DIGITAL FORENSICS II
Experiment 9

Submitted to: Mr. Keshav Kaushik
Submitted by: Kashish Srivastava
500067405
R134218079

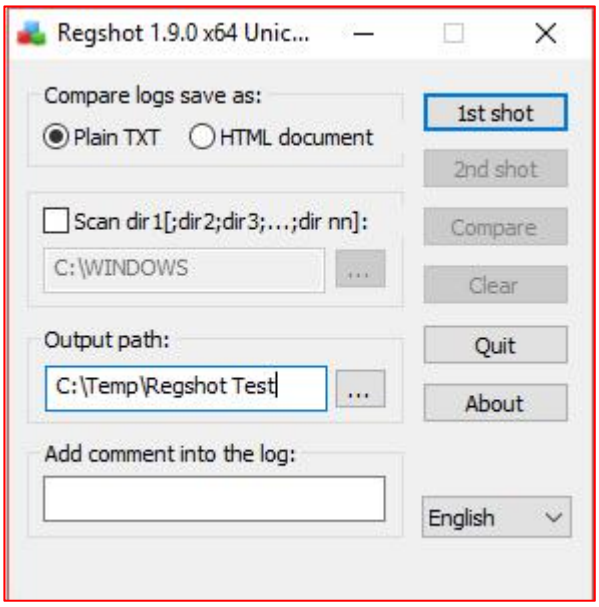
Aim: Analyzing Registry files using Regshot

Regshot is an open-source (LGPL) registry compare utility that allows you to quickly take a snapshot of your registry and then compare it with a second one - done after doing system changes or installing a new software product.
The goal is to identify any changes to the registry that the malware made. This may give more indication as to what the malware is capable of, if any additional files are dropped, or any other Indicators of Compromise ("IOCs"). In many cases, including my own, Regshot lives within its own Virtual Machine that is reserved for dynamic analysis.

Regshot has very simple steps:

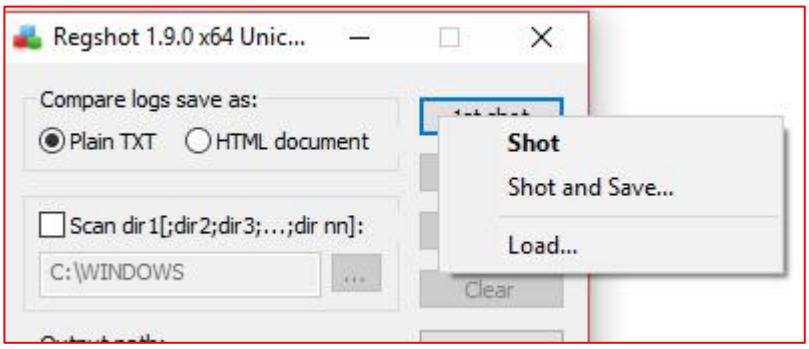
1. Take a shot of the system's registry now.
2. Do something to the system.
3. Take a shot of the system's registry again.
4. Wash, rinse, and repeat.

Assigning the path. C:\Temp\Regshot Test



There are options to save the changes as either a text or HTML file.

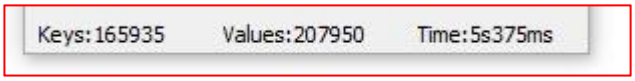
When taking registry shots, the user is presented with the options Shot, Shot and Save, or Load.



These are some of the greatest options available in Regshot.

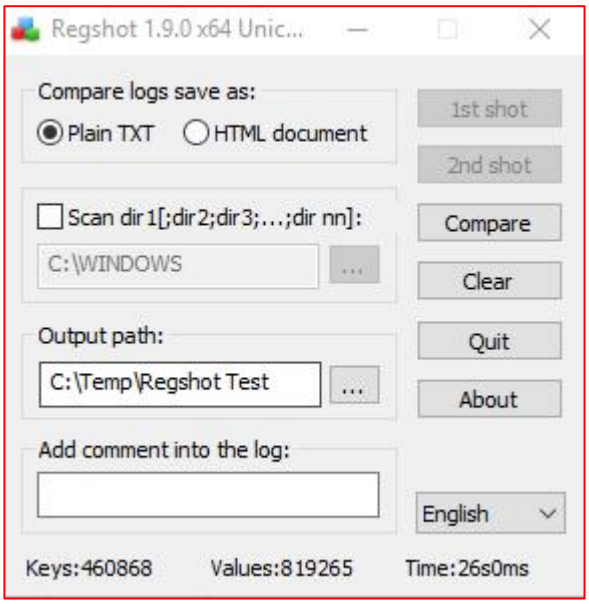
- **Shot** will simply take a shot of the current system's registry. The calculations of taking this are provided at the bottom of the GUI.
- **Shot and Save** will take the same shot of the registry, and also save it to an encoded file (either ANSI or Unicode)
- **Load** allows you to load a **previously-taken** Regshot hive for either the before or after position.

Once the shot is taken, you'll be presented with statistics on the shot:



Now, we do some things. Run or move some files around the system, open a file or two.

Clicking **2nd shot** will take the second shot. At this point, both snapshots of the registry are saved temporarily. Once this has taken place, the 'Compare' button will become available:



If we haven't saved any files, Regshot will popup a text editor with the changed registry keys within. The top of the file begins with system identification information:

```
Regshot 1.9.0 x64 Unicode
Comments:
Datetime: 2020/12/2 04:21:30 , 2020/12/2 04:22:16
Computer and Username too
```

Below are the keys that were changed.

```
----------------------------------
Total changes: 21
----------------------------------
```

Not only are we presented with the number of changes, but also the registry contents:

```
\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\MinPos1920x1080x96(2).x: 0xFFFF8300
\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\MinPos1920x1080x96(2).x: 0xFFFFFFFF
\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\MinPos1920x1080x96(2).y: 0xFFFF8300
\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\MinPos1920x1080x96(2).y: 0xFFFFFFFF
\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\WinPos1920x1080x96(2).left: 0x00000910
\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\WinPos1920x1080x96(2).left: 0x000008D6
\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\WinPos1920x1080x96(2).top: 0x000000F3
\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\WinPos1920x1080x96(2).top: 0x0000018B
\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\WinPos1920x1080x96(2).right: 0x00000D83
\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\WinPos1920x1080x96(2).right: 0x00000D49
\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\WinPos1920x1080x96(2).bottom: 0x00000349
\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\WinPos1920x1080x96(2).bottom: 0x000003E1
```

In this example I simply changed the ShellBags for a few folders.

For development purposes,we can take a shot and see what installing your application does to the system