***Incident Response Triage 2:***

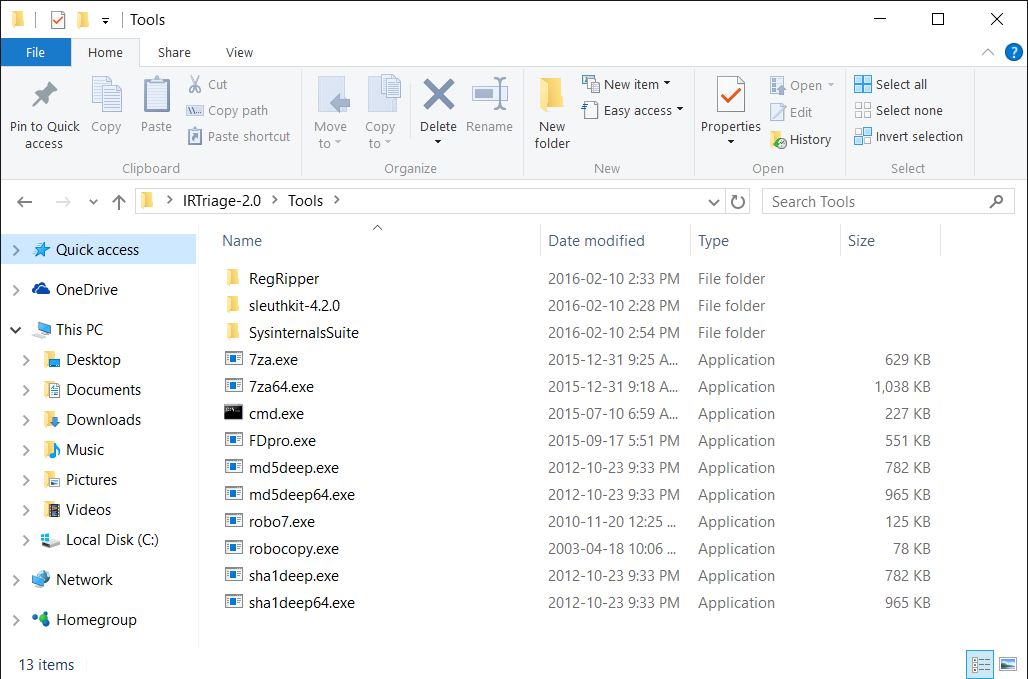
IRTriage is intended for incident responders who need to rapidly acquire host data. The tool will run a plethora of commands automatically based on the responder's selection. Data will copy to a unique subfolder located where the script is stored. IRTriage is intended to be run from a flash drive locally on the machine, or via network shared drive.

***Dependencies***

IRTriage utilizes various tools in order to obtain system artifacts\information. Some of the utilities are included, others are not due to licensing issues. You can get them from the following locations:

* DumpIt from MoonSols: <http://www.moonsols.com/>
* Sysinternals Suite from Microsoft and Mark Russinovich: [http://technet.microsoft.com/en- us/sysinternals/bb842062](http://technet.microsoft.com/en-%20us/sysinternals/bb842062)
* RegRipper from Harlan Carvey: [http://code.google.com/p/winforensicaanalysis/downloads/list](%20http://code.google.com/p/winforensicaanalysis/downloads/list)
* md5deep and sha1deep from Jesse Kornblum: <http://md5deep.sourceforge.net/>
* 7zip Command Line: <http://www.7-zip.org/>

The tools will need to be placed in the appropriate locations in order to run properly. When you download IRTriage, it is zipped, unzipped you’ll notice a Tools folder. Everything needs to be placed in there; RegRipper and SysInternalsSuite are in their own folders for ease of viewing. The folder should look something like this when completed:



***Triage.INI File***

Version 0.78 of Triage-ir was the first implementation of an INI file to formulate how you wished to configure the default settings. This allows for unique customization of the application without needing to know how to modify the source code and recompile it completely. The INI is structured currently with 2 sections: GUI and Function. GUI is straight forward, either enter “Yes” or “No” and this will either load the GUI or run the functions from the command line. The “Function” portion is a list of runnable functions within the utility. Again, you can set the function to “Yes” or “No” and this will select whether or not the function will run.

***Graphic User Interface***

The default GUI:

