



How Digital Forensics Gets Behind the "Facts"

There's More to Evidence than Meets the Eye



www.kbgrp.com

By:
Richard E. Goble,
CPA/CFF/EnCE®
(Shareholder)

Kerkering, Barberio & Co.
Certified Public Accountants
1990 Main Street, Suite 801
Sarasota, FL 34236
and
6320 Venture Drive, Suite 203
Lakewood Ranch, FL 34202

Phone:
(941) 365-4617
Email:
rgoble@kbgrp.com
www.kbgrp.com

Dated:
October 18, 2011

About the Author:
Mr. Goble's practice areas include Forensic Accounting and Litigation Support, Individual and Business Tax Consulting, and Real Estate Support. He joined Kerkering Barberio in 1978 and was admitted as a Shareholder in 1979.

Certified Public Accountant
Certified in Financial
Forensics
EnCase® Certified Examiner

If you're a fan of shows like *Law & Order* or *CSI*, you have heard about digital forensics. Whenever someone analyzes a cell phone, a digital camera or a computer, they are using digital forensic tools.

In cases ranging from fraudulent business transactions to marital disputes and alleged money laundering, it's the job of the digital forensics analyst to obtain and evaluate electronic data.

Although there are a number of specialists in the field, only a handful of them are also CPAs and even fewer hold the CFF (Certified in Financial Forensics) designation. I find that this combination provides me with a unique skill set when it comes to providing services as a forensic accountant.

Behind the Bits and Bytes

We typically follow a three-step process to uncover information. The first step is to create a forensically sound image of an electronic storage device. This is most often a computer hard drive. But it could also be a thumb drive, CD, iPod, camera, Smartphone – even a watch or pen that contains digital storage media.

That image is a bit-by-bit copy of the entire device. To the untrained eye, it appears to be nothing but gibberish. But by applying sophisticated tools to that "gibberish," we are able to interpret the content.

Now, Analyze

The next step is to perform a detailed analysis of that image. What we search for is determined by the type of evidence or content the client or law enforcement agency is requesting. For example, we can look for files that have been deleted or whose extension has been changed to hide the true nature of the file. We can also search for files containing key words relevant to the matter at hand. Keep in mind that when you delete a file on your computer, all you are really doing is telling the operating system that the space occupied by that file is now available for use, and until the operating system actually uses that space, the "deleted" file is still there. Another category of evidence is what's known as operating system artifacts. These are not files, but a kind of digital footprint that can reveal, for example, where on the internet an individual has been.

These findings represent the third step – acquiring and presenting relevant evidence. In most civil cases, results are reported to the client and their attorney. In other instances, digital forensic analysts are hired by and report directly to law enforcement or government agencies.

Why It Matters

There is more to the data than meets the eye. That's why it's so important to be able to reach into the digital background to obtain hidden, deleted or incorrect information. In one famous case, Dennis Rader, also known as the BTK killer, sent a floppy disk to Fox TV station KSAS in Wichita, Kansas. Forensic analysis of something known as metadata quickly determined that the disk had been used by the Christ Lutheran Church in Wichita, as well as a reference to the name "Dennis." An internet search determined that a "Dennis Rader" was president of the church council. He was arrested based on this information.

Many business owners mistakenly assume that digital forensics applies only to criminal courtroom proceedings. In fact, there are many non-criminal applications. For example, some companies routinely request a digital image of a computer hard drive for any employee who leaves under less than favorable circumstances. Others seek our help to substantively wipe out and reformat computers when they are assigned to new hires.

While your business may never be involved in high-profile criminal cases like those that draw audiences to shows like *CSI*, keep in mind the potential for digital forensic analysis to help get to the facts, wherever they may be hiding.

###

I would be happy to assist you with any of your questions. Please call 941-365-4617 or email me at rgoble@kbgrp.com.

