D18 USB Portable Operating System and File System Circumvention Capability Analysis

Monte Swank, BS, 1401 Forensic Science Drive, Huntington, WV 25701*

After attending this presentation, attendees will be familiarized with the functionality of portable operating systems and programs used on USB flash devices, as well as their file system circumvention capabilities.

This presentation will impact the forensic community and/or humanity by identifying residual data specific for USB portable operating systems.

The emergence and availability of personal computer technology has resulted in a broad spectrum of uses, ranging from the recreational to the criminal. Everyday computer use inherently leaves traces of residual data available for forensic analysis and identification. With the advent of solid- state data storage devices (e.g. USB flash media, memory cards), programs and/or operating systems can be made portable while essentially circumventing normal operating system artifacts. These removable storage mediums are becoming increasingly large in memory and small in size while their prices drop.

Even though a USB apparatus may be small and easily removed from a computer, it is not gone without a trace. Plugging in a thumb drive creates several identifiers in the registry, which can be used to help identify a particular device. The registry is made up of a series of files that is utilized by Microsoft Windows to store various computer configurations. There is a lot of information that a digital investigator can ascertain such as: typed URLs, run command history, and user accounts. Once individual keys in the registry are identified, their last write times can be used to create a timeline of events.

Four programs/portable operating systems were used in this study to determine their operability and circumvention success; Flash-Puppy (portable version of linux), U3 (dual partition file system with start menu), MojoPac (virtual Windows XP), and Portable Apps (single partition file system with start menu). These were chosen to show a little variety in the route taken to achieve the company's stated goals while still using a removable storage device.

In order to ensure that only the changes to the host operating system were analyzed, an image of a basic installation of Windows XP was put onto a 40 GB, zero-wiped hard drive for each experiment. An initial image of the hard drive disk (HDD) was taken using EnCase. Then, the HDD was put into a computer, booted up, and the USB device was plugged in. Basic flash drive programs (such as Mozilla Firefox Portable, Open Office, Skype, and Trillian) were accessed and files were created and saved to the flash drive before ejecting the USB drive and shutting down the computer. After the experiment, the HDD was re-imaged to look for changes to the system. Of the four programs tested, Flash-Puppy returned the best results for someone who didn't want their tracks traced, followed by MojoPac, U3, and Portable Apps.

As removable storage media continues to increase in popularity and become more widely available, people begin to fear that any personal data which is stored on these devices may be intercepted or left behind after their use. In response, companies and developers have created programs which claim to make it appear as if you were never there. However, when a flash drive is plugged into a USB 2.0 Port, its unique information is imprinted onto the registry in many places.

Digital Forensics, File System Circumvention, USB Flash Drive

 ** Presenting Author*