REPORT TYPE	OFFICE OF THE DISTRICT ATTORNEY	BOI CASE NUMBER
General Criminal	Bureau of Investigation NARRATIVE	B20080903230

DEFENDANT

Ciampi, Joseph

Summary:

ASF video files saved on a hard disk drive (item 101A) and compact disk (item A) were compared based on MD5 hash values generated during the course of my examination. The hash value was different for each file; however the differences could be accounted for by the difference in metadata for each video file.

Investigation:

Forensic images of the hard drive (item 101A) were created using Safeback and "FTK Imager". The Safeback forensic image was saved to data tape (LAB2). A forensic image of the compact disk (item A) was created using "FTK Imager". Subsequent examinations of the forensic images were conducted using Forensic Toolkit (FTK).

A MD5 hash is a 128-bit value, which can be generated based on the contents of a file. Hash values are commonly used to check the integrity of files. When files have different hash values, the contents of the files are different.

Metadata is information about a file, stored within the file itself. For example, digital camera image and video files can contain information such as the make/model of the camera used, the date and time the image was taken along with any other data chosen by the camera manufacturer. Metadata is typically not displayed when the image or video file is viewed.

The Microsoft Windows XP operating system allows the creation of separate accounts for each computer user. One such account on the hard drive was named "npowers". The "Taser Cam" software, version 2.2, was installed on the computer. The "Taser Cam" program is used to export video files from a "Taser Cam" recorder sold by "Taser International". The application exports video files using the "ASF" format.

Six ASF video files were currently saved in the user's folders for the "npowers" account on the hard disk drive (item 101A). Five ASF video files were in the "Recycle Bin" folder for the "npowers" account. Two ASF video files were saved on the compact disk (item A). Three video files saved on the hard disk drive (item 101A) have the same names as the compact disk video files.

The MD5 hash values of the three video files on the hard drive and the two video files on the compact disk were compared. The five video files each had a different MD5 hash value. During the course of my examination I noticed the camera and "weapon" serial numbers along with a MD5 hash value were stored as metadata within each video file. Each of the metadata MD5 hash values was different. This difference in metadata alone would cause the difference in the MD5 values that were generated as part of my examination. The MD5 hash values generated for each ASF video file and the metadata MD5 hash values were saved in a document named "MD5HashSummary.pdf". The MD5 hash summary was included in a FTK report.

OFFICER/ANALYST	ID NUMBER	DATE	REVIEWED BY	ID NUMBER	DATE	PAGE
Mario Soto	S2754	11/19/08	M. Lott TN/MM	S3028	11/19/08	1 of 2

DB1

REPORT TYPE	OFFICE OF THE DISTRICT ATTORNEY	BDI CASE NUMBER
General Criminal	Bureau of Investigation NARRATIVE	B20080903230

DEFENDANT

Ciampi, Joseph

A web based FTK report was created which includes the ASF video files and "Weapon Summary" PDF files copied from the submitted hard drive (item 101A) and compact disk (item A). The report includes MD5 hash values and file properties for each of the exported files. Also included is the Recycle Bin data that lists the original name for each of the files located in the Recycle Bin of the "npowers account". The FTK report was then written to two compact disks. One compact disk was packaged for release (LAB1), the second disk will be kept in the laboratory case file.

Evidence:

Item	Description
101A L02790	One tape-sealed evidence envelope containing a Western Digital hard disk drive, serial number WMAJ71535835.
A L02791	One tape-sealed evidence envelope containing one CD-R compact disk.
LAB1 L02801	One tape-sealed evidence envelope containing a compact disk with the FTK report which includes file properties, MD5 hash values and exported files from hard drive (101A) and compact disk (A).
LAB2 L02802	One tape-sealed evidence envelope containing the Safeback image of the hard drive (item 101A) saved on data tape. Encase and ISO images of hard drive (101A) and compact disk (A) saved on DVDs.

All of the above items were returned to the laboratory property room. Please pick up the evidence at your earliest convenience.

OFFICER'S NAME	ID NUMBER	DATE	REVIEWED BY	ID NUMBER	DATE	PAGE
Mario Soto	S2754	11/19/08	m/14m	S3028	11/19/08	2 of 2

Mario Soto

082