B4 A Case Study: Overcoming Anti-Forensic Methods Used on External Storage Drives

Michael Andrew, CyberSecurity Institute, 21816 132nd Street Southeast, Monroe, WA 98272; and Steven Hailey, CyberSecurity Institute, 17716 Trombley Road, Snohomish, WA 98290*

This presentation is based on a case study involving theft of proprietary data and efforts to conceal the offense. After attending this presentation, attendees will be able to identify and overcome certain efforts made to mislead and frustrate forensic analysis of file system activities on external storage drives.

This presentation will impact the digital forensic science community by providing analysts a methodology and practical technique that will assist in accurate analysis of data stored on external hard drives.

There are three primary learning objectives for this presentation: (1) facilitate analysis of external storage drives that have been used with a computer running a Microsoft Windows operating system that utilizes the NTFS file system, (2) identify and interpret certain data artifacts recorded on an external storage drive by the operating system, and (3) utilize these artifacts and overcome anti-forensic methods, assisting in the accurate analysis of file creation, deleting, copying, and moving processes.

This case study outlines a methodology that can be used to detect the manipulation of creation date and time stamps associated with files copied to an external storage drive. The case study also presents a process that can be used to track the movement of files to and from an external drive without reliance on recovery of latent data, (i.e., relevant file data and meta-data), or access to records located on the computer system that was used to copy the files onto the external drive.

The case concerns a large quantity of proprietary data that was downloaded to an external USB storage drive by employees, prior to departing a company. Analysis of records located in the USBSTOR sub-key on computers at the company revealed the date that the external drive was connected and used to copy the proprietary data.

In response to a court order, the defendants presented an external USB hard drive for analysis. The defendants refused to make available any computers that had been used to access the surrendered USB drive. They maintained they had never copied the proprietary data onto their personal computers and that their personal data was always kept separate from the downloaded data.

Analysis of the USB storage drive revealed the presence of proprietary files with creation date and time stamps that appeared to correlate with the connection records recovered from the USBSTOR sub-key on the company computers. However, further analysis revealed that the date and time had been manipulated at least three times during file creation processes, indicating multiple attempts to mislead and frustrate the analysis. The deception was discovered through analysis of artifacts on the USB drive that were generated as part of the System Restore function used by certain Microsoft Windows operating systems. Consequently, analysis was able to show that the presented drive was doctored in an attempt to make it appear as though it was the drive used to originally download proprietary data at the company.

Inspection of the artifacts also revealed that other relevant proprietary data had once been present on the drive, despite the claims of the defendants. The analysis was able to track the movement of these undisclosed files onto and off of the USB drive, demonstrating that the defendants had misrepresented their actions regarding the proprietary data and their compliance with the order of the court.

This case study is centered on a situation that presents significant challenges to an analyst; an external storage device is presented for analysis and the analyst does not have access to the computer that created the data on the storage device. The analyst cannot inspect records on the connected system to check if the file creation and file access date and time stamps for data on the storage device - derived from the system time set on the connected computer - have been manipulated. The methodology used in this case will be beneficial to the analyst in these types of situations, and can provide independent verification of activities surrounding the data on an external storage drive or device.

Anti-Forensics, Storage Drive, Time-Stamp

 ** Presenting Author*