W12 Eric Zimmerman's Open Source Forensic Tools Library

Alan E. Brill, MBA, Kroll Cyber Security, 300 Harmon Meadow Boulevard, Ste 305, Secaucus, NJ 07094; Marla E. Carroll, BS, Forensic Video & Audio Associates, Inc, 6919 W Broward Boulevard, Ste 222, Plantation, FL 33317; and Eric Zimmerman, BS*, Kroll Associates, Inc, 600 Third Avenue, New York, NY 10016*

After participating in this workshop, attendees will better understand the challenges facing digital forensic software developers to both design and maintain open source tools and will understand how to prepare and use an open source digital forensic toolkit to conduct examinations. Attendees will better understand the relative advantages of commercial forensic packages and open source tools and where they can be used in concert to impact the work of digital forensic examiners. Those attending will learn the specific capabilities and methods of use of one of the most well-known open source libraries of digital forensic software. Issues vital to those who would develop and maintain forensic software, such are architecting through plug-ins to evolve functionality as opposed to monolithic executables, will be discussed as well as how that architecture can allow forensic examiners to expand the tools' capabilities by developing plug-ins to meet their particular casework needs and challenges. Finally, this session will help forensic examiners better understand how growing complexity and evidence volumes are making the ability to perform triage and focus on those elements most likely to be relevant to the investigation. This session will help the forensic community understand the balance between thoroughness and timeliness that is the hallmark of real-world cases that our examiner community faces every day.

This presentation will impact the forensic science community by demonstrating that freely available, open source forensic tools and forensic libraries can help both public and private sector organizations.

Software initially developed to support investigations into online sexual exploitation of children (which in one year resulted in the rescue of at least 45 children, the execution of 300 search warrants, and 222 arrests of suspects) was recognized as having value to the forensic community as a whole and was evolved into an open source library. Challenges faced in child trafficking and child pornography investigations — such as the need to quickly and efficiently parse hundreds of thousands of files when time and resources are limited — have become challenges for all forensic examiners as typical storage drives have come to contain hundreds of thousands of system, application, and user files. Attendees will also learn how open source forensic software can be created and modified as new operating system versions and forensic challenges arise. These tools are now used by thousands of forensic examiners in more than 50 countries; this workshop will help make the knowledge of how to employ these important tools available to forensic investigators worldwide. Because of the use of both open source and plug-in architecture, forensic examiners can develop and publish their own plug-ins to the benefit of the forensic community as a whole.

Tools, Computer, Open Source

*Presenting Author