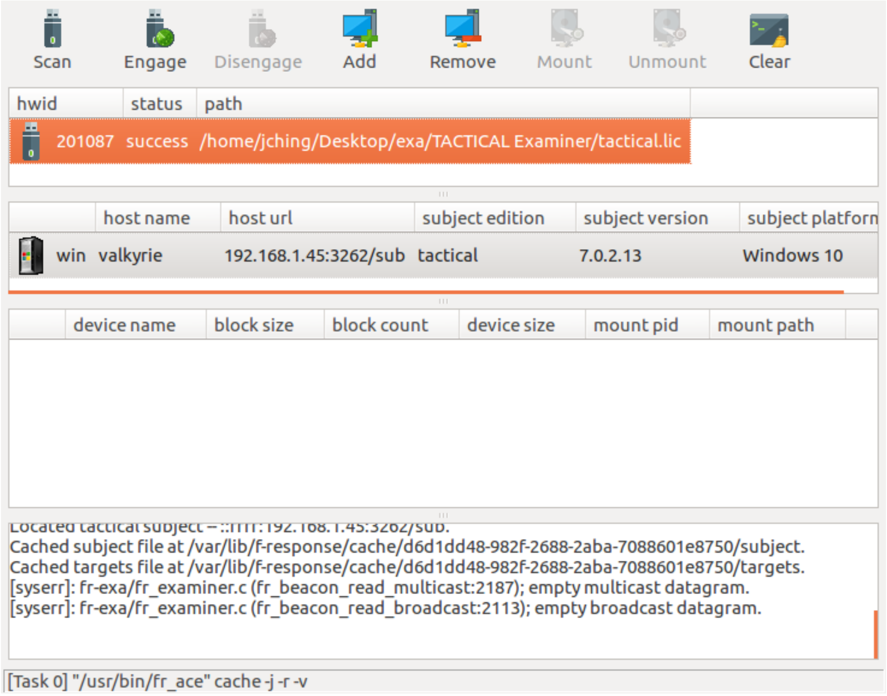


```
jching@siftworkstation:~$ fr_ace scan
F-Response Linux Examiner 0.0.0.0 Accelerator Edition
Copyright F-Response, All Rights Reserved
Loaded tactical examiner license -- /home/jching/exa/TACTICAL Examiner/tactical.
lic.
Verified tactical dongle with license -- 201087.
Listening on multicast and broadcast for tactical subject ... success.
Located tactical subject -- ::ffff:192.168.1.45:3262/sub.
Cached subject file at /var/lib/f-response/cache/d9a985e5-bd8f-04f7-38dc-05940f8
de0dc/subject.
Cached targets file at /var/lib/f-response/cache/d9a985e5-bd8f-04f7-38dc-05940f8
de0dc/targets.
jching@siftworkstation:~$
```

Figure 6: An example use of the `scan` command from the `fr_ace` interface.

Graphical User Interface using `fr_ace_ui`

To listen for the tactical subject, press the scan button, select a tactical examiner license, and press the engage button.



hwid	status	path
201087	success	/home/jching/Desktop/exa/TACTICAL Examiner/tactical.lic

	host name	host url	subject edition	subject version	subject platforn
win	valkyrie	192.168.1.45:3262/sub	tactical	7.0.2.13	Windows 10

	device name	block size	block count	device size	mount pid	mount path

```
Located tactical subject – ::ffff:192.168.1.45:3262/sub.
Cached subject file at /var/lib/f-response/cache/d6d1dd48-982f-2688-2aba-7088601e8750/subject.
Cached targets file at /var/lib/f-response/cache/d6d1dd48-982f-2688-2aba-7088601e8750/targets.
[syserr]: fr-exa/fr_examiner.c (fr_beacon_read_multicast:2187); empty multicast datagram.
[syserr]: fr-exa/fr_examiner.c (fr_beacon_read_broadcast:2113); empty broadcast datagram.
```

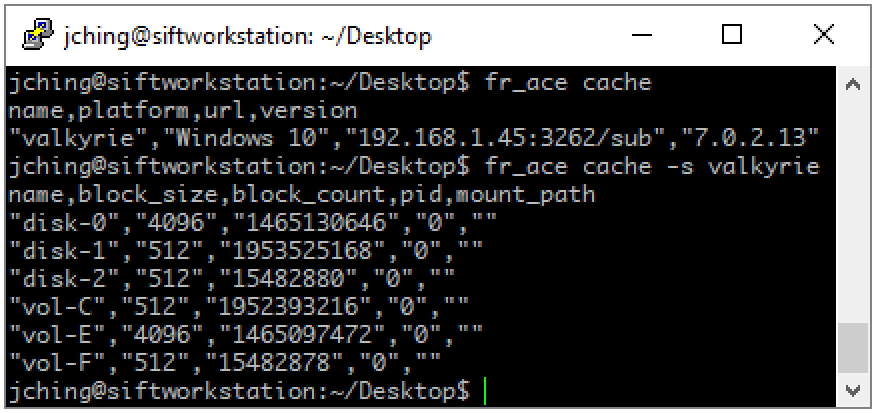
```
[Task 0] "/usr/bin/fr_ace" cache -j -r -v
```

Figure 7: An example view of the fr_ace_ui interface.

Step 5: List the Tactical Subjects

Command Line Interface using `fr_ace`

To list the subject and targets, run the `` `fr_ace cache` `` command.



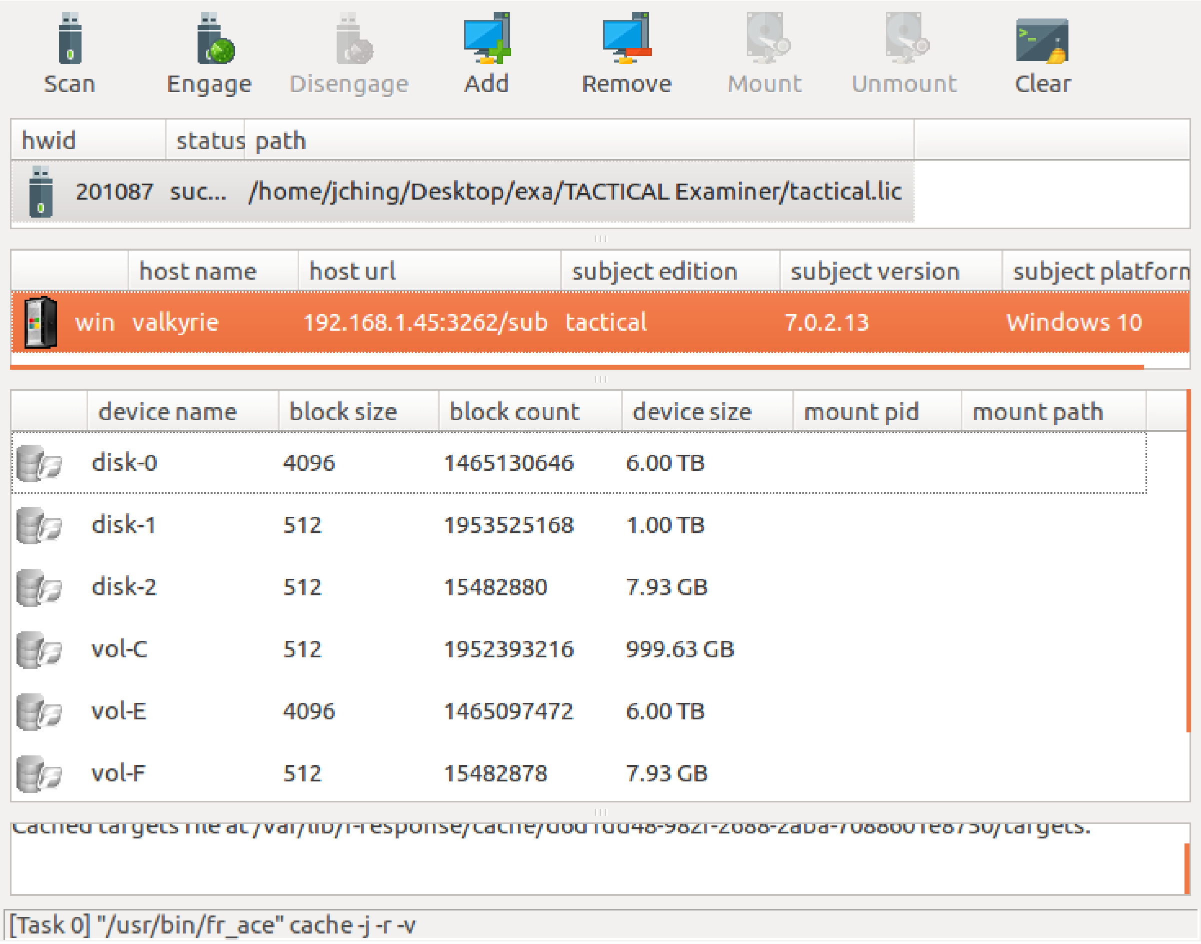
jching@siftworkstation: ~/Desktop

```
jching@siftworkstation:~/Desktop$ fr_ace cache
name,platform,url,version
"valkyrie","Windows 10","192.168.1.45:3262/sub","7.0.2.13"
jching@siftworkstation:~/Desktop$ fr_ace cache -s valkyrie
name,block_size,block_count,pid,mount_path
"disk-0","4096","1465130646","0",""
"disk-1","512","1953525168","0",""
"disk-2","512","15482880","0",""
"vol-C","512","1952393216","0",""
"vol-E","4096","1465097472","0",""
"vol-F","512","15482878","0",""
jching@siftworkstation:~/Desktop$
```

Figure 8: An example use of the cache command from the fr_ace interface.

Graphical User Interface using `fr_ace_ui`

To view the target list, select a subject.



hwid	status	path
201087	suc...	/home/jching/Desktop/exa/TACTICAL Examiner/tactical.lic

	host name	host url	subject edition	subject version	subject platforn
win	valkyrie	192.168.1.45:3262/sub	tactical	7.0.2.13	Windows 10

device name	block size	block count	device size	mount pid	mount path
disk-0	4096	1465130646	6.00 TB		
disk-1	512	1953525168	1.00 TB		
disk-2	512	15482880	7.93 GB		
vol-C	512	1952393216	999.63 GB		
vol-E	4096	1465097472	6.00 TB		
vol-F	512	15482878	7.93 GB		

Cached targets file at /var/lib/f-response/cache/d0d1dd48-9821-2688-2aba-708860fe8730/targets.

[Task 0] "/usr/bin/fr_ace" cache -j -r -v

Figure 9: An example view of the target list.