## *Forensic Scanner Usage*

This document is intended to describe how the Forensic Scanner is set up and can be used.

### Step 1 – Mount your image file

The first step to using the Forensic Scanner is to mount your image file as an accessible volume. There are a number of tools and methods available to do so; for example, you can use FTK Imager, or ImDisk, or modify the image file to a VHD or VMDK file and use the appropriate method to mount the image.

Using FTK Imager to mount an image as a volume is straightforward process. Open FTK Imager and select "Image Mounting…" from the File menu, as illustrated in Figure 1.

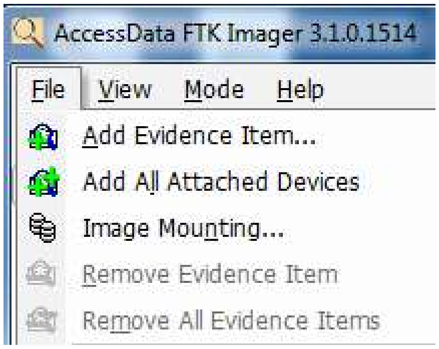


*Figure 1: FTK Imager File menu options*

After the "Mount Image to Drive" dialog appears, select the image file that you want to mount, and click the "Mount" button, as illustrated in Figure 2.

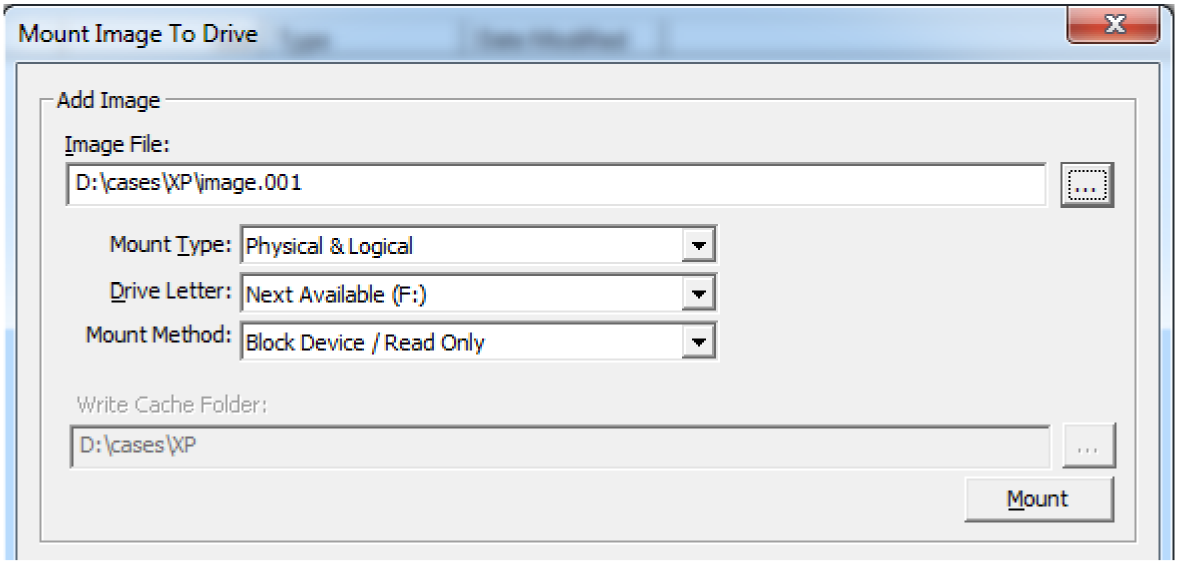


Image File: D:\cases\XP\image.001

Mount Type: Physical & Logical

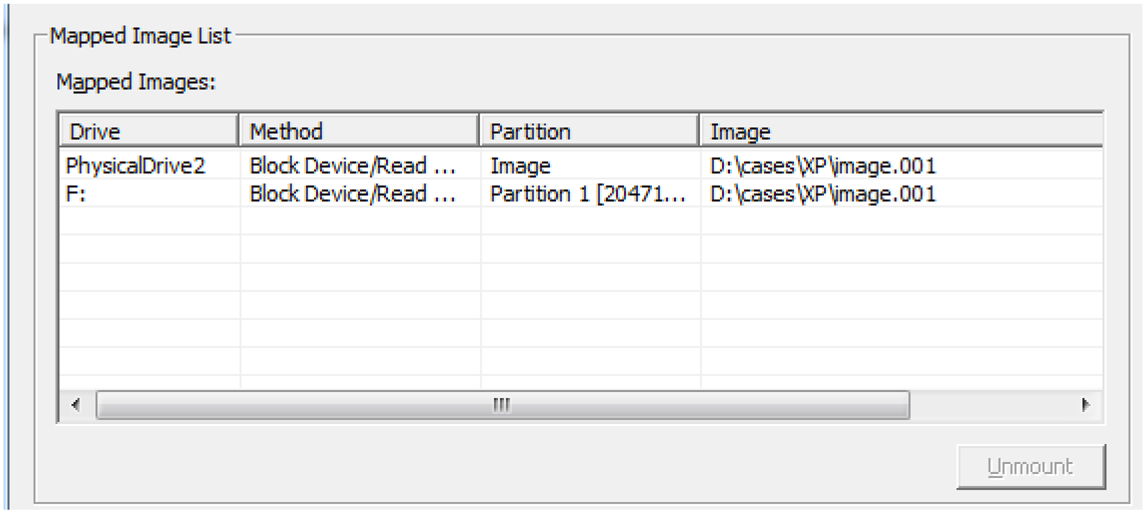
Drive Letter: Next Available (F:)

Mount Method: Block Device / Read Only

Write Cache Folder: D:\cases\XP

*Figure 2: Mounting an image*

Once you click the "Mount" button, your image will be mounted as a read-only volume on your analysis system, as illustrated in Figure 3.

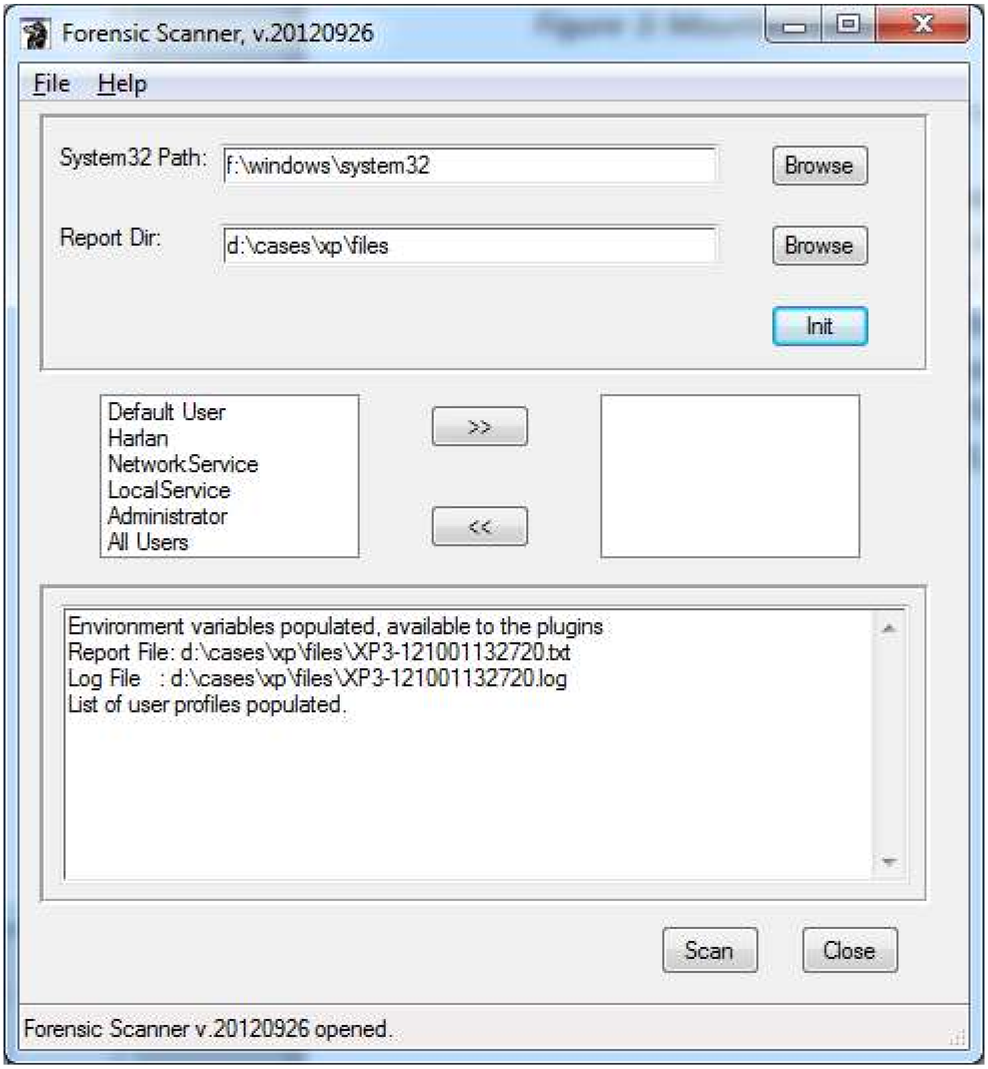


| Drive | Method | Partition | Image |
|---|---|---|---|
| PhysicalDrive2 | Block Device/Read ... | Image | D:\cases\XP\image.001 |
| F: | Block Device/Read ... | Partition 1 [20471... | D:\cases\XP\image.001 |

*Figure 3: Mounted Volume*

With this, you're ready to scan your mounted image.

**Step 2 – Set up the Forensic Scanner**
In order to run the Forensic Scanner, be sure to log into your analysis system using an Administrator account. Then navigate to the directory where you copied the Forensic Scanner archive files, and double click "scanner.exe". After the GUI launches, enter the path to the "system32"directory within your mounted image in the first text field (you can use the BrowseForFolder selector via the "Browse" button to the right of the text field), and then enter the path to where you would like the report files written in the second text field. Once you've done this, click the "Init" button, and the left-hand pane in the middle of the GUI should be populated with the available user profiles from within your mounted image, as illustrated in Figure 4.



Forensic Scanner, v.20120926

System32 Path: f:\windows\system32

Report Dir: d:\cases\xp\files

Default User
Harlan
NetworkService
LocalService
Administrator
All Users

```
Environment variables populated, available to the plugins
Report File: d:\cases\xp\files\XP3-121001132720.txt
Log File   : d:\cases\xp\files\XP3-121001132720.log
List of user profiles populated.
```

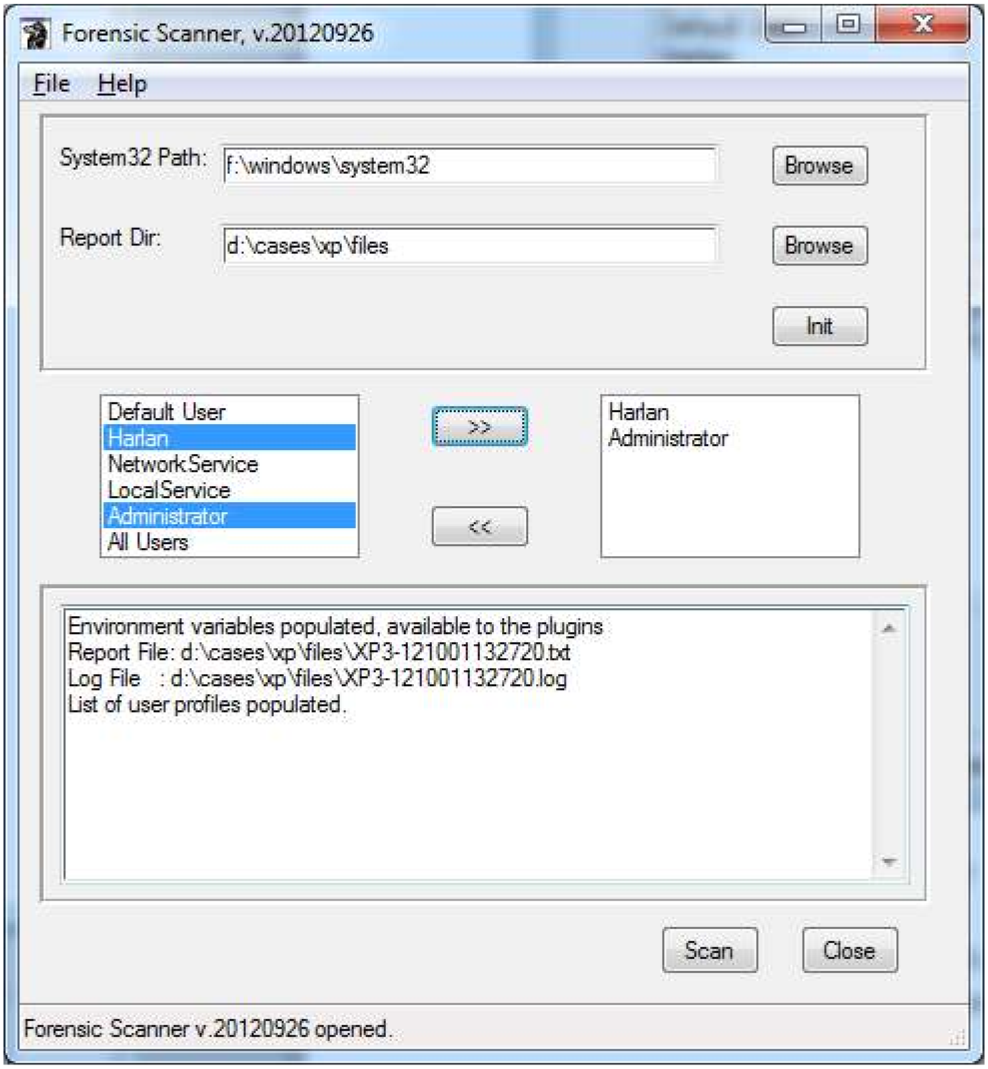
Forensic Scanner v.20120926 opened.

*Figure 4: Forensic Scanner GUI*

The scanner populates the GUI with the available user profiles by reading the appropriate directory structure, based on the version of the Windows operating system found in the mounted volume.

Next, in the left-hand pane, select the user profiles that you want to scan.  You can select multiple profiles by holding down the Control key on the keyboard, and clicking on additional profiles.

When you've selected all of the profiles you'd like to include in the scan, click the ">>" button so that the profiles are copied to the right-hand pane, as illustrated in Figure 5.



System32 Path: f:\windows\system32

Report Dir: d:\cases\xp\files

Default User
Harlan
NetworkService
LocalService
Administrator
All Users

Harlan
Administrator

```
Environment variables populated, available to the plugins
Report File: d:\cases\xp\files\XP3-121001132720.txt
Log File   : d:\cases\xp\files\XP3-121001132720.log
List of user profiles populated.
```

Forensic Scanner v.20120926 opened.

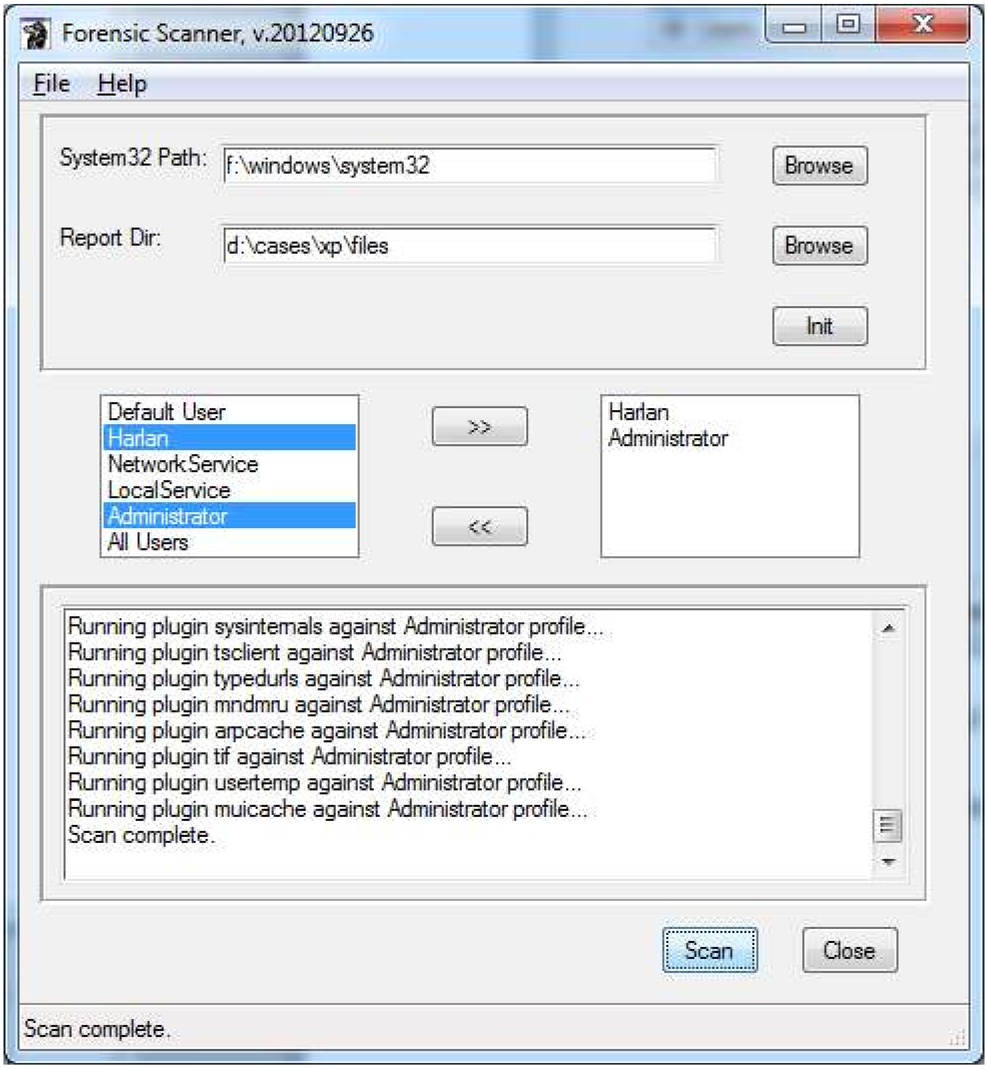
*Figure 5: User profiles selected*

**Step 3 – Run your scan**

Now you're ready to launch the scan.  To so, simply click the "Scan" button. The scanner will automatically locate all of the plugins that pertain to the version of Windows found within the mounted image, and sort those plugins by scan class (system or user) as well as by category.  This is done so that all plugins from the same category are run consecutively and their output is grouped together in the report file.

NOTE: For plugins that belong to multiple categories, the scanner will only run the plugin for the first category to which the plugin applies.  The scan log will include indications of plugins with multiple categories being skipped for subsequent categories.

When the scan is complete, "Scan complete" will be displayed in the text area as well as in the status bar at the bottom of the GUI, as illustrated in Figure 6.



System32 Path: f:\windows\system32

Report Dir: d:\cases\xp\files

Default User
Harlan
NetworkService
LocalService
Administrator
All Users

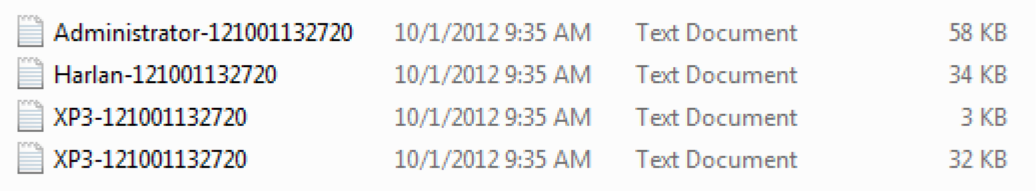
Harlan
Administrator

```
Running plugin sysinternals against Administrator profile...
Running plugin tsclient against Administrator profile...
Running plugin typedurls against Administrator profile...
Running plugin mndmru against Administrator profile...
Running plugin arpcache against Administrator profile...
Running plugin tif against Administrator profile...
Running plugin usertemp against Administrator profile...
Running plugin muicache against Administrator profile...
Scan complete.
```

Scan complete.

*Figure 6: Completed scan*

**Step 4 – Review the results**
To view your scan results, navigate to the directory where you chose to have the reports written, and you should see files similar to what is illustrated in Figure 7.



| | | | |
|---|---|---|---|
| Administrator-121001132720 | 10/1/2012 9:35 AM | Text Document | 58 KB |
| Harlan-121001132720 | 10/1/2012 9:35 AM | Text Document | 34 KB |
| XP3-121001132720 | 10/1/2012 9:35 AM | Text Document | 3 KB |
| XP3-121001132720 | 10/1/2012 9:35 AM | Text Document | 32 KB |

*Figure 7: Scan results*

The report directory should include a report file for the system portion of the scan, a report file for each user profile scanned, and a scan log file. These files are ASCII text and can be reviewed in Notepad, or any other editor.