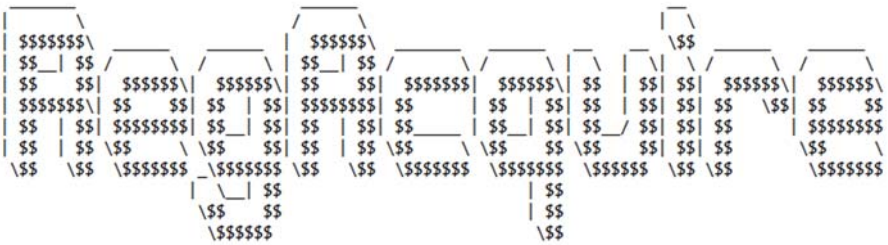
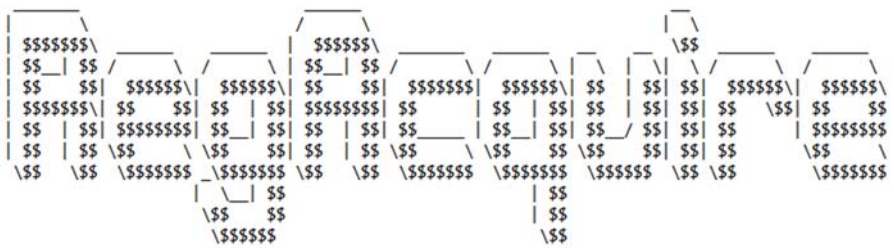


&

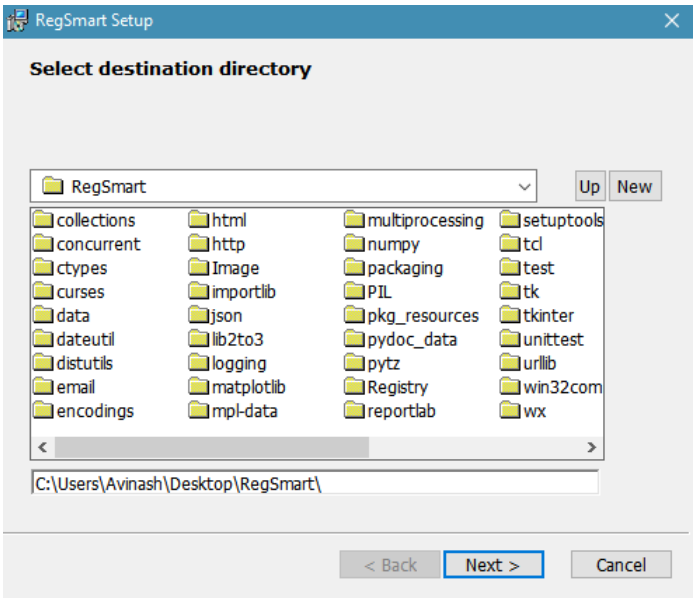
USER MANUAL



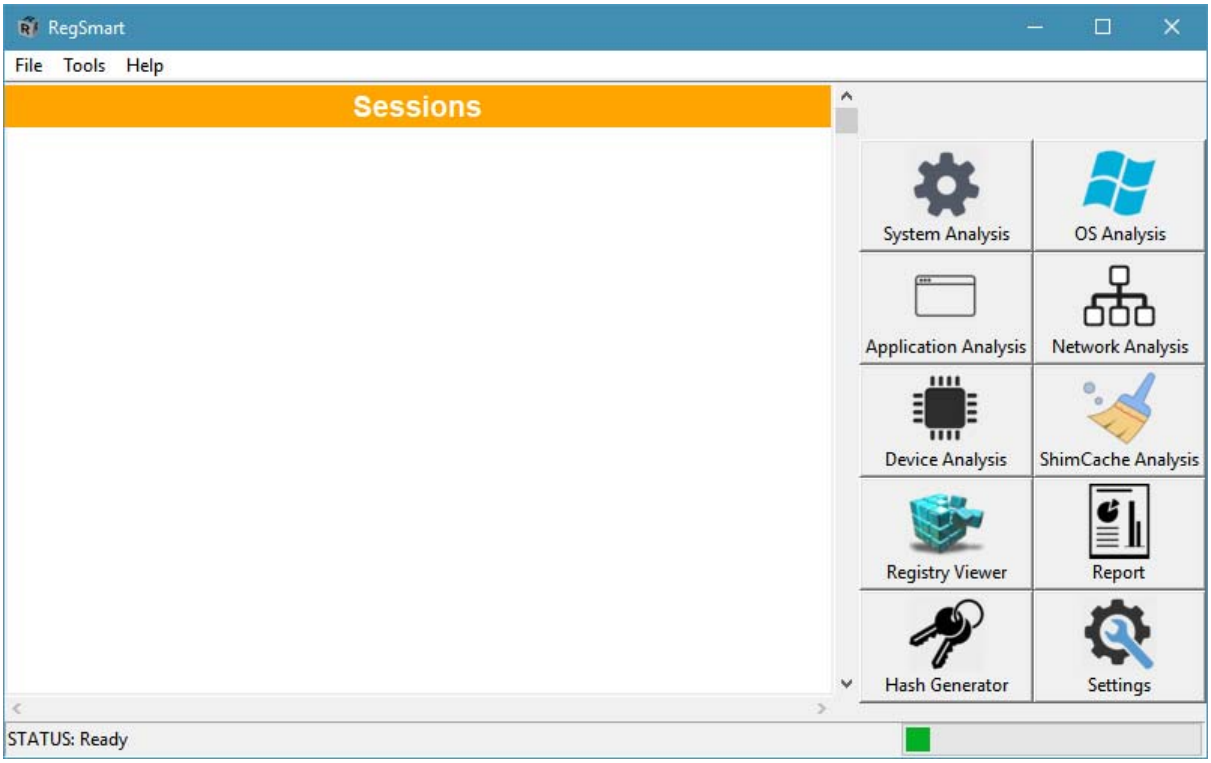
RegAcquire is a simple batch program that acquires Windows Registry dumps on a live computer. The purpose of this tool is for live acquisition and aids incident response. For simplicity this script and the necessary supporting files have been converted to an executable. RegAcquire is simple to use, all you need to do is run the executable and the program will automatically acquire the registry dumps and save it to a folder called “dumps”. Please note that if you acquire more than one dump from the same machine on the same day it will ask you to overwrite, however It moves the old dumps to a folder called “deleted” in case you didn’t mean to delete it. The dumps that will be created will be stored in a folder combined from the “username_machinename_date” this folder will be needed for creating a new session and importing the dumps in RegSmart as illustrated later in the document.

RegSmart is an analysis tool that aims to harness the Windows Registry and extract information from various parts of the Registry to easily perform forensic investigations. There are several analysis processes that are performed. Below are instructions on how to use the program:

1. **Run the MSI installer, please make sure it installs to the desktop, or documents and not program files due to permission requirements when executed.**

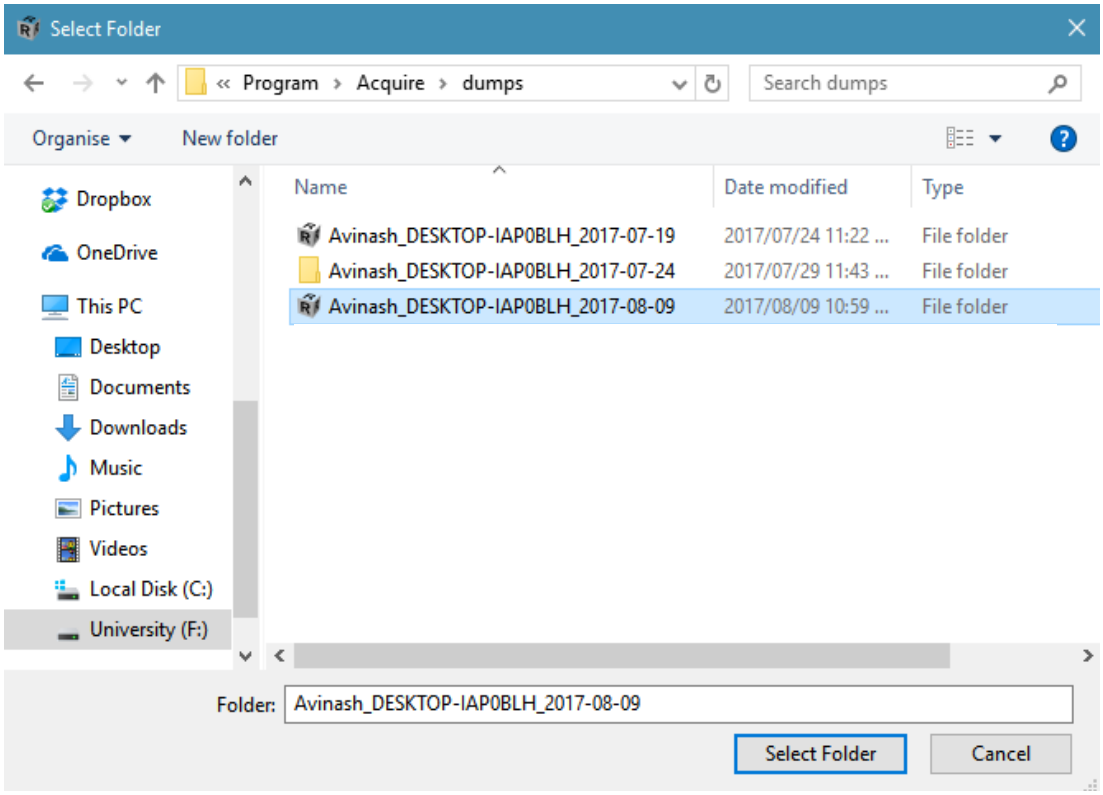


2. **Once the installation is complete you will see a shortcut icon on the desktop called "RegSmart" double click on it and it should open if it doesn't then please run it in Administrator mode.**
3. **You will be prompted to enter your name followed by your ID, this ID can be the one given by your organization or any unique identifier.**
4. **The program will then load any available sessions.**

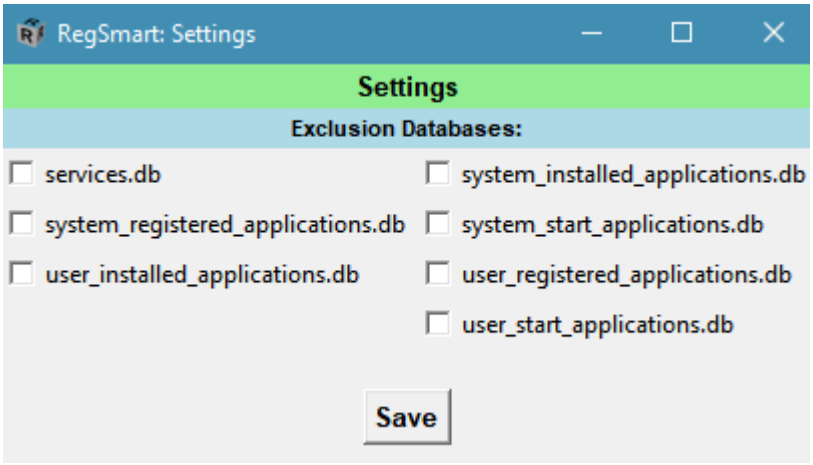


5. **If there are no available sessions, you need to add one by clicking "File->New Session"**

6. **Then navigate to the acquired dumps from RegAcquire and import the folder so that RegSmart can validate and process the data.**



7. **You may notice that an icon on the folder, this is to tell you the entire folder is needed for the import and validation of the Registry dumps.**
8. **Once you have selected the folder RegSmart will start importing the dumps followed by validating the dumps to check if they have been modified. If there is any errors, they will be displayed and the session will not be created.**
9. **Once validated and successfully loaded it will appear in the sessions column, if you wish to change the session you can simply close the session via "File->Close Session" or simply click on another session to load.**
10. **There is a list of tools available on the right hand side that perform different types of analysis.**
11. **There is also a hash generator that can hash files and folders, the way folders are hashed is all the sorted contents of the folder and other folders inside (i.e. recursively) are hashed and stored once all the contents are hashed they are concatenated and hashed again to get the final hash of the folder.**
12. **Settings: For now, there is only one type of settings and that is exclusion databases, these exclusion databases are only used for report generation, to limit the amount of data that is generated. These databases act like a filter and filter out items that not relevant to the organization. These databases are not maintained and by default, they are empty and not set to be filtered. These databases are just for organizations to maintain and exclude information that they find is not useful, since there are so many items and events that are system related and may have no use for the organization.**



13. **Reporting: This module allows you to choose what type of analysis you wish to include in the report and requires you to enter some business information that will be attached to the report. Once a report has been generated if it was validated and if no errors or nothing invalid happened there will be a stamp saying "RegSmart certified". This holds no warranty or guarantees this is just to notify that the reporting process completed successfully with all the necessary checks performed was successful.**

To get more information about each type of analysis you can visit the website available on the help menu of RegSmart interface.

If there are any queries or problems, please feel free to contact:

Avinash Singh at tashan.avi@gmail.com