Yet Another Forensic Tool (YAFORTO)

Welcome to the powershell script Yet another Forensic tool script (YAFORTO). This repository is the home of the Powershell Script I designed. Having earned the Giac Certified Forensic Engineer certification, I saw an opportunity to combine some initial steps taken, and fulfill a need to remotely capture information using available tools. I hope you find it useful.

The goal of the script is to use other Forensic engineer's windows executables to:

- Gather a remote forensic triage image
- Gather a remote Memory dump
- Ask the Forensic examiner about what type of investigation this is
- Use that information to comb through the forensic image and memory dump to give the examiner some starting information.

This script is not meant to replace any tools. Rather, it's designed for the growing avenue of Forensic response inside an Incident response framework. Ideally the forensic analyst would take a full disk image, a full memory image, and bring both into a Forensic Platform for investigation using multiple tools. The use of this tool is to help the forensic examiner determine if the effort and time needed matches the initial information found. Instead of obtaining a full image. This script runs a series of commands associated in grabbing a Triage image.

8-22-2019

Final release