E37 Digital Forensics — What Lawyers Need to Know

Jessica J. Reust Smith, MFS, Stroz Friedberg, LLC, 1150 Connecticut Avenue, Northwest, Suite 200, Washington, DC 20036*

The goal of this presentation is to describe the fundamentals of digital forensics and the types of questions examination of digital evidence can answer, with an emphasis on what lawyers need to know to make strategic decisions about the digital evidence in their cases and to navigate this relatively new discipline of forensic science.

This presentation will impact the forensic science community by providing the attendees with the fundamentals for making that assessment, both in support of their client's claims and in anticipation of opposing counsel's counterclaims. In addition, this presentation will discuss when it makes sense to call in a digital forensic expert, what to look for when choosing an expert, and the questions to ask to ensure an expert has performed his or her due diligence before reaching a conclusion.

Desktop, laptop, netbook, flash drive, Playstation, cell phone, PDA, iPod, and digital camera. Although this sounds like a birthday wish list it is just as likely to be the list of evidence collected in one's latest criminal or civil case. The ubiquitous nature of digital media and the breadth of information that can be gleaned from them, if properly examined, have led to a dramatic increase in the number of digital media items collected in investigations. This presentation will describe the fundamentals of digital forensics and the types of questions examination of digital evidence can answer, with an emphasis on what lawyers need to know to make strategic decisions about the digital evidence in their cases and to navigate this relatively new discipline of forensic science.

The analysis of digital evidence can provide a wealth of information about both the content of the data and contextual information regarding how the digital media was used and the activities and knowledge of the user. Having a basic understanding of how data is stored on the media and the types of information that can be extracted through a digital examination will assist in one's ability to understand the questions that can be answered and to also assess the evidentiary value of the digital evidence.

Was the iPod carried by a suspect in a rape case previously used by the victim? Who is sending the anonymous harassing e-mails to the CEO? Is the key document in a contract dispute case authentic? Did the CFO view and therefore have knowledge of the spreadsheet e-mail attachment containing the company's fraudulent financial information? Was confidential data stolen from a company by the hackers who gained unauthorized access to their network? These are all questions that may be answered through digital forensic examinations.

As the number of type of digital devices turning up in criminal and civil cases continues to grow, so too does the importance of a lawyer's ability to assess the evidentiary value of the digital evidence and make informed strategic decisions. This presentation will provide the attendees with the fundamentals for making that assessment, both in support of their client's claims and in anticipation of opposing counsel's counterclaims. In addition, this presentation will discuss when it makes sense to call in a digital forensic expert, what to look for when choosing an expert, and the questions to ask to ensure your expert has performed their due diligence before reaching a conclusion.

Digital Forensics, Computer Forensics, Digital Media

* *Presenting Author*