PyVol
Steve Lang - wonder9876

03-25-2011

Freelancer Project

Created: 03/24/2011 at 10:55 CET
Project Creator: hdrakensen

Description

A graphical user interface is required to use the tkinter module in python to create a series of related GUI platforms to process volatility framework scripts.
interfaces should be 1.main menu
2.menus
3.individual menu items .e.g connections
the main menu should have the list of the script names,which when clicked open separate "pages".in this should be choices on what the user will like to do,such as choose volatility script,choose memory image file to load from computer,analyse memory dump image file,print results and save results to database.the database should be made of either sqllite or ms access.
if a wrong file type has been selected the user should be informed,if the user has not entered a value correctly or they have left a blank field they should be informed.
a separate gui should be able to allow the user to open the db and choose which results to print or view.

Additional Informations :
Hi,
yes i want an implementation of volatility tools in GUI.The following tools scripts from volatility framework need to be used,connections,processes,psscans,pslists and network.these should be used to analyse a memory dump image and the results printed or saved to a db. this is based on the website https://www.volatilesystems.com/default/volatility

i can run all the commands using command line but i want a GUI interface running the commands e.g if i run this command python volatility ident -f c:\images\image1.dump
i get the results i want,now i want the same but in GUI.SIX OR MORE GUI pages will do,that equates to four volatility scripts.
THE USER SHOULD BE ASKED TO EITHER PRINT OR SAVE THE RESULTS TO A DB,(SQLITE OR ACCESS)

THE PDF YOU SENT IS A VERY GOOD MODEL OF HOW I WOULD LIKE MINE TO LOOK LIKE,SO INSTEAD OF PROCESS BUTTON YOU WOULD HAVE ANALYSE(WHICH WILL ANALYSE THE IAMGE FILE AND GIVE THE RESULTS)

THE SAMPLE YOU PROVIDED IS EXACTLY WHAT I NEED,
IF YOU CAN MAKE IT THIS WAY
FIRST SCREEN-MAIN MENU
CONTENTS-NAME OF APP.,BUTTTON TO GO TO A SCREEN SIMILAR (OR THE ONE)TO THE ONE YOU PROVIDED,ABOUT BUTTON,CONTACTS,
SCREEN TWO SHALL BE THE ONE YOU PROVIDED
OTHER SCREENS-ABOUT THE SOFTWARE,
CONTACTS- OF THE OWNER (ME)IL WILL INSERT MY NAME IN THE CODE WHEN YOU HAVE DELIVERED IT.

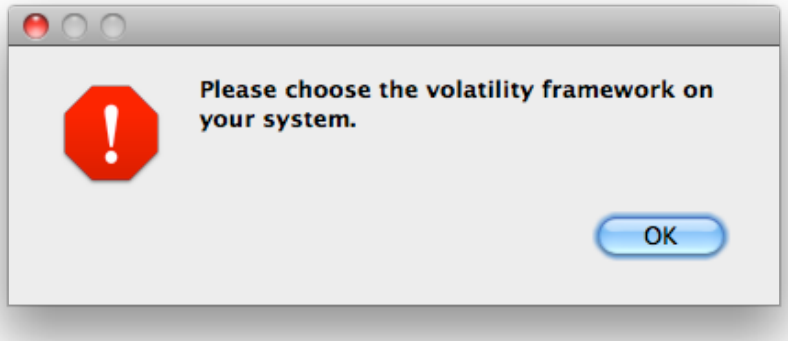
YOU CAN USE QT,MAKE SURE ITS CROSS PLATFORMED,THAT IS CAN OPEN IN MOST OPERATING SYSTEMS,I LIKE THE COLOR AND FEEL OF THE SAMPLE YOU SENT.

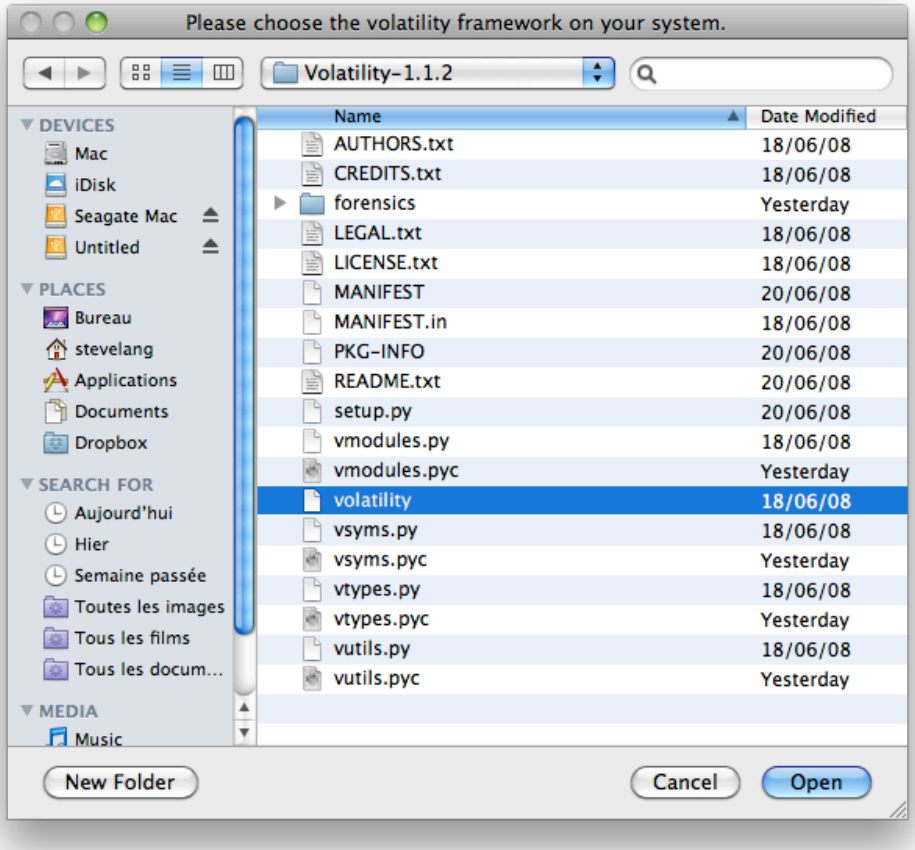
THE SAMPLES YOU PROVIDED ARE CORRECT,EXCEPT THAT YOU DIDNT INCLUDE A BUTTON/DROP DOWN BUTTON TO SELECT THE VOLATILITY SCRIPT TO USE,E.G CONNECTIONS,PSSCANS,PSLISTS,NETWORKS.BECAUSE WHEN YOU CHOOSE IMAGE,YOU HAVE TO CHOOSE THE VOLATILITY TOOL TO USE ON IT.THIS IS THE REASON I INCLUDED THE COMMAND LINE EXAMPLE
SOME COMMANDS I USED ARE: CONNECTIONS-PYTHON VOLATILITY CONNECTIONS f C:IMAGE1/IMAGE1.IMG
PSSCANS-PYTHON VOLATILITY PSSCANS C:IMAGE1/IMAGE1.IMG

Work Complete :
waiting for validation :

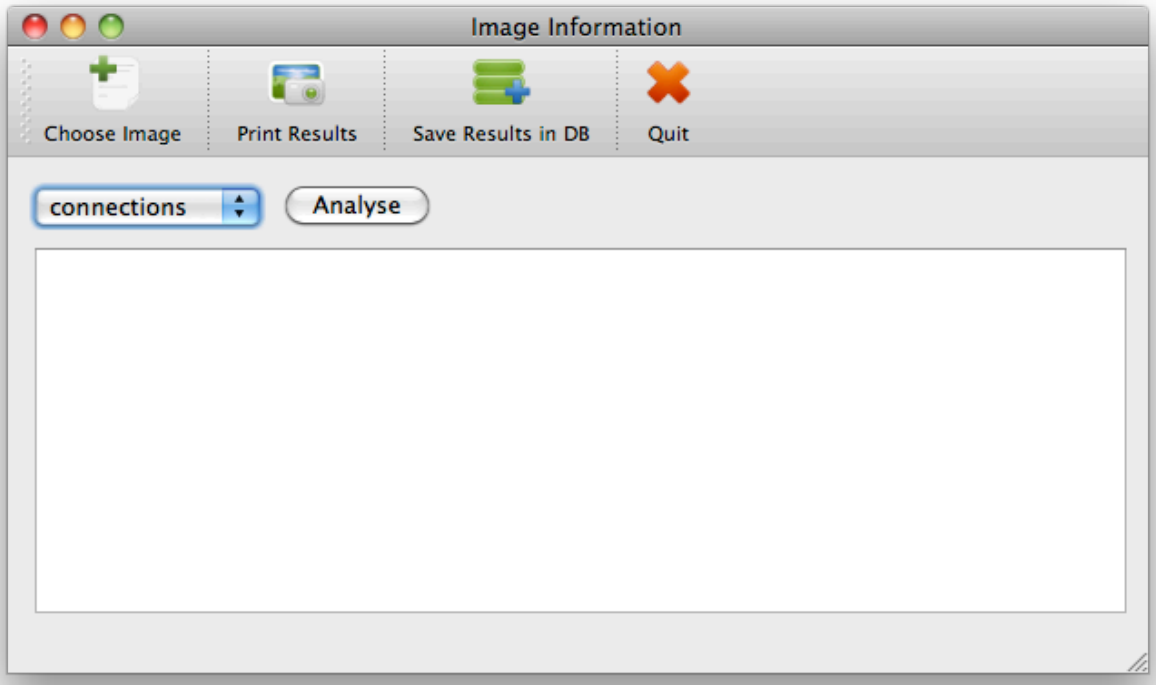
MainWindow :

Click on Image Information :
On the very first launch of the program on your system, it'll ask you to choose the volatility framework on your system.



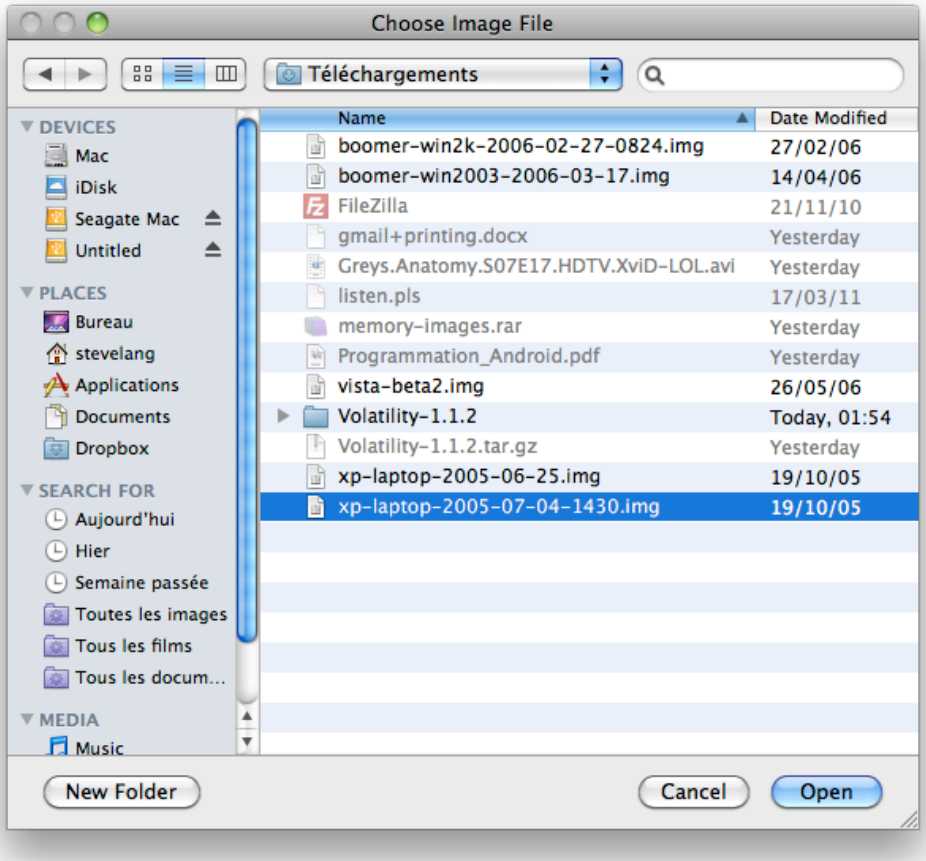


Now that the path to your framework is known by PyVol everything is OK.
Click on Image Information :

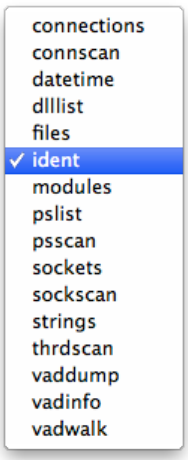


‘Analyse’ button will generate an error if no image has been chosen :

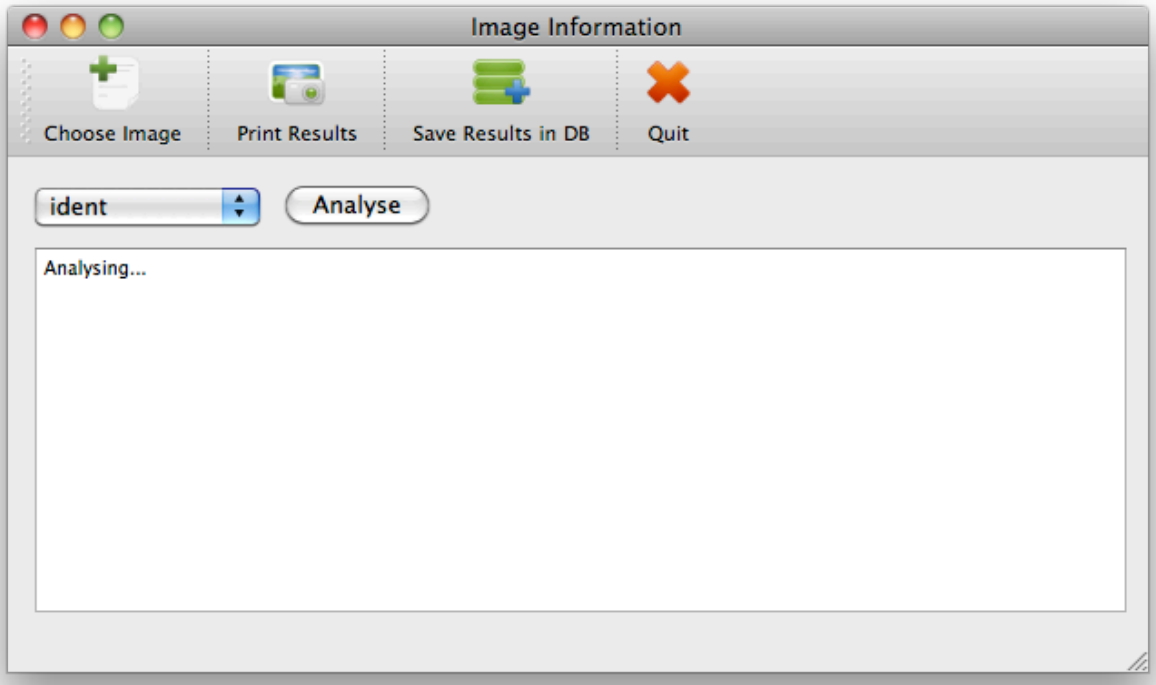
Let’s select an image file to analyse :



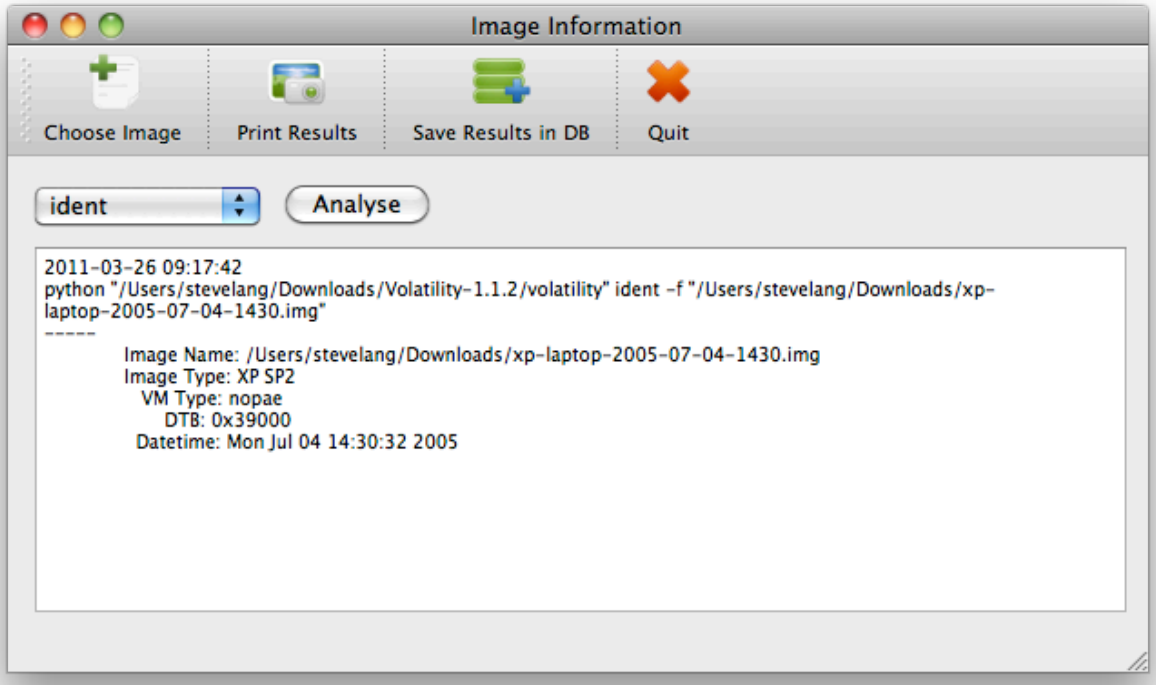
Let’s select an option in the list :



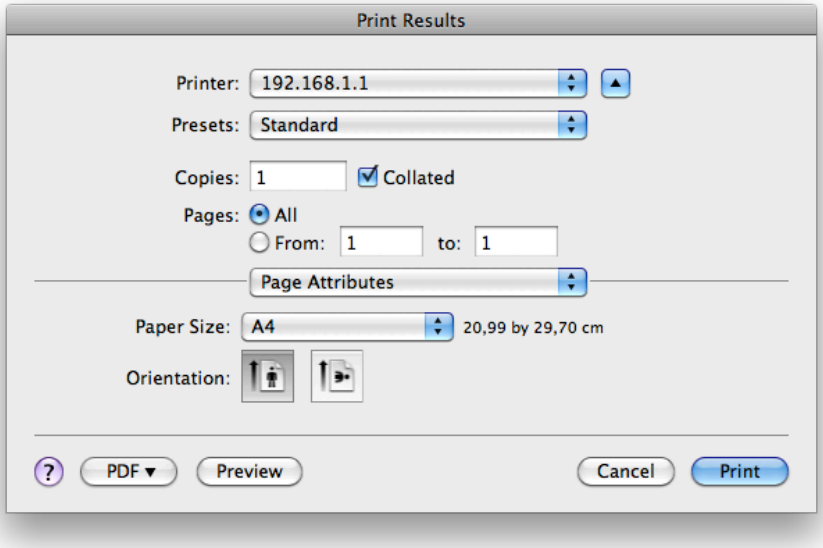
Time to Analyse :
the command will always be formated like this :
‘python [path to volatility] [option] -f [path to image]’



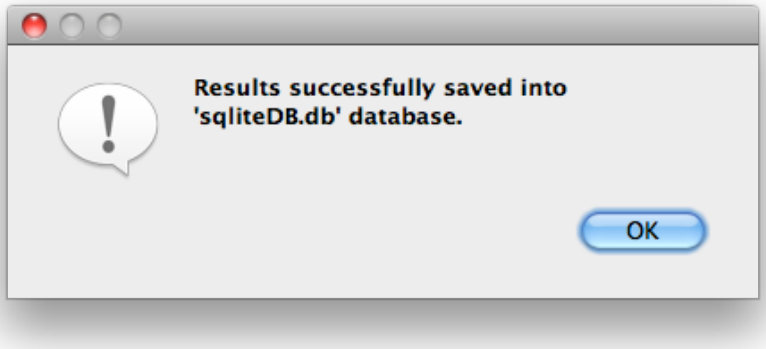
Note : Every analyse is threaded
After computing:



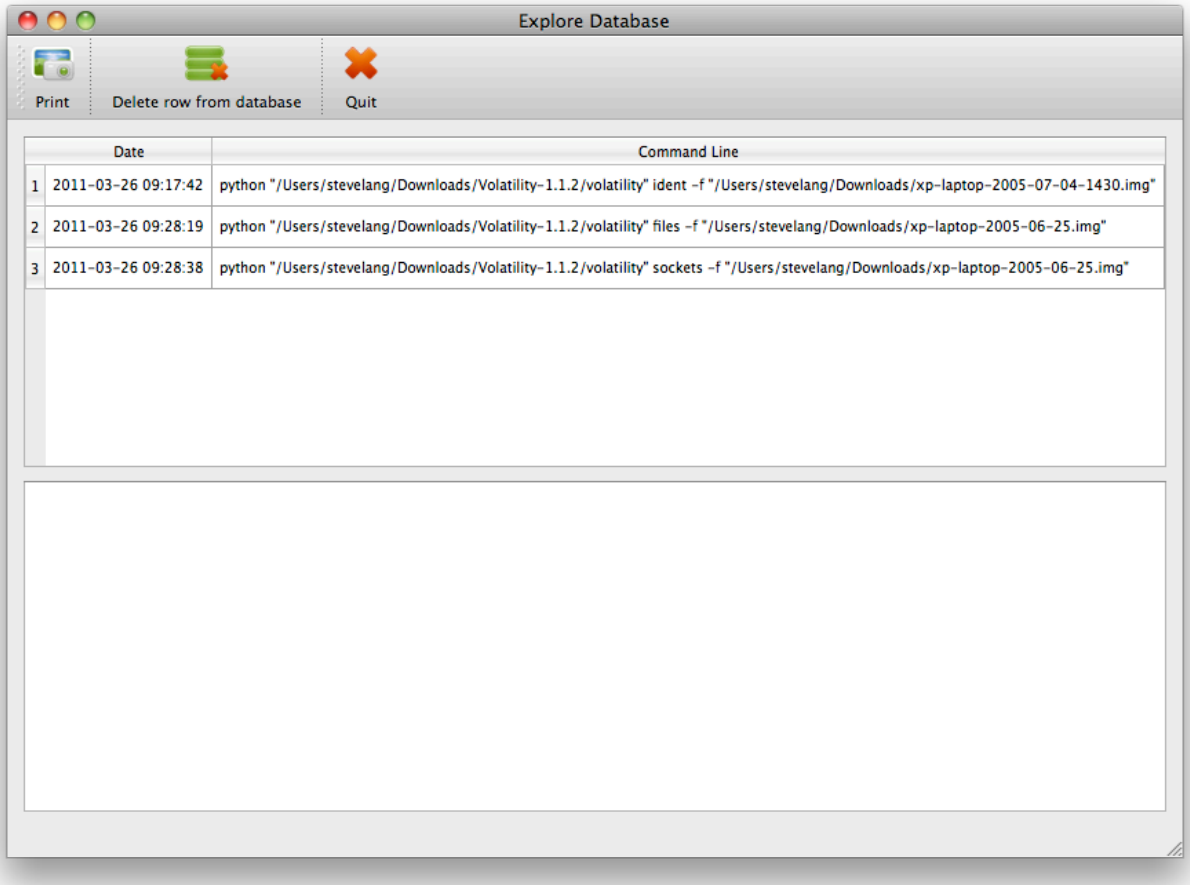
You can print the results:



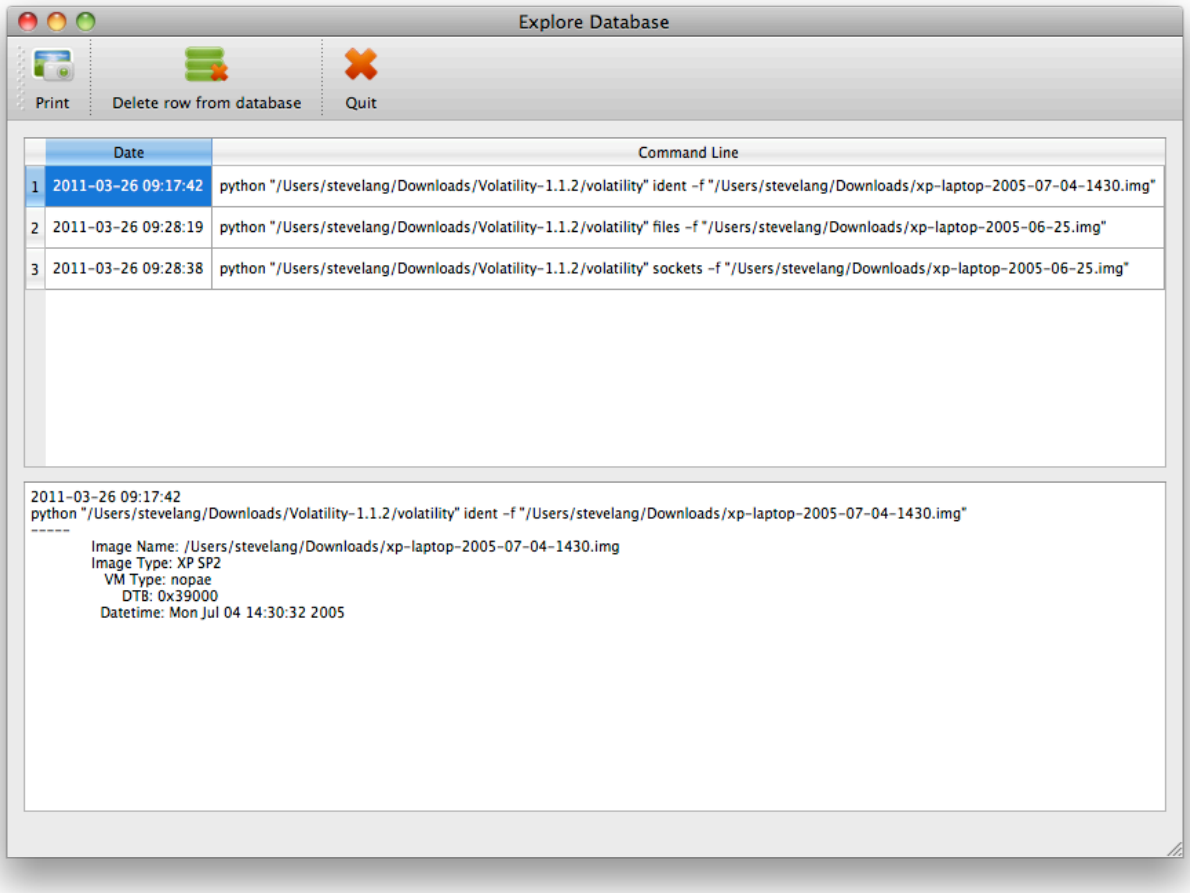
You can save the results in the DataBase ‘sqliteDB.db’:



Explore Database :

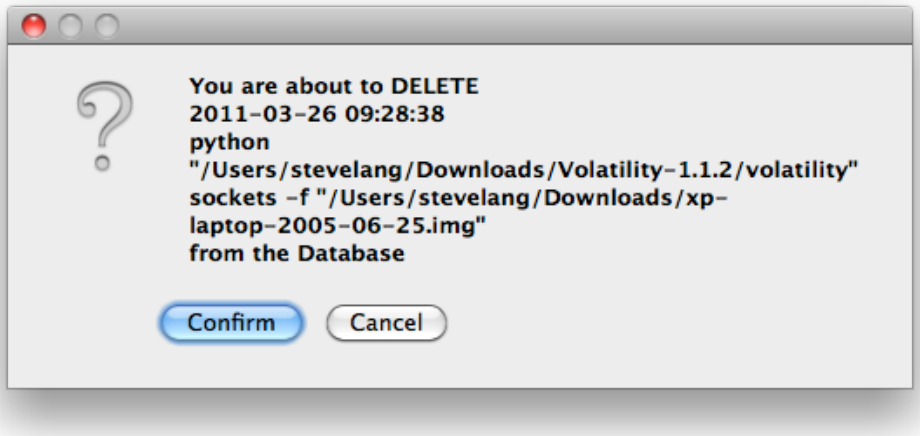


Select a Date or a Command Line

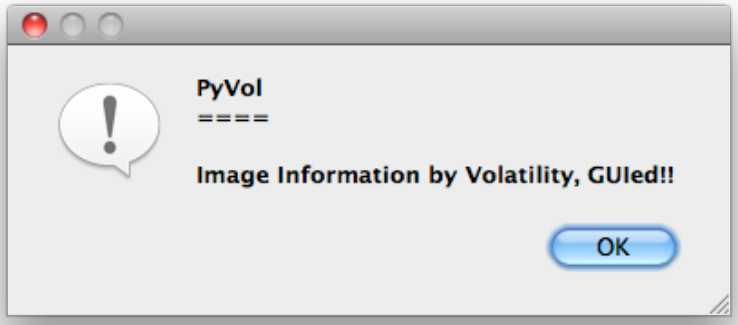


Note:
- Printing is available
- You can act on the database to delete an entry.

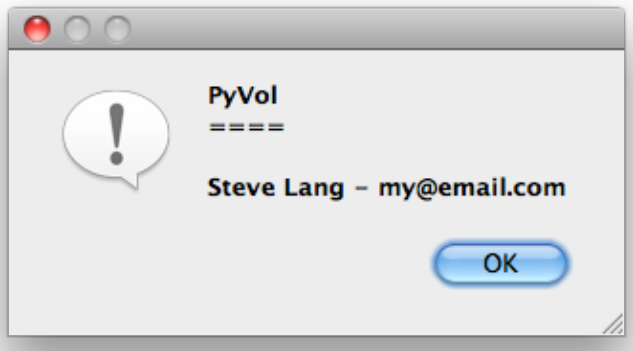
Delete an entry :



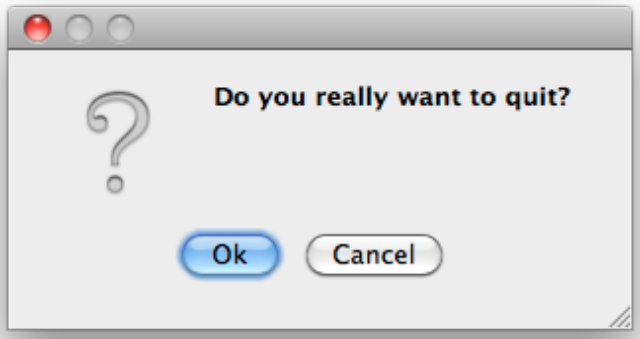
Note : About and Contact can be modified at the end of PyVolMain.py in the about and contact definitions.
About :



Contact :



Quit :



Tricky Question !