B25 Indication of CD Burning by Detailed Examination of $MFT: A Case Review

Douglas Elrick, BA, Digital Intelligence, 17165 West Glendale Drive, New Berlin, WI 53066*

After attending this presentation, attendees will be able to examine a Windows based computer or evidence that files have been burned to an optical disc.

This presentation will impact the forensic science community by providing new sources of potential evidence in digital investigations.

One of most common case scenarios in civil computer forensics is one in which an employee leaves a company and is suspected of taking intellectual property to a competitor. Examiners are routinely asked to analyze the work computer and look for file activity prior to the employee's departure, what external storage devices have been attached, what files have been attached to emails, and if any files have been burned to a CD or DVD disc. The first three requests are fairly straightforward to complete but the detection of files that have been burned to disc has been difficult to determine. Thousands of files and gigabytes of proprietary information can be absconded with few methods for detection.

In a recent case, several hundred documents were found to have been last accessed just prior to the employee leaving. Not all the files in a particular subfolder were accessed which suggests a selective process and not an automated routine. Further examination revealed that the NTFS entry modified date and time was also updated within seconds of the last accessed time. Test burning of files through Windows XP SP2 revealed similar date and time results with the last accessed date and time and the entry modified date and time.

Through a detailed examination of the $MFT, clues are revealed indicating that files have been burned using the Windows operating system. Testing has shown that this detection can be accomplished for Windows XP through Windows 7 beta. A thorough understanding of the $MFT record structure including file attributes, record headers and record slack is needed for recognition of these indicators.

This presentation will demonstrate the artifacts left behind by which the Windows CD Burning process. While the evidence found is not conclusive that particular files and folders have been stored on optical disc, the artifacts found will provide strong indicators.

CD-Burning, MFT, File Attributes

** Presenting Author*