Differential EnScript

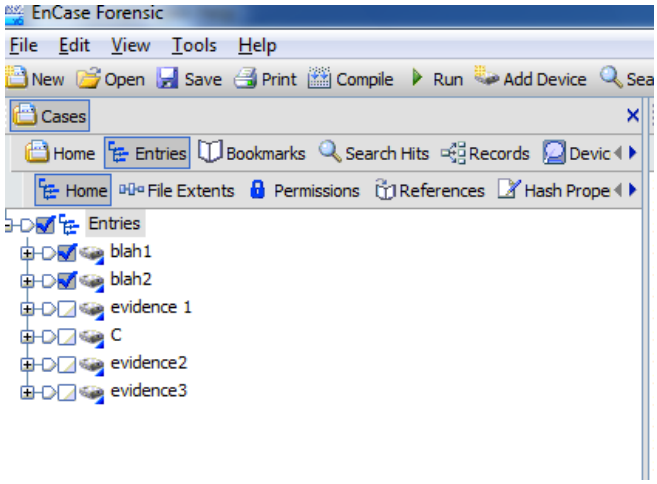
Jamie Levy
jamie.levy@gmail.com
http://gleeda.blogspot.com

Background

Occasionally there is a need to see what file system changes take place after a particular event, whether it is installing a program, running malware or interacting with the system in some other way. In order to make things easier for myself to keep track of file system changes, I wrote an EnScript. After some thought I decided that it might be beneficial to others for me to release it to the public. This is just a brief overview of how the script works. I hope you will find it useful and give feedback.

Setting Up

Place the Differential.EnScript into your EnScript directory as usual. (In my case the path to my EnScript directory is C:\Program Files\EnCase6.18\EnScript). Create a case and load your evidence files as usual. Below you can see a screenshot of several evidence files I have loaded into my case:



Notice that each evidence file is named differently. This can be achieved by various methods, two of which are below:

1) When adding a device, right before you press “Finish” hit “Enter” and you will be presented with a menu that allows you to name the evidence file
2) Right-clicking on an evidence file and choosing “Rename” from the menu

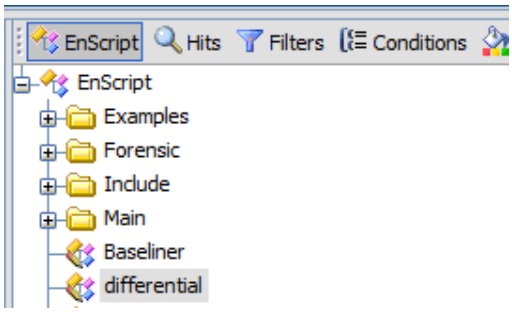
This is important, because the two evidence files that you want to compare must be named differently for the script to work correctly.

Jamie Levy
jamie.levy@gmail.com
http://gleeda.blogspot.com

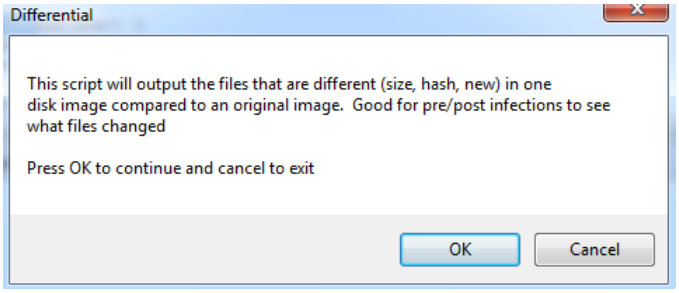
As long as you have your case created, evidence files loaded and the Differential.EnScript placed in your EnScript directory, you are ready to proceed.

Running the Script

Double-click the Differential.EnScript in your EnScript pane, located in the lower-right-hand side by default:

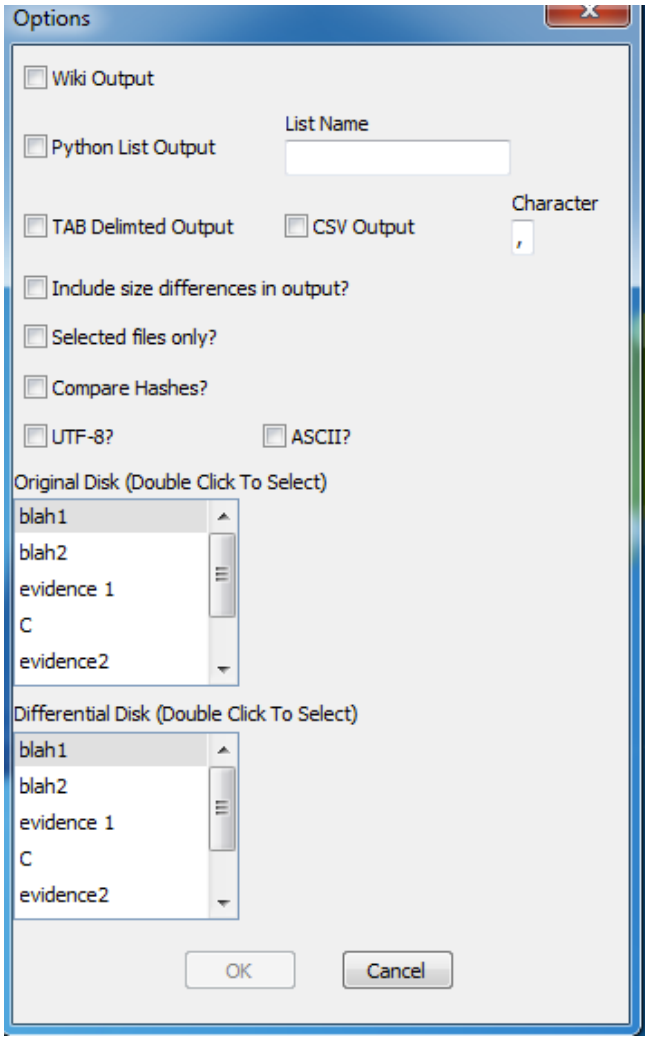


You will see a message box describing what the script does and asking if you want to proceed, click OK:



Jamie Levy
jamie.levy@gmail.com
http://gleeda.blogspot.com

At this point you will be able to choose various options for running the script:

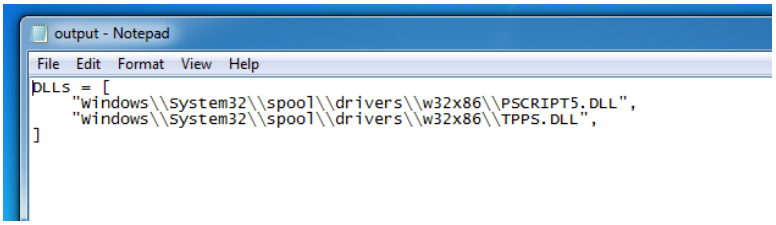


1) "Wiki Output" is of the following form and is good for collaborative sites:

   | Change | File | Original Size | Original Hash | New Size | New Hash |

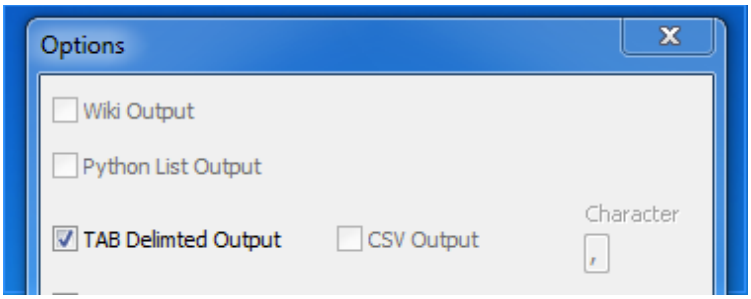
2) "Python List Output" consists of only the files names in the output file such that it could be easily transformed into a python list. You must specify the list name in the text box on the same row, which says "List Name". If you do not write something with valid characters [A-Za-z0-9] or if you leave it blank, you will see an error message and the script will end execution. Example output can be seen below:

Jamie Levy
jamie.levy@gmail.com
http://gleeda.blogspot.com



3) Then you have "Tab Delimited Output" which is self explanatory
4) "CSV Output" defaults to a comma (",") delimiter, but can be changed using the "Character" field next to it.

Choosing any of these output types will block out the options to choose another output type until the original choice is unchecked. For example, if I choose "Tab Delimited Output" all other output options will become greyed out, but will become valid options again if I uncheck the checkbox:

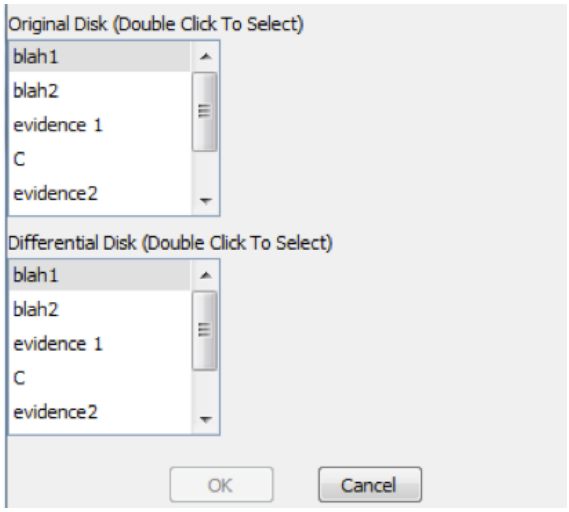


Also the script will not allow you to proceed until you have chosen the type of output you want.

5) "Include size differences in output?" Sometimes you want to know what files were changed and sometimes you just want to know about new files. This checkbox lets you control these options. If you select it, files that have changed in size from the original evidence file will also appear in your output file.
6) The "Selected files only?" option allows you to only look at files that you are interested in, instead of the entire evidence file. For example, if you are only interested in executables, you can write a condition to filter all executables, select them (bluecheck) and then run this script and check this box to only look at those files. All other files will be ignored. If you choose this option, make sure you select files from both evidence files ;-)
7) The "Compare Hashes?" option allows you to hash files of interest on the fly and put these in your output file if the hashes are not the same as the files original evidence file. This is an expensive operation since hashing takes time, but useful if you have a file that is the same name and size, but of different content.

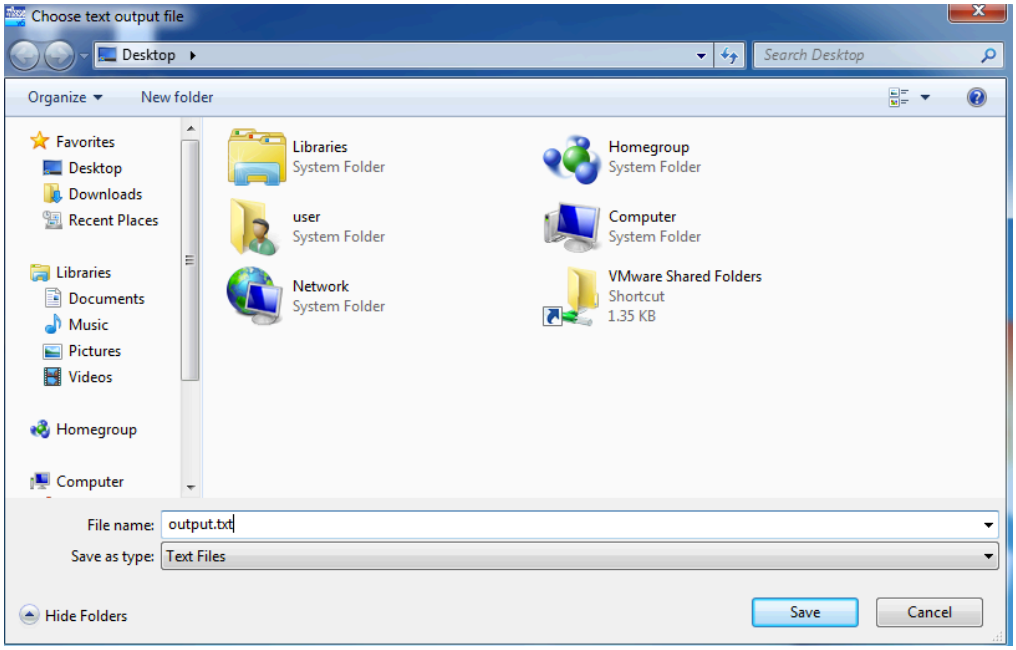
Jamie Levy
jamie.levy@gmail.com
http://gleeda.blogspot.com

8) "UTF8?" and "ASCII? " These options allow you to output in UTF-8 or ASCII (ANSI) formats. The default output setting is UTF-16, which is the EnCase default. These other codings are useful if you plan to process the output file with a tool that doesn't handle UTF-16, like grep. You can only choose one of these output formats at a time.
9) Finally we come to the menu to select our original and changed evidence files. These are auto populated from the evidence files in the case. You must choose a different file in each of the menus. To choose a file, you must double click the name of the evidence file. Notice that if you have several evidence files, the scrollbar will appear, allowing you to scroll to files listed later:

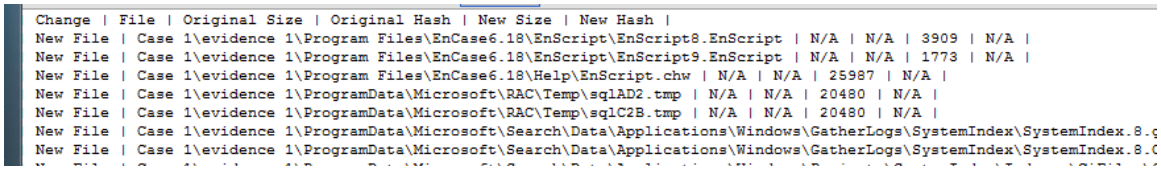


Once everything is filled out, type of output and other options, the "OK" button will become activated and you can press it to proceed. At this point you will see the "Save As" dialog allowing you to choose where you would like to save your output file:

Jamie Levy
jamie.levy@gmail.com
http://gleeda.blogspot.com



Give it name and press "Save". The script will run, you will see output in the Console as it runs:



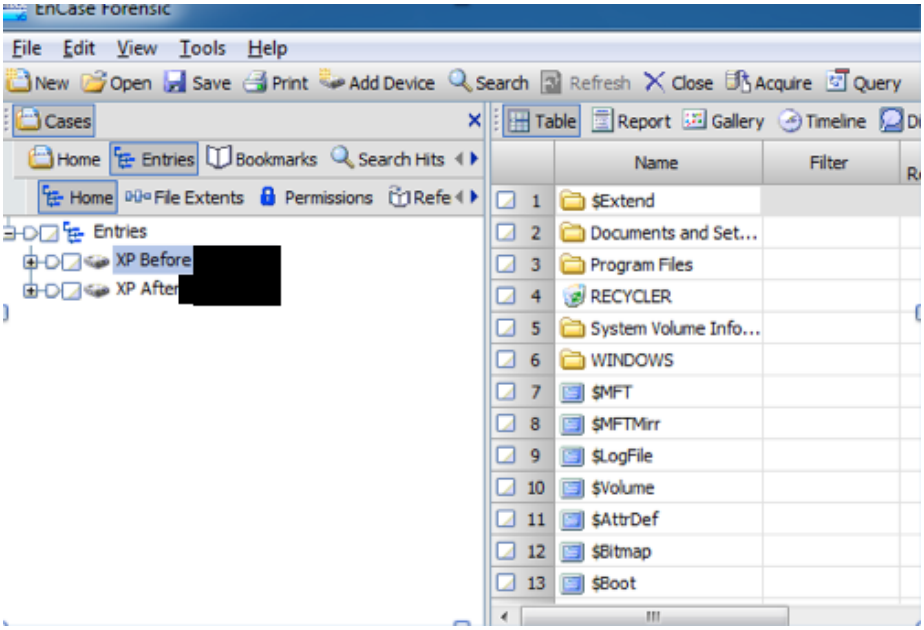
```
Change | File | Original Size | Original Hash | New Size | New Hash |
New File | Case 1\evidence 1\Program Files\EnCase6.18\EnScript\EnScript8.EnScript | N/A | N/A | 3909 | N/A |
New File | Case 1\evidence 1\Program Files\EnCase6.18\EnScript\EnScript9.EnScript | N/A | N/A | 1773 | N/A |
New File | Case 1\evidence 1\Program Files\EnCase6.18\Help\EnScript.chw | N/A | N/A | 25987 | N/A |
New File | Case 1\evidence 1\ProgramData\Microsoft\RAC\Temp\sqlAD2.tmp | N/A | N/A | 20480 | N/A |
New File | Case 1\evidence 1\ProgramData\Microsoft\RAC\Temp\sqlC2B.tmp | N/A | N/A | 20480 | N/A |
New File | Case 1\evidence 1\ProgramData\Microsoft\Search\Data\Applications\Windows\GatherLogs\SystemIndex\SystemIndex.8.
New File | Case 1\evidence 1\ProgramData\Microsoft\Search\Data\Applications\Windows\GatherLogs\SystemIndex\SystemIndex.8.
```

Everything should be saved in the output file.

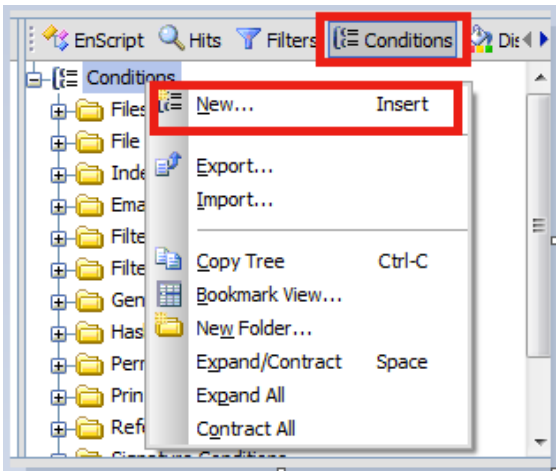
Example

Suppose I want to see all DLL and EXE files that were added after installing an application. First we will add our evidence files of before and after disk images.

Jamie Levy
jamie.levy@gmail.com
http://gleeda.blogspot.com

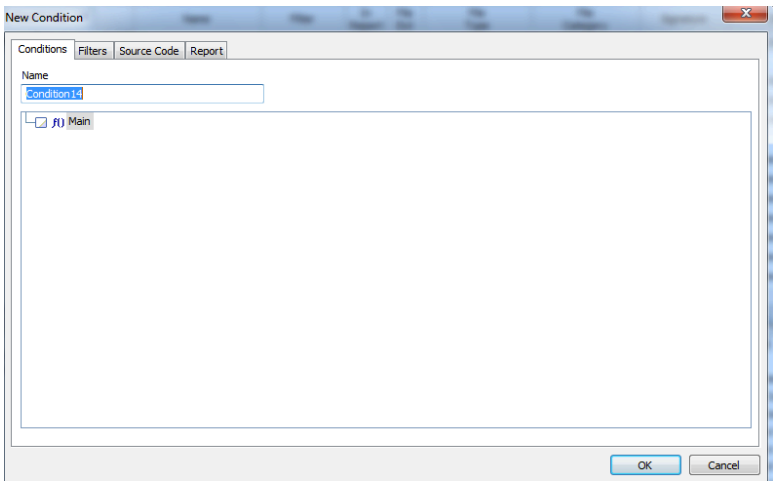


Now we need to create a condition. In the bottom right-hand corner you will see the "Conditions" menu. Click it, then right-click at the root (on "Conditions") and click "New":

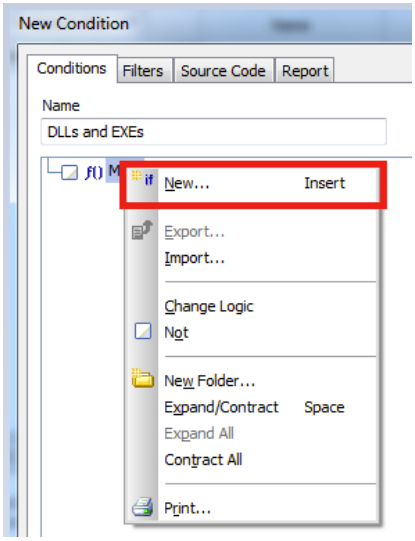


Jamie Levy
jamie.levy@gmail.com
http://gleeda.blogspot.com

The condition dialog will pop up:

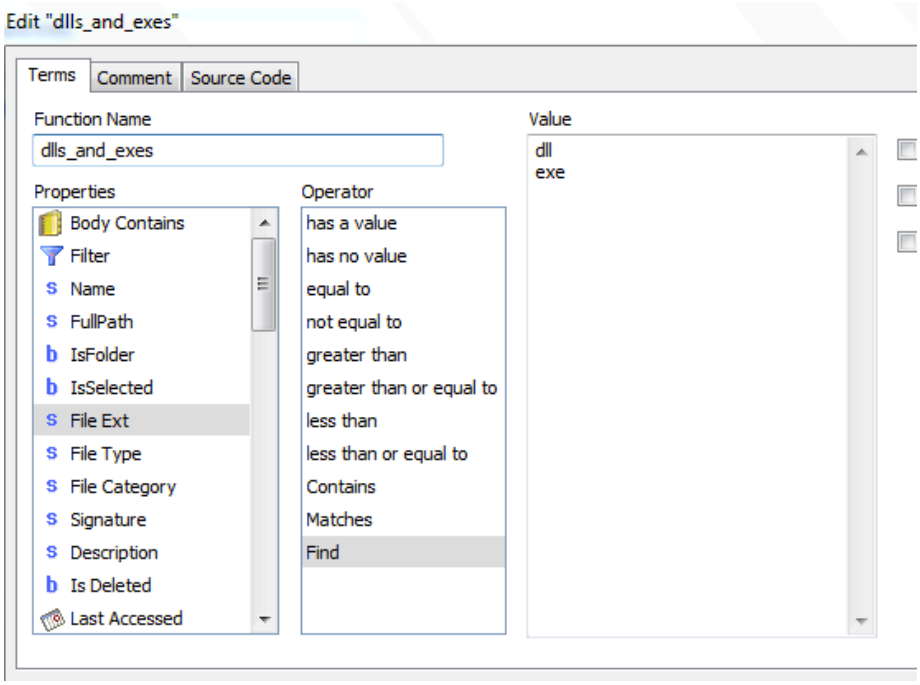


Rename it to “DLLs and EXEs”. Right-click on the “f() Main” section to add a condition; click “New”:

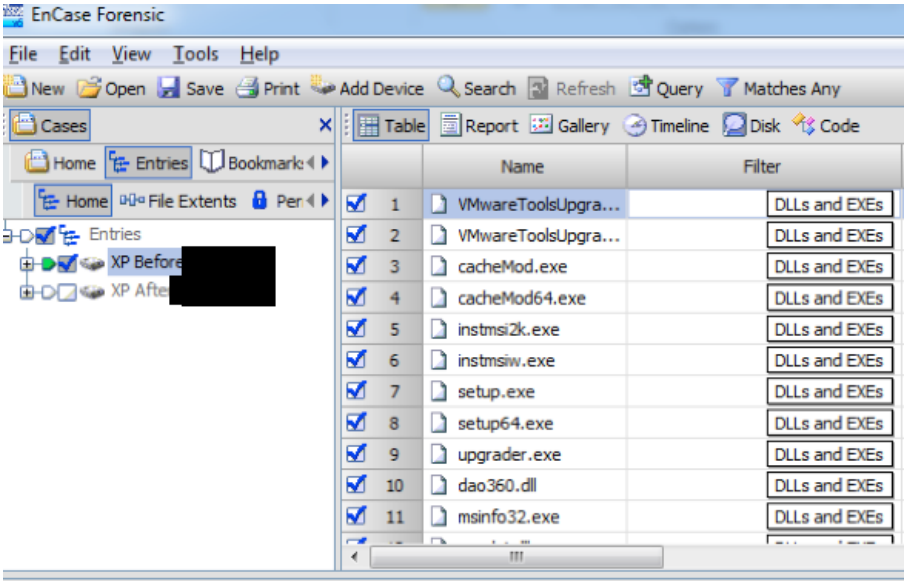


We’ll make a condition for both DLLs and EXEs. Name the function “dlls_and_exes” and choose “File Ext” from the first column and “find” in the second column, then type “dll” in the value column, then “exe” on the next line:

Jamie Levy
jamie.levy@gmail.com
http://gleeda.blogspot.com

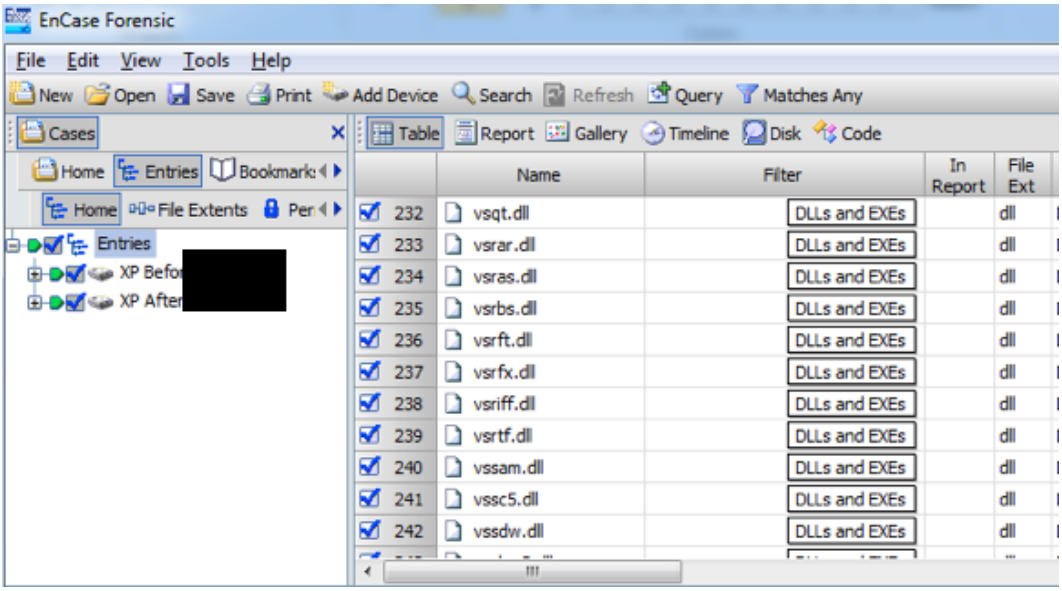


Press "OK" twice to save and get out of the condition writing menus. Now double-click your newly created condition. You will not see any files in the table view until you "green-plate" one of the evidence drives. "Green-plate" the original drive and you will see all the DLL and EXE files in the table view. You can select all of these files ("blue-check") by clicking the first one, pressing "CTRL" and then "SPACEBAR".



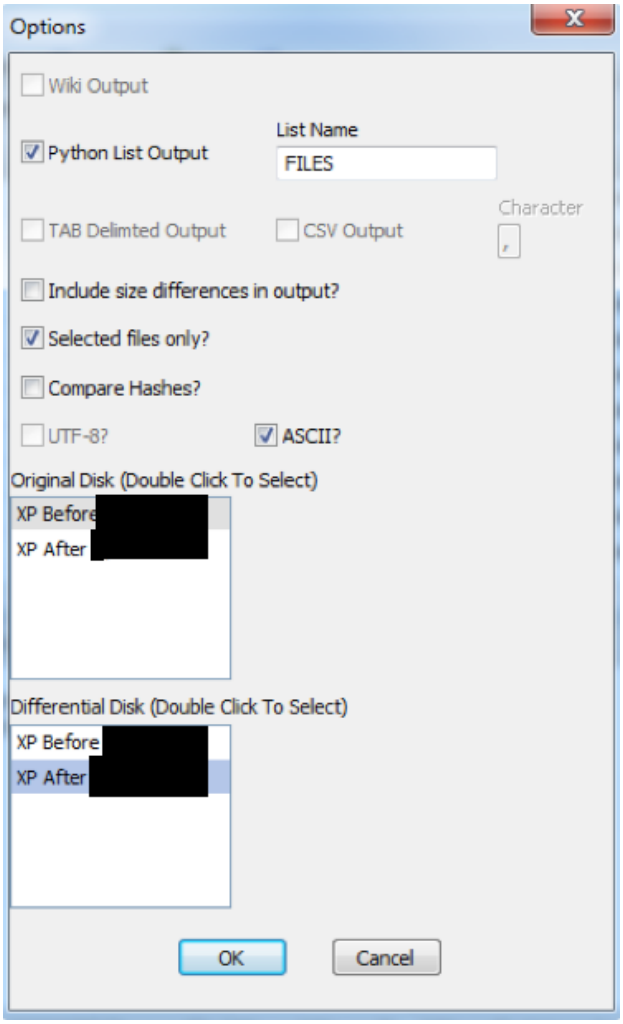
You can green-plate the two evidence files that you want to compare at the same time and select all files at once to save time:

Jamie Levy
jamie.levy@gmail.com
http://gleeda.blogspot.com

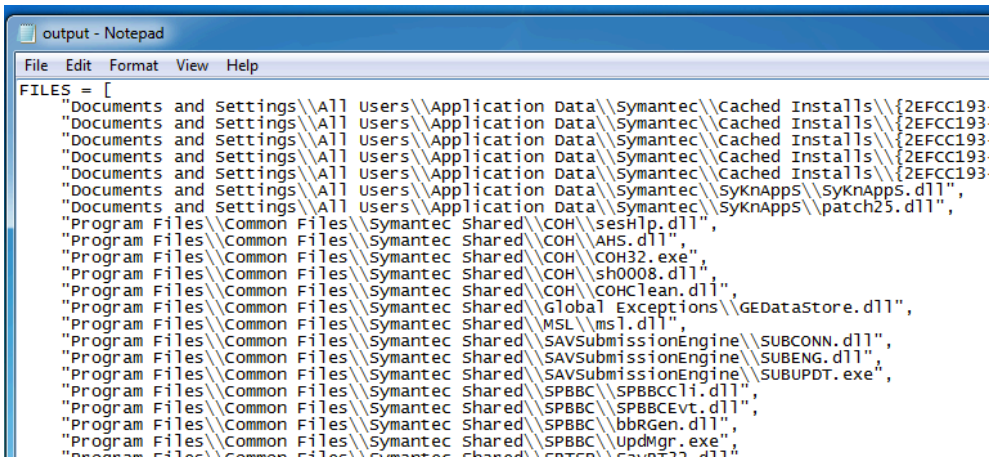


Now run the Differential.EnScript and make sure to choose “Selected files only?” You can see an example setup of the script below, where I am only interested in new files:

Jamie Levy
jamie.levy@gmail.com
http://gleeda.blogspot.com



Checking the output I can see that I have all the files I want:



Jamie Levy
jamie.levy@gmail.com
http://gleeda.blogspot.com