

Smoke and Mirrors: The Fabrication and Alteration of Electronic Evidence

By Sharon D. Nelson & John W. Simek

“Sufficiently advanced technology is indistinguishable from magic.”

— Arthur C. Clarke

Welcome to the Digital Tech Fun House of the next millennium. Does some putz at NBC want Katie Couric to look 20 pounds slimmer? A wave of his electronic wand, and it is so. Does a Reuters photographer in Beirut want his photos of violent explosions to have a greater “shock and awe” factor? No sweat – he just uses a graphics program to darken the explosions. Mad at your former lover and want to put her head on a porn queen’s body and post it on your website? A quick cut and paste . . . presto change-o . . . it is done.

Nothing in the world is really new, so they say. In truth, the alteration of photos is an old story – remember all the UFO photos of the ‘50s that turned out to be an aluminum wrapped, gussied-up version of Mom’s dinner plate? If you don’t, shame on you for being so young!

The digital alterations of things can be charming – witness the use of digital alteration in Forrest Gump to make him a part of history. Absolutely inspired. Then look again – at *Time* magazine’s bizarre editorial decision to artificially darken O.J. Simpson’s face on its cover. Dispiriting how far we, as a society,

have *not* come.

Someone, presumably not a [John] Kerry fan, stitched together two separate photos to make a composite allegedly showing his speaking with Jane Fonda at an anti-war rally. When you see the original photos, you can see what happened. But barring that, your eyes would likely believe what they see – and therein lies the great danger of accepting things electronic as real..

How do the pros spot digital alteration? Often, by blowing things up. When viewed at the pixel level, doctored photos don’t “fit.” Rarely does anyone doctor photos with so much precision that the doctoring can’t be seen when enlarged. What is not apparent to the naked eye becomes readily apparent when looking at a photo under the equivalent of a microscope. Today, there are even mathematical algorithms to help determine whether a photo has been altered.

There are harmless and even fun uses for digital alteration – a charming but fake photo of President Clinton in a pink tutu, which made the Internet rounds some years ago, comes immediately to mind. But there are grave uses, many with criminal complications. The most common one, by a country mile, is e-mail spoofing.

E-MAIL SPOOFING: WHO DO YOU WANT TO BE TODAY?

Stealing someone’s identity by using

their e-mail address is done all the time – the average 13-year-old knows how to create and transmit falsified e-mail. Look at all the spam that we receive every day, where the messages appear to come from people we know or from what appear to be otherwise legitimate sources. Viruses and worms are also known to gather e-mail addresses from an infected machine and send messages appearing to come from one of the newly harvested addresses. Unfortunately, there is nothing you can do to stop someone else from sending an e-mail appearing to come from you. Even if you do succeed in tracking them down, they are often in foreign countries where the incentive to cooperate with U.S. authorities is non-existent. Imagine our embarrassment several years ago when pornographic spammers were sending rather risqué e-mail messages, complete with images, with made up addresses from our domain name. You can’t imagine our relief when they moved on to some other hapless victim.

Although you can’t directly stop falsified transmissions, how do you determine if the e-mail is authentic or spoofed? If you are involved in a case where e-mail is at issue, do not accept the presentation of the message on paper. Anybody can use a typical word processor package to create a document that looks like a printed e-mail. Get the message in electronic form so that you

can interrogate the headers. Don't know what an e-mail header is? The message header is electronically stored information that shows values such as sender, recipient, message ID number, routing information (the servers and devices that transmitted the message along its path), priority level and other similar information. Viewing the header

information varies depending on the e-mail client that is used. As an example, to view the header data in an open message using Microsoft Outlook, select 'view' and then 'options,' which will then show the information in the dialog box.

How do you read a header or even understand it? Probably one of the most

popular software tools for decoding headers is a product called Sam Spade. The official web site for Sam Spade has been having technical difficulties for several months, but a Google search should show alternate locations to download the software. You read e-mail message headers from the bottom up. Figure 1 shows a sample of a recently received message.

Figure 1

Received: from mail126c25.carrierzone.com
([64.29.147.196]) by ffx3975.senseient.com with Microsoft SMTPSVC(6.0.3790.1830);
Mon, 18 Dec 2006 15:02:23 -0500

MIME-Version: 1.0

Content-Type: multipart/alternative; bound-
Ary+”_=_NextPart_001_01C722DF.6E7BB180”

**Received: from intern (static-68-236-214-31.nwrk.east.verizon.net [68.236.214.31])
(authenticated bits=9) by mail126c25.carrier-Zone.com (8.13.6.20060614/8.13.1)
with ESMTTP id kBIJo28u026412; Mon, 18 Dec2006 19:50:04 GMT**

Return-Path: <markszep@sandpiperpartners.com>

X-Mailer: Microsoft Office Outlook, Build 11.0.5510

X-OriginalArrivalTime: 18 Dec 2006
20:02:23.0636 (UTC)

FILETIME=[6EDCBD40:04C722DF]

X-MimeOLE: Produced by Microsoft Exchange V6.5

X-Authenticated User: markszep.sandpiperpartners.com

Content-class: urn:content-classes:message

Subject: Your Nomination for the E-Discovery
Special Master and Expert Witness Directory

Date: Mon, 18 Dec 2006 14:50:03 -0500

Message-ID: <200612181950.kBIJo28u026412@mail126c25.carrierzone.com>

X-MS-Has-Attach:

X-MS-TNEF-Correlator:

Thread-Topic: Your Nomination for the E-Discovery Special Master and Expert Witness Directory

thread-index: Acci36Wn9hp+8QoPTROaF3G
ji23D9Q==

From: "Mark Szep" <markszep@sandpiperpartners.com>

To: "Mark Szep" <markszep@sandpiperparnters.com>

As you read from the bottom up, go until you reach the first “Received:” information (marked in bold in Figure 1). In our example (headers from a real message) the originating e-mail server is named “intern” and has an IP address of 68.236.214.31. This is the first point to determine if the message is spoofed. Spammers will normally “bounce” their messages off of an unsecured server. In those cases, the transmitting server has no relationship to the originating domain. As you can see, decoding headers can get very complicated, but it is absolutely essential in determining the authenticity of the message. Is this a do-it-yourself proposition? Probably not, unless you are pretty tech-savvy.

In the typical case we see, angry ex-spouses or significant others spoof the e-mail of their former loved one to prove that they wrote hateful or threatening messages to them, usually for the purpose of gaining an advantage in a custody battle, but sometimes just to humiliate them, or to try to cause them to lose their jobs. We’ve even seen an angry supervisor pretend to be his own employee writing threatening e-mails to the supervisor for the purpose of laying the groundwork for firing him. It’s a wacky world out there.

FABRICATION THAT PAYS HANDSOMELY: PFISHING

We’ve all gotten them – those fraudulent e-mails that purport to be from our bank or credit card company asking us to kindly verify our financial information. The number of new phishing sites has spiked dramatically from 4,367 in October of 2005 to 37,444 in October of 2006, according to the Anti-Phishing Working Group. Gone are the days when the e-mail was clearly written by someone for whom English was a distant second language (“Please

to come to our site to complete you’re Citibank data securities form”). Gone are the clumsy attempts to replicate graphics. Now the phishing e-mails are so clever that even the experts sometimes have trouble discerning the fakes. For those poor saps who are taken in, they click on “their bank’s” link, only to find themselves in a clever imitation of their bank’s website where they obligingly fill out the requested financial data form and thereby ensure that their real bank account will soon be substantially lightened. The best of these bogus sites are a real tribute to the ingenuity of the criminal mind – and a continual thorn in the side of law enforcement as these sites are shifted from server to server in a matter of days, making these operations nearly impossible to track down and shut down.

METADATA: PAY VERY CLOSE ATTENTION TO THE MAN BEHIND THE CURTAIN

More and more attorneys are becoming familiar with metadata, especially as it relates to documents and spreadsheets. Generally, metadata refers to “data about data,” which isn’t a very helpful definition. When referring to a Word document, metadata would be such information as the author, last date printed, file creation, number of words, tracked changes, etc.

So how do you tell if an electronically produced document is authentic? Viewing the metadata can determine if there may be suspicions that the document is falsified. Perhaps you receive the Word document from your client, which is a contract supposedly drafted by the president. However, when you look at the metadata it shows the author as being a competitor and further reveals that the document was

created several years earlier. Your radar should light up like a Christmas tree.

How do you see the metadata? The simplest way is to go to ‘File’ and then ‘Properties.’ Using this method doesn’t show all of the available metadata, but is enough for many purposes. Another alternative is to use a product that removes metadata (a good thing for you) but also shows you metadata in documents received from someone else (often a bad thing for the other side). Several well known software applications for viewing and “scrubbing” metadata are Metadata Assistant, Workshare Protect and iScrub. We’ve had many a case where metadata was important, but here’s one that lawyers should heed. An attorney up on disciplinary charges for mishandling a case suddenly produced a letter to his client that, on her instructions, he would do nothing further in the case. The problem? The metadata proved conclusively that the letter had been created after the disciplinary proceedings had been filed. This brings to mind the old adage about going from the pot directly into the fire. To no one’s surprise, his license was suspended.

WINDOWS METADATA: TOYING WITH THE FOURTH DIMENSION

There is also metadata for the operating system. We’ll address Microsoft Windows metadata since it is the most widely used operating system. Windows metadata is the information that a user can observe by selecting “file” and then the “properties” function. The most commonly known metadata values are known as MAC (modified, accessed, created) dates. These times/dates can be used to identify when files were created, or

perhaps accessed. Internet searching activity on a computer may have great significance when dealing with child custody cases and determining the fitness of a parent, particularly where there are allegations of Net pornography addiction or searching for child pornography.

Authentication of the MAC values assumes that the clock or the computer was accurate at the time the files were created or accessed. This can be problematic since the computer clock is so easy to change. Before you get paranoid about the file dates on your client's computer, clock manipulation is not normally seen in the "real world" and those that attempt it are usually caught. There are several ways to determine if an intentional clock change has occurred. The simplest way is to look at the system logs using the Event Viewer application in Windows. The Event Viewer can be accessed from the 'Administrative Tools' group. When the Event Viewer is opened, observe the entries in the System and Application logs. Entries in these logs are written in a sequential fashion, therefore the date and time entries should be consistently decreasing as you read down the entries. There will be an obvious gap or jump in the dates if the computer clock has been intentionally modified. There are other methods to determine clock manipulation, but those are best left to forensic technologists. The good news is that the Windows MAC values are typically what they purport to be.

Though we've rarely seen clock manipulation, there was a case in which a computer-savvy wife planted child pornography on her husband's computer, changing the clock so the created dates would indicate only times when he was home and she was not. She obviously had not read the paragraph above.

LAW ENFORCEMENT'S CONTINUAL BLACK EYE: STOMPING ON THE EVIDENCE

Sometimes the alteration of evidence can be the answer to an attorney's prayer. In spite of a concerted effort by law enforcement to teach first responders how to properly seize electronic evidence, we still see instances where the last access dates of files have been altered by officers looking at the evidence post-seizure. It appears to be particularly alluring to "take a peek" at anything involving sex, but trampling on the evidence in their eagerness to see what they have provides (for the ardent defense counsel) a happy result in which proper forensic procedures were not followed and the dates of last access by the defendant are now unknown.

Are there hundreds of other examples of digital alteration? Sure . . . and stay tuned, because they are appearing more and more often in the courts. The good news is that we have gotten better and better at detecting the alteration of electronic evidence. More good news is that most people who try to fabricate or alter evidence aren't the brightest

bulbs in the chandelier and are easy to catch. The bad news is that there is a cadre of unprincipled criminals who are doggone good at evidence alteration – and they are often one step (and sometimes light years) ahead of the good guys.

Reprinted with permission of The Nebraska Lawyer © 2007.



Sharon D. Nelson, Esq., is the president of Sensei Enterprises, Inc. and president of the Fairfax (VA) Bar Association. Nelson graduated from Georgetown University Law Center in 1978 and has been in private practice ever since. Her primary practice areas include technology and internet law. She can be reached at (703) 359-0700 or at sensei@senseient.com.



John W. Simek is the vice president of Sensei Enterprises, Inc. He holds a degree in engineering from the U.S. Merchant Marine Academy and an MBA in finance from Saint Joseph's University. He is an EnCase certified forensic technologist who provides credible and comprehensive court testimony as an expert witness.