IGI PUBLISHING ITJ 4562

701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.igi-global.com

This paper appears in the publication, International Journal of Digital Crime and Forensics,Volume 1, Issue 1
edited by **Chang-Tsun Li © 2009, IGI Global**

Providing Cryptographic Security and Evidentiary Chain-of-Custody with the Advanced Forensic Format, Library, and Tools[1]

Simson L. Garfinkel, Naval Postgraduate School and Harvard University, USA

ABSTRACT

This article presents improvements in the Advanced Forensics Format Library version 3 that provide for digital signatures and other cryptographic protections for digital evidence, allowing an investigator to establish a reliable chain-of-custody for electronic evidence from the crime scene to the court room. No other system for handling and storing electronic evidence currently provides such capabilities. This article discusses implementation details, user level commands, and the AFFLIB programmer's API.

Keywords: AFF; AFFLIB; AImage, Advanced Disk Imager; disk imaging; EnCase

INTRODUCTION

Chain-of-custody for evidence from the crime scene to the court room is a bedrock principle of both civil and criminal law. Without a clear and unambiguous chain-of-custody there is no way to be sure that an object presented to the court is the same object that was collected at the scene of the crime. Even evidence presented to technical experts needs to have chain-of-custody: without it, there is no way to assure that the expert's testimony pertains to evidence from the actual case that is under consideration.

A paper notebook found at a crime scene can be put into an evidence bag, tagged, and locked away in an evidence locker. Each time the evidence is accessed or moved to another location this fact will be noted. In this manner the prosecution can show that the evidence has not been tampered; in the rare cases where tampering takes place, it can be detected.

But unlike records written with pen and paper, digital files can be modified without leaving a trace of the original message. This is one of the great challenges of digital forensics—establishing that a particular arrangement of bits on a digital storage medium is the result of on specific computational history (*e.g.,* deleting a file) and not of another (*e.g.,* using a hex editor to write raw sectors onto the disk drive that are indicative of a deleted file)[Carrier, 2006].

Of course, hard drives, USB memory sticks, and cell phones are tagged and bagged. But at some point, the information on these devices needs to be copied onto another computer system for analysis. In a modern forensic laboratory these files might be placed on a high-capacity server or a Storage Area Network (SAN) to allow for flexible use and simultaneous access by multiple examiners. Such environments require highly reliable technical measures to provide assurances that evidence is kept intact and unmodified.

Although computer forensics practitioners understand the importance of chain-of-custody, today's tools for preserving this chain are poor. Programs such as EnCase[Keightley, 2003] and dcfldd[Harbour, 2006] will compute an MD5 or SHA-1 cryptographic hash of a disk when it is copied by an investigator into an *image file*. Later, when the image file is provided to a forensic analyst, the analyst can compare the hash of the image received with the hash of the original to determine if the file has been modified. If the hashes match, the assumption is that the file is unchanged from the original.

This article introduces an improved method for assuring the integrity of digital evidence that is based on public key cryptography. In addition to providing improved integrity, the method presented also allows for:

- digital documentation of evidentiary transfer from one agent to another;
- reconstruction of evidence that has been inadvertently damaged during transfer;
- forensically sound methods for recovering partial evidence in cases where so much digital evidence has been damaged that reconstruction is no longer possible;
- encryption with both symmetric and public key cryptography, so that evidence that is acquired in a hostile environment can be safely transferred back to a secure facility.

These new methods have been implemented in the Advanced Forensic Format Library (AFFLIB) Version 3[Garfinkel, 2008]. AFFLIB is an open source software package written in the C/C++ programming language that allows for the imaging, manipulation, storage and use of digital evidence. The software is available free of charge for incorporation into both open source and proprietary forensic applications.

BACKGROUND AND PRIOR WORK

Disks and Disk Images

Computer hard drives, optical drives, and solid state drives are mass storage devices that organize the information they store as a series of numbered, fix-sized *sectors*. Traditionally hard drives employ a sector size of 512 bytes and CDROM drives used 2048-byte sectors, although a standard for 4096-byte sectors is currently under development[Fonseca, 2007].

A *disk image file*, or more generally an *image file*, is a file that contains a sector-for-sector copy of the contents of a mass storage device. Image files are intended to be perfect copies of the disk's contents. Image files are produced with programs called *imagers*.[2]

Although the discussion to this point has focused on disk image files, in practice any data carrying device can be imaged. Once a device is imaged, the forensic investigator works with the image, rather than the original device, in order to preserve the device's integrity: most computer forensic tools can directly read and process disk image files.

Image files are particularly important when it is necessary to record the state of a device that must then be returned to service—for example, in the event of a network attack. In these cases, the image file may be the only tangible evidence of the crime that has taken place after the system has been restored to operation.

Imaging also provides a simple and operating system independent means for backing up a hard drive: the drive is simply imaged into a file or onto another drive. To restore the backup, the image is *restored* on the original