

CyberBytes



Subject: Proving the Authenticity of an E-Mail or Document

At CyberControls' data forensics laboratory, a noticeable increase in case engagements involving the pursuit of establishing the authenticity of an e-mail message or document has become a pivotal issue in more and more civil cases.

While there are many different factors to be examined that are somewhat unique to e-mail examinations versus document examinations, there are some common approaches that computer forensics examiners will enlist when working with attorneys to establish authenticity or challenge it.

First, when documents and e-mails are created on a computer, the software being utilized to create it, also generates a fair amount of specific identity- oriented information (metadata) that is unique to each individual e-mail or document.

Second, because the metadata is like a fingerprint, it is crucial to preserve this information (potential evidence) by safeguarding the subject computer whenever possible. For the requesting party attorney, it is important to notify the producing party that they are under an obligation to preserve this evidence. For the producing party's attorney, it might be advisable to have a computer forensic expert perform a bitstream copy of the computer hard drive to avoid inadvertent spoliation.

Third, do not accept anything less than a computer forensic examination of the subject computer's hard drive to

gather all of the pertinent metadata information to determine the originality and authenticity of a document. In addition, the forensic examination will also be able to identify and recover any deleted copies or versions of the same document to help determine whether or not content or possibly the dates were altered.

As for determining an e-mail's originality or whether in fact a certain e-mail was ever created by the alleged sender or whether the content of an e-mail was altered by the sender or recipient, a computer forensic examination is essential. Critical information having to do with the computer ID, date and time of the message being sent, the content size of the e-mail, the e-mail address of the sender, the IP address of the sender's machine, and the original message ID of the sender's machine are all things that can only be retrieved from the computer are what is required to establish or refute an e-mail's admissibility as evidence in court.

Don't wait any longer in exploring the possibilities as to how computer forensic discovery can support your most difficult cases. Call and ask to speak with one of our forensic consultants for an assessment as to how computer forensics may be a fit for a particular legal matter at **847-756-4890**, or see us on the web at www.cybercontrols.net