IDEA GROUP PUBLISHING **ITB13048**

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

This paper appears in the publication, *Digital Crim and Forensic Science in Cyberspace*
edited by Panagiotis Kanellis, Evangelos Kiountouzis, Nicholas Kolokotronis, and Drakoulis Martakos

Chapter XV

Digital "Evidence" is Often Evidence of Nothing

Michael A. Caloyannides, Mitretek Systems Inc., USA

Abstract

Digital data increasingly presented in courts as evidence is mistakenly viewed by judges and juries as inherently unalterable. In fact, digital data can be very easily altered and it can be impossible for this falsification to be detected. A number of common ways are described whereby data in one's computer can enter without the computer owner's knowledge, let alone complicity. The same applies to all digital storage media, such as those used in digital cameras, digital "tape" recorders, digital divers' computers, GPS "navigators", and all other digital devices in common use today. It is important for judges and juries to be highly skeptical of any claims by prosecution that digital "evidence" proves anything at all.

Introduction

Unlike conventional analog data, such as the shade of grey or the subjective recollection of a witness, whose believability and validity is scrutinized in depth, digital data which takes one of two very unambiguous values (zero or one) is misperceived by the average person as being endowed with intrinsic and unassailable truth.

In fact, quite the opposite is true. Unlike conventional, analog, data and evidence whose tampering can often be detected by experts with the right equipment, digital data can be manipulated at will and, depending on the sophistication of the manipulator, the alteration can be undetectable regardless of digital forensics experts' competence and equipment.

The reason is quite simple: The ones and zeros of digital data can be changed and, if some minimal precautions are taken by the changer, the alteration leaves no traces of either the change or the identity of the person who made the change.

Stated differently, computer forensics can determine what is on the suspect's digital storage media at the time of the forensics investigation, but is never able to determine who put it there, when, how, or whether or not the data has been changed. The only possible exception is if the suspect elects to confess, but even that is proof of nothing given the long historical record of coerced false confessions worldwide.

The potential for miscarriage of justice is vast, given that many defense lawyers, judges and juries are unaware of the esoteric details of computer science. Worse yet, malicious prosecutors may take advantage of this ignorance by courts and defense lawyers by falsely asserting that digital evidence is "proof" of the guilt of the accused.

This "dirty little secret" about digital "evidence" is conveniently soft-pedaled by the computer forensics industry and by the prosecution, both of which focus on those *other* aspects of the process of collecting, preserving and presenting digital data evidence which can indeed be unassailable *if* done properly, such as the "chain of custody" portion of handling digital evidence.

Let's take a common example of "computer evidence". A suspect's hard disk is confiscated, subjected to forensics analysis and a report is generated for the court which states that the hard disk contained this or that file, and that these files dates' were this and that, that these files were renamed or printed on this and that date, thereby appearing to negate the suspect's claim that he or she did not know of the existence of these files.

A typical judge or jury will accept these facts at face value. In fact, it should not; for the following factual reasons:

1. The data found in someone's hard disk could have entered that hard disk (or any other digital data storage media, such as USB keys, CD ROMs, floppy disks, etc.) through any one or more of the following ways without the suspect's knowledge, let alone complicity. All of these paths for surreptitious data entry are very commonplace and occur on a daily basis. Situations where this happens routinely include the following:
    a. The hard disk was not new when the suspect purchased it, and contained files from before the suspect ever took custody of it. This applies even in the case of purchases of "new" computers because they could have been resold after being returned by a previous buyer. Even if that hard disk had been "wiped" by the seller and the software reinstalled, there is no physical way to guarantee that some data were not left behind; this is why the militaries and security services of most countries will never allow a disk to leave a secure installation, but will physically destruct it instead.