D37 Potential Anomalous Results - Calculation of One-Way Cryptographic Hashes in Universal Serial Bus Devices

Mark Pollitt, MS, J. Philip Craiger, PhD, Chris Marberry, BS, and Paul Burke, BS, National Center for Forensic Science , University of Central Florida, PO Box 162367, Orlando, FL 3281*

After attending this presentation, attendees will develop an understanding of the interplay between USB storage devices and cryptographic hashing tools.

This presentation will impact the forensic science community by. As a result of attending this session, examiners may be able 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 developing simulated forensic evidence for teaching purposes, anomalous hash values were noted using certain combinations of imaging tools and Universal Storage Bus (USB) storage devices. The differences noted were limited to instances where the imaging tool was attempting to obtain an image of the "physical" drive.

One significant difference in the data structures for USB devices is that they normally lack a partition table. It is therefore possible that imaging software may make erroneous assumptions concerning the size of the media resulting in an image that is either the incorrect size or the included data bytes are different from what is read by another imaging tool.

Storage drives which utilize "autoplay" technology are becoming very common. Initial examination of these reveals that they may contain applications which change information on the USB drive, which could result in an altered hash value.

Given the increasing number, size and importance of USB devices, it is important to ensure that complete and accurate images are created from the original evidence.

Digital Forensics, Cryptographic Hash, Universal Storage Bus (USB)

 ** Presenting Author*