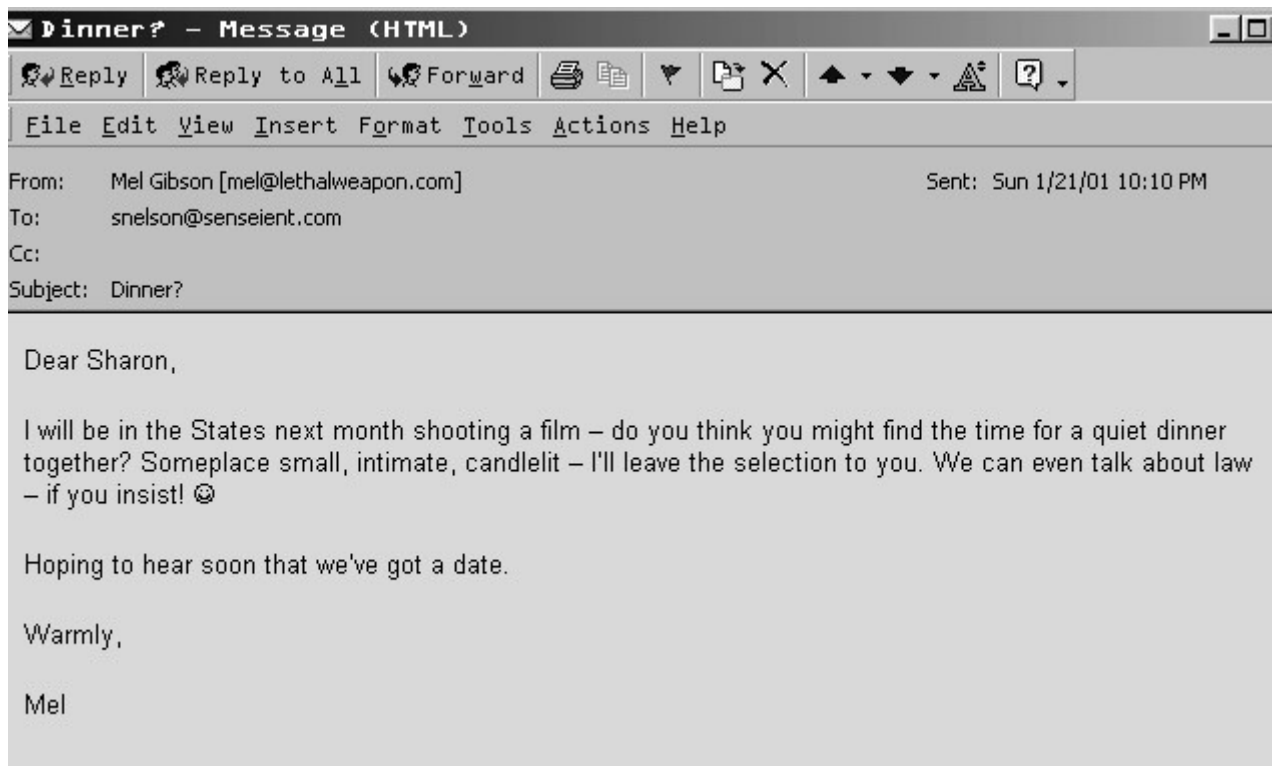
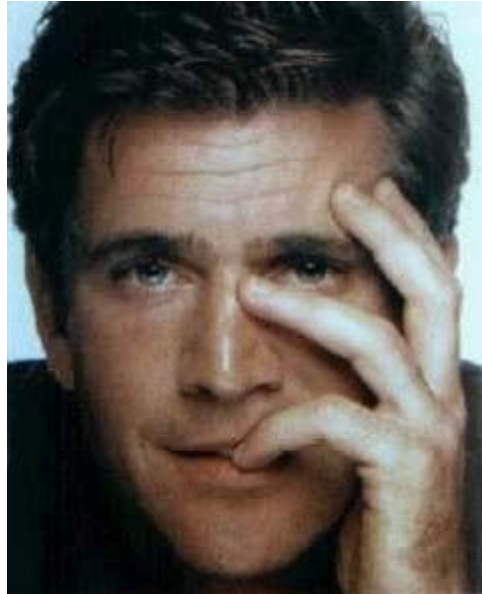


## Mel Gibson Proves That You Should Be Wary of Electronic Evidence!

By Sharon D. Nelson, Esq. and John W. Simek  
© 2002 Sensei Enterprises, Inc.



No, doggone it, he didn't write it. But it sure looks real enough, doesn't it?

It took the authors just a couple of minutes to "spoofer" Mr. Gibson's e-mail address. Since we were by then having our own nerdy idea of a great time, we then spoofed George Bush's address and wrote bogus e-mails to one another. The President wrote Sharon inviting her to be his Attorney General and wrote John inviting him to be the National Technology Czar (a position the President confidentially advised us that he intended to

create). Yes, we really do spend nights doing goofy stuff like this, but along with the goofiness, we were proving a point with our assumption of other identities.

This is not rocket science. It is fast and easy to spoof other people's e-mail and to produce a credible result that a court might well accept as real, whether it is or not.

Larry Ellison, the President of Oracle, had his e-mail spoofed by a disgruntled employee. The bogus e-mail suggested all sorts of heinous acts on his behalf. He was not amused, prosecuted her, and the highest position to which she can now aspire is President of the Computer Prison Club.

Spoofing is very common, as most of you know from the spam that clutters your mailbox. The address of the sender is never real. Ever try to reply? The zap you hear from your speakers is the message boomeranging back at you.

The use of spoofing to fake evidence is a relatively new phenomenon. Where are you likely to encounter it? In business, to discredit someone. In the propagation of stock related news, to artificially lower or raise the price of stock. In divorce cases, to construct an adultery or other illegal conduct where none exists. These are a few of many possibilities. A creative mind can have a field day – add criminal intent and the rest of us would do well to be very wary indeed of an e-mail's authenticity.

Should printed or forwarded e-mail EVER be accepted on its face? No, never, never, never. Without the message "headers" (under-the-covers Internet tracking information) which accompany the e-mail, you have very little information. With the headers, you can at least track the servers along the way, but keep in mind that several of them may be phony too. Can you spoof IP addresses too? Yes, to a point. More complicated, but yes. Unbelievable as it may sound, there are now federal agents who specialize exclusively in the science of tracing e-mail to its origin. It is their technical skills, not old fashioned legwork, that has led to the arrest of some of the notorious virus writers of our time.

The authentication of e-mail has become a major issue in court these days. When we are expert witnesses, our testimony (while completely accurate in either case) can have two slants. We can present all the reasons that support the validity of e-mail or all the reasons why it might be invalid. We are of course silent as to the contravening factors of either stance, unless asked directly. Few attorneys seem to understand this technology well enough to ask questions that might undercut expert testimony. More and more, the authentication of e-mail will become a battle between experts, with the side having the better expert having a distinct advantage. If the other side has a credible expert, heaven help you if you don't – the average attorney doesn't have a prayer of undercutting the technical arguments made by an expert in electronic evidence.

What are judges to make of the credibility of electronic evidence? The clear tendency has been for them to accept the evidence at face value, absent a suggestion that the evidence has been manufactured or altered. In one notable Virginia case, a judge determined custody in part based on a finding that the father was regularly surfing on child

pornography sites. Perhaps, but the father was steadfast in his protest that he had never been to such sites and his attorney told us with great conviction that she believed the father had been framed by his wife, a computer expert. It was spilt milk at this point, but the truth is that it isn't hard to create a surfing history, and even to partially cover your tracks.

Let's take the case above. If you want to establish a history of visiting child pornography sites, and you have access to the computer of the person you want to frame, you can simply visit the sites yourself and the machine will dutifully take note of each site visited and include it in the history. The machine's process is robotic – it does not know WHO initiated the visits, only that the visits themselves took place.

This is of course a weakness. If there are multiple people who have access to the computer, it isn't possible to prove who was doing the surfing. Under ordinary circumstances, where perhaps only two people had access to the computer (husband and wife), a judge is unlikely to believe that the wife was visiting child porn sites. In a divorce or custody case, however, where a wife might be motivated to manufacture evidence, the adjudicating party should be considerably more wary.

One factor we look at is the time of the visits. What if it can be proven that the husband was out of town or at work when some of the visits took place? If we represent the husband, we strike pay dirt if this is true. But how clever is the wife? Is she clever enough to realize she can reset the machine's clock? If so, while her husband is in California on business, she can set the clock to late at night last weekend when he was home, and then visit the porn sites. The machine will, once again, dutifully record the visits and note the time according to its own clock. Can we now trap the wife and reveal the evidence to be fraudulent? If the connection to the Net was made by a dial-up connection, yes, by subpoenaing the records of the ISP which may prove that no one was connected during some or all of the time in which the child porn sites were supposedly accessed.

There are other ways to determine the manipulation of the clock setting, but we will retain those trump cards – and it is unwise to divulge all the subtleties of electronic evidence lest someone be tempted to abuse the knowledge. Fortunately, most people who manufacture electronic evidence suppose themselves to be smarter than they are – and they are therefore often tripped up by technical professionals.

How about photographs? What convincing evidence they can be! How many trials have been won or lost on the basis of photographs? Here's a scenario . . .

A prominent businessman has disappeared. Foul play by a colleague is suspected. Circumstantial evidence leads to the colleague's arrest. No body is found. A photograph comes into the hands of her defense attorney.

The photograph depicts a body, twisted on the floor, a gaping wound in the chest. Across the room, on the floor, is a pistol. On the white wall above the victim's body, scrawled in the victim's own blood, are the words, "I'll kill again. You'll never catch me." Certainly a

homicide, and perhaps damning to the defendant in the context of the circumstantial evidence. Suppose that a digital camera created the photograph and the defense attorney is unscrupulous. The entire picture is made up of binary digits, ones and zeros, which can be altered without detection using off the shelf software. So the defense attorney rearranges the digits. He "cleans" the wall, removing the bloody words. He closes the chest wound, and artistically arranges to have blood trickling from the victim's temple. He moves the gun into the victim's hand. The case is now clear: the photograph "proves" that the victim committed suicide. The murderer is acquitted.

Implausible? Not at all. This particular falsification of evidence was actually done as far back as 1991, in a demonstration at a meeting of the Federal Computer Investigations Committee. The Committee had been established by a handful of federal and state law enforcement personnel who were among the first to appreciate how emerging technologies were both providing new opportunities for criminals and creating new challenges for law enforcement officials and the courts.

Nor will these authenticity problems be limited to photographs. When was the last time you went to "Best Buy" and signed for your credit card charges? You signed on a machine, didn't you? What happened then? The magic of our age sent the digital information to a computer that validated your signature. BUT IT ALSO would allow the recreation of your signature. Who knows where or when, or with what consequences? You have, in fact, just entrusted your signature to Best Buy.

Scary? Sure, it's downright unnerving. What's above is just the tip of an iceberg the size of which is sure to ensure legal disasters of Titanic proportions. Even the experts are often befuddled by technical possibilities. The authors study this field daily, and yet the ground keeps shifting under our feet. What was impossible yesterday is possible today and child's play tomorrow. In fact, our 15 year old intern has altered crime photographs for our presentations – "just for fun" as he puts it. Take a look at all the hacking attacks by teenagers, some of them geniuses, but some just "script kiddies" who take the technical knowledge of others and use it for mischief. What judge or lawyer, bedeviled by technology, has not looked to their 12 year old to rectify their computing problems?

The generation that did not grow up at the keyboard is handicapped when it comes to discerning the potential for altering or wholesale manufacturing of electronic evidence. Yet this is precisely what we must do if the law is to keep pace with technology. The moral for judges and attorneys is simple. Beware electronic evidence – it may not be what it seems.

*The authors are the President and Vice President of Sensei Enterprises, Inc., a computer forensics and legal technology firm based in Fairfax, VA. 703-359-0700 (phone) 703-359-8434 (fax) [sensei@senseient.com](mailto:sensei@senseient.com) (e-mail), <http://www.senseient.com> (web site)*