C33 Known Source Artifacts Examination With Digital Forensic Tools

Hayden A. Hendrickson, BS, Eastern Kentucky University, Computer Science, Richmond, KY 40475; Amanda A. Moses, BS, Kentucky State Police, Frankfort, KY 40601; Kimberly Bradley, MS, Kentucky State Police, Electronic Crime, Frankfort, KY 40601; Shuangteng Zhang, PhD, Eastern Kentucky University, Richmond, KY 40475*

Learning Overview: After attending this presentation, attendees will understand the capability of various digital forensic tools when used to examine devices with known, documented activities. Recovery of artifacts related to activity is attempted by using each tool. Each tool's data extraction will be reviewed for the tool's ability and accuracy of locating the artifact.

Impact on the Forensic Science Community: This presentation will impact the forensic science community by introducing knowledge regarding how forensic tools extract known expected artifacts. This knowledge will help examiners validate examination results and know which tool could be used to get a more precise representation of what has occurred on a device. This presentation will not only give examiners knowledge on forensic tools for Windows® computers, but also for mobile devices.

In the field of digital forensics, forensic software plays a major role in obtaining the evidence used in convicting or excluding someone of a crime. Multiple different digital forensic tools have come to the market in recent years and all these tools are claimed to be the best for all the examiner's needs for extracting and reporting digital evidence. However, because these tools process the data using different methods and present the recovered evidence in various ways, it is very challenging for the examiners to know how each tool behaves. In order to overcome this challenge, it is important for digital forensic investigators to have the knowledge of what tools are best at doing certain tasks they want the tools to do. This presentation is designed to provide digital forensic practitioners with that knowledge.

Digital forensic examiners must prepare every examination as if it were to be presented in court. Having confidence in the tools and methods used for data extraction is a critical element for testimony. This presentation will provide attendees with information about effectively comparing the forensic tools and how the results can vary depending on the software used. Windows® computers and mobile device technology change at a rapid rate and the amount of people who use mobile devices grows every year. With more devices that are constantly changing, it has become increasingly important that examiners be aware of the differences in examination results and know how to validate their findings.

This presentation will provide an overview of methods to validate different forensic software tools and their capabilities for discovering related digital evidence on Windows® computers and mobile devices.

Digital Forensics, Artifacts, Digital Forensic Tools

*Presenting Author