Pros:

Very good for looking at network traffic.

Lists processes currently running and the PIDs, PATH, what user is running them, and the parent process.

Lists the drivers for the computer.

Can list the entire filesystem but you can not view what the file contains, only the name and if it has been modified. Can not see deleted files on the system.

Cons:

To start you will be collecting the data using either the standard collector or the comprehensive collector.

The comprehensive collector is recommended for if you do not know what to look for. I would personally recommend the comprehensive collector running it before and after an attack. Using this program with the comprehensive collector is slow, depending on how much information is stored on the device. The collector is more of a tool to funnel your view to look for with other tools. Redline is not supposed to be used by itself, that is at least the feeling I get from the tool.

The tool is at its most powerful when it can be paired with another forensics’ tool like FTK or if you have physical access to the machine to see the files that got moved/edited. The downsides of the tool is the linear scale of time with amount of information on the system to do a comprehensive search.

There is options to remove and create your own collector. There are tabs that separate what you can edit, Memory, Disk, System, Networking, and Other. Memory has Process Listing, Drivers Enumeration, Hook Detection, and you can acquire a memory image for of the device. Disk has File Enumeration where you can get deleted files in RAW format only, and you can get the hash values of the files to compare between your original scan and after your scan. You can also enumerate the disks and the volumes on the system. The System tab contains the system information, the registry enumeration, and gathering event logs. Networking can grab the ports on the machine that are open, ARP, DNS, and Routing tables. Browsing history is also available if you are inclined to search through there for websites that are suspicious. The task tab contains Services, Tasks and Common Persistence Mechanisms.