D31 CD-ROM Write Options Affect Calculation of One-Way Cryptographic Hashes

Philip Craiger, PhD, and Mark M. Pollitt, MS, Department of Engineering Technology, University of Central Florida, National Center for Forensic Science, PO Box 162367, Orlando, FL 32816- 2367; and Chris Marberry, BS, and Paul Burke, BS, National Center for Forensic Science, University of Central Florida, PO Box 162367, Orlando, FL 32826*

After attending this presentation, attendees will develop an understanding of the interplay between CDROM file systems and cryptographic hashing tools.

This presentation will impact the forensic community and/or humanity by assisting examiners to avoid incorrectly interpreting the results of hashing algorithms and will be able to develop protocols which will prevent obtaining incorrect results.

One-way cryptographic hashes (or 'hashes' for short) are mathematical algorithms applied to digital media. A common use of hashes in forensics is to demonstrate that digital media has not changed (i.e., not been tampered with subsequent to seizure). The application of a hashing algorithm to a piece of digital media (a file, a forensic image, etc.) should always result in the same unique number, typically of size 128 or 160 bits depending on the particular hashing algorithm used. Change of a single bit on the digital media will result in a significant change to the resulting hash, indicating that the contents of the media have changed.

While validating several comparable hashing software tools against a CD-ROM developed for a competency test several anomalies were found, including the inability of some tools to hash the CD-ROM at all (i.e., the tool 'errors out'), and other tools returning different hashes. Replicating the same tests with the same tools and CD-ROM on different hardware resulted in the same anomalous results. (This eliminated the hardware as the possible explanation of the problem). Therefore two explanations were postulated. The first was that the software tools were not written properly. This solution was eliminated because of the widespread use of these tools in digital forensics and computer security research and practice. It was surmised that the write options used for the CD-ROM affected the ability of the hashing tools to properly calculate the hash.

There are several options that can manipulated when writing CDs, including disk-at-once versus track-at-once, long versus short file names, multi-session versus single session, and to finalize the CD, to name a few. Note that these options do not change the actual files written to the CD, but only add 'overhead' to the CD. A fully crossed experiment was conducted combining several CD write options across five commonly used hashing tools. The results indicated that the anomalies disappeared when CDs were written using the disk-at-once option. The anomalies reappeared when using the track-at-once option.

The results of the experiments indicate that the options used when writing CDs affect the ability of different tools to properly hash a CD. This may be of great importance in a case, particularly when the expert witnesses use different tools to hash a CD and obtain different results. This kind of incident may cause doubt in the minds of the jurors that could have an adverse impact on the results of a case. This research proposal intends to extend this research to include DVD-ROMS, DVD- RW (read-write) as well as CD-RW (read-write).

Digital Media, Computer Forensics, Authentication

 ** Presenting Author*