E5 Computer Forensics and Digital Evidence for Attorneys and Investigators

Michael Buratowski, MS, General Dynamics - AIS, 7001 Club House Circle, New Market, MD 21774; Brian Bataille, JD, Department of Defense, Pentagon, Arlington, VA; and Michael J. Salyards, PhD*, United States Army Criminal Investigation Laboratory, 4930 North 31st Street, Forest Park, GA 30297*

The goal of this presentation is to present attorneys and investigators a solid overview into what can and cannot be determined with computer forensics.

This presentation will impact the forensic science community by providing attorneys and investigators a better understanding of the capabilities, limitations, and opportunities in computer forensics and the examination of digital evidence.

The need for computer forensics and examination digital evidence has grown exponentially over the past two decades. Historically, this forensic discipline was focused on elaborate embezzlement schemes, high tech crimes like network intrusions, and possession/distribution of child pornography. With the growing popularity of smart phones, GPS devices, and social networking sites, digital media now captures a wealth of information about our daily activities. As a result, computers capture all manner of criminal activity. Sexual assaults are often preceded by frequent text messaging between the suspect and victim. Death investigations are often solved by the discovery of digital suicide notes, internet activity researching harmful chemicals, and even video clips of suicides and homicides; and drug deals are frequently conducted completely with digital communications. Liability and malfeasance in civil cases are often proven by the discovery of computer files that were altered or deleted. Finally, terrorists often rely on cell phones and email schemes to exercise command and control of their resources. As a result, just about every criminal investigation has digital media associated with it. Some of the key topics are described below.

The Anatomy & Scope of an Exam: Digital media, in general, has four types of stored data: (1) User created files like documents and spreadsheets; (2) Metadata (sometime called “data about data) that provides information about various files; (3) operating system files and file system data that direct and keep track of information about how and when programs are running; and, (4) latent information from files that were previously deleted. Attendees will have an opportunity to review some of the basics of computer science and how these principles are exploited to extract evidence from digital media.

Judicial Disposition and the Key Court Cases and Documents in Digital Evidence – *Frye*, the *Daubert* Trilogy, *Melendez-Diaz*, *Ashcroft vs. Free Speech*, ISO 17025, and several others: Attendees will explore several important legal aspects of computer forensics. Fundamentally, there is some confusion about whether computers are “searched” or “examined.” Validation poses special challenges in computer forensics because hardware, firmware, and software are often changing. Finally, computer forensics has some special challenges in defining and applying common laboratory ideas like calibration, measurement uncertainty, and error rates.

How to Write the Ideal Lab Request and Understand a Computer Forensics Lab Report: Examination requests that take the form of, “please tell me everything about this computer,” often result in delays and confusion. Attendees will learn how to tailor their request to get the information they are looking for and how to work with examiners to shape reports that make sense.

Key Questions for Direct & Cross Examination: (1) Validation Studies?; (2) Calibration?; (3) Protocol/Order of Exam?; (4) Role of Malicious Code?; (5) Attribution of Contraband?; and, (6) Electronic Discovery and the Role of Peer-to-Peer Networks and Social Networking?

Although this presentation is geared towards attorneys and investigators who are fairly new to computer forensics, it will contain material that will serve as a nice review for those with more experience.

The opinions or assertions contained herein are the private views of the authors and are not to be construed as official or as reflecting the views of the Department of the Air Force, Department of the Army, Defense Intelligence Agency or the Department of Defense.

Computer Forensics, Digital Evidence, Media Exploitation

* *Presenting Author*