



F56 Digital Evidence 101 — The Evidentiary Value of Digital Evidence: The Impact of Digital Evidence on the Investigation and Brief of Evidence

Paul Reedy, BS, DC Department of Forensic Sciences, 401 E Street, SW, Washington, DC 20024*

The goal of this presentation is to assist the forensic science community in understanding recent developments in information and communications technology, its use by perpetrators and victims in the context of criminal activity, and its evidentiary value in investigations and criminal proceedings.

This presentation will impact the forensic science community by providing attendees with a practical understanding of the role of information technology in various criminal activities plus anticipation of possible future directions.

Information (and communications) technology is ubiquitous to modern human existence. It follows that this technology is involved in nearly every facet of human activity, including criminal activity, whether it is simply the act of a person carrying a phone, a computer used to transact business, or a device that informs about an individual's state of mind and interests. Consequently, any investigation of criminal activity will potentially have lines of inquiry that include digital evidence. Digital evidence can be used for the investigation of homicide, extortion, assault, sexual assault, online child exploitation, stalking and intimidation, fraud, arson, sudden infant death syndrome, and others; it can include exculpatory as well as inculpatory evidence.

It is no secret that information technology evolves at a rapid rate with the occasional revolution thrown in for good measure. Criminals are notorious for being early adopters of technology, comfortable in the knowledge that law enforcement agencies will struggle to attain the capability and capacity to keep up.

The challenge for digital evidence experts is understanding and deciphering new technologies, including "the latest app," as critical evidence is invariably present in these new formats. The digital evidence analyst must be sufficiently qualified and experienced to reflect an understanding of the evidence under examination.

The challenge for the prosecutor is to understand the probative value of the evidence and to ensure that it is presented in a manner that is easily understood by the court.

The challenge for the defense counsel is to understand the nature of the evidence under examination, identify any insufficiencies in the forensic examination that lead the conclusions, and to identify alternative credible hypotheses based on the available evidence.

This presentation will provide descriptions of places digital evidence may be located; several case examples where digital evidence is critical to, or augments, the investigation and/or brief of evidence; the applicability of international standards to digital evidence; anticipated developments in information technology; and, some introductory remarks concerning the current legal environment.

Digital, Evidentiary, Case