Incident Response Triage 2:

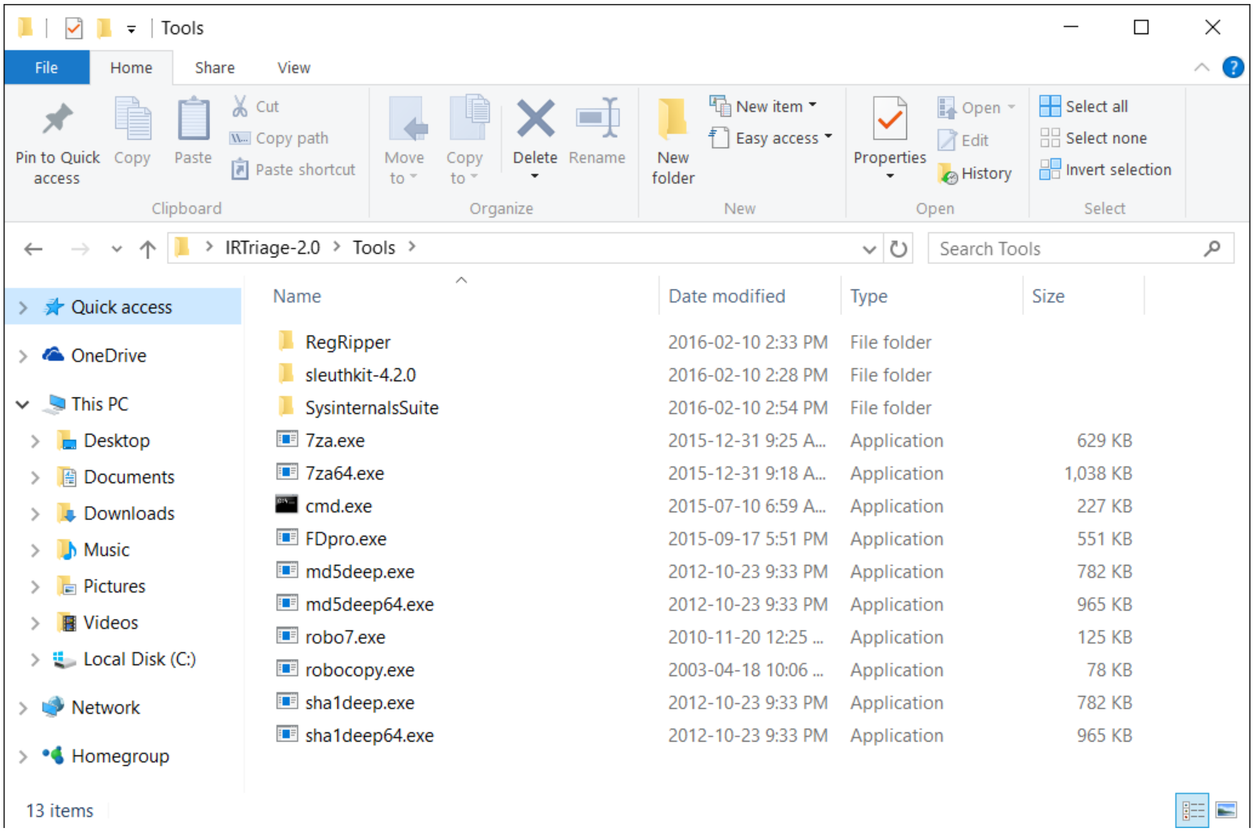
IRTriage is intended for incident responders who need to rapidly acquire host data. The tool will run a plethora of commands automatically based on the responder's selection. Data will copy to a unique subfolder located where the script is stored. IRTriage is intended to be run from a flash drive locally 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
- RegRipper from Harlan Carvey: http://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:



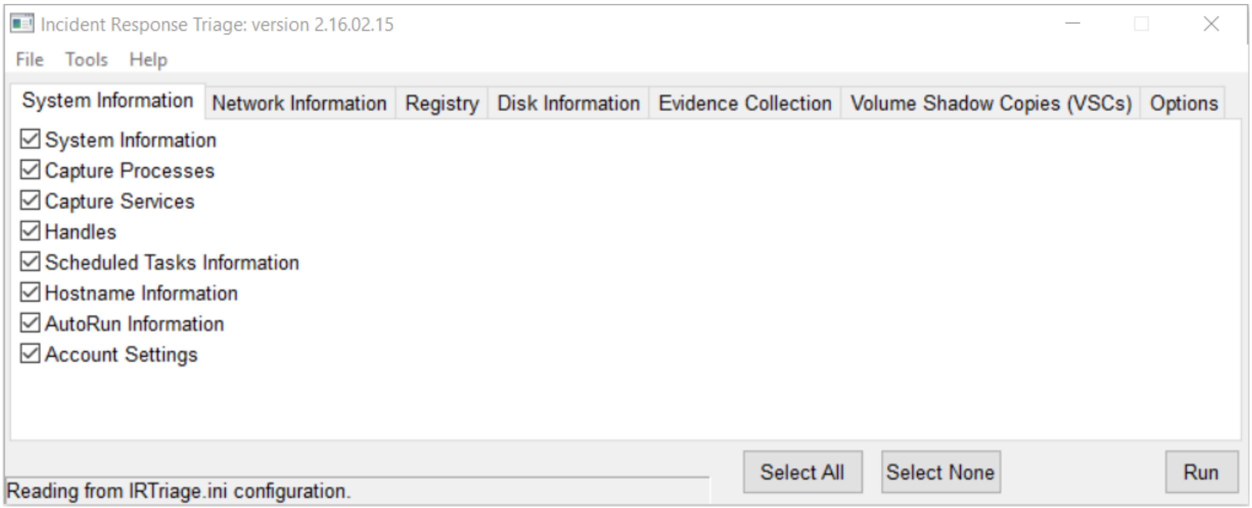
Name	Date modified	Type	Size
RegRipper	2016-02-10 2:33 PM	File folder	
sleuthkit-4.2.0	2016-02-10 2:28 PM	File folder	
SysinternalsSuite	2016-02-10 2:54 PM	File folder	
7za.exe	2015-12-31 9:25 A...	Application	629 KB
7za64.exe	2015-12-31 9:18 A...	Application	1,038 KB
cmd.exe	2015-07-10 6:59 A...	Application	227 KB
FDpro.exe	2015-09-17 5:51 PM	Application	551 KB
md5deep.exe	2012-10-23 9:33 PM	Application	782 KB
md5deep64.exe	2012-10-23 9:33 PM	Application	965 KB
robo7.exe	2010-11-20 12:25 ...	Application	125 KB
robocopy.exe	2003-04-18 10:06 ...	Application	78 KB
sha1deep.exe	2012-10-23 9:33 PM	Application	782 KB
sha1deep64.exe	2012-10-23 9:33 PM	Application	965 KB

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.

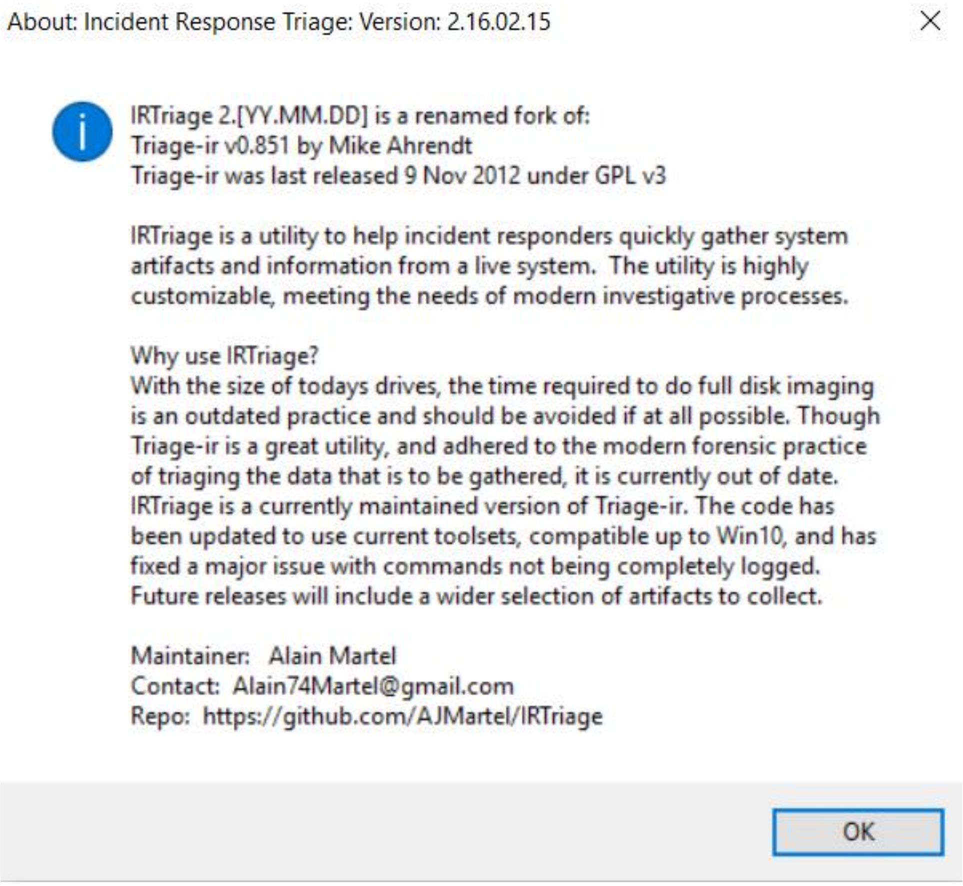
Graphic User Interface

The default GUI:



☑ System Information
☑ Capture Processes
☑ Capture Services
☑ Handles
☑ Scheduled Tasks Information
☑ Hostname Information
☑ AutoRun Information
☑ Account Settings

Reading from IRTriage.ini configuration.



About: Incident Response Triage: Version: 2.16.02.15

IRTriage 2.[YY.MM.DD] is a renamed fork of:
Triage-ir v0.851 by Mike Ahrendt
Triage-ir was last released 9 Nov 2012 under GPL v3

IRTriage is a utility to help incident responders quickly gather system artifacts and information from a live system. The utility is highly customizable, meeting the needs of modern investigative processes.

Why use IRTriage?
With the size of todays drives, the time required to do full disk imaging is an outdated practice and should be avoided if at all possible. Though Triage-ir is a great utility, and adhered to the modern forensic practice of triaging the data that is to be gathered, it is currently out of date. IRTriage is a currently maintained version of Triage-ir. The code has been updated to use current toolsets, compatible up to Win10, and has fixed a major issue with commands not being completely logged. Future releases will include a wider selection of artifacts to collect.

Maintainer: Alain Martel
Contact: Alain74Martel@gmail.com
Repo: https://github.com/AJMartel/IRTriage