C33 Representing and Exchanging Cyber-Investigation Information in a Standard Format

Sean Barnum, BS, MITRE, 7515 Colshire Drive, McLean, VA 22102; Eoghan Casey, PhD, University of Lausanne, Batochime, CH-1015 Lausanne-Dorigny, Lausanne, Vaud, SWITZERLAND; Ryan Griffith, BS, DC3, 911 Elkridge Landing Road, Linthicum, MD 21090; and Jonathan Snyder, BS, DC3, 911 Elkridge Landing Road, Linthicum, MD 21090*

After attending this presentation, attendees will have learned about the community-driven standard format for representing digital evidence and other cyber-investigation information. Uses and benefits of this standard are presented and initial implementations are demonstrated.

This presentation will impact the forensic science community by demonstrating how the adoption of this standard by forensic laboratories, tool developers, and other members of the digital evidence community will enable sharing, increase efficiency, enhance analysis, and reduce linkage blindness.

Any type of investigation can have a digital dimension, ranging from computers as a source of information in homicides and terrorist attacks to computers as instrumentalities of fraud and cyber-attacks. Offenders, violent and white collar alike, including drug dealers making simple use of cell phones and organized criminals making sophisticated use of computer networks, use technology in various ways. As a result, cyber-investigations are complex, multifaceted, and have specific applications within broader contexts of criminal justice systems, enterprise governance, and military operations.

Furthermore, investigations of cybercrime can involve multiple investigating entities, forensic tools, and jurisdictions that each have pieces of information needed to solve the case. It is important to bring these pieces of information together to support forensic analysis and reduce the risk of overlooked linkages. Current approaches to sharing cyber-investigation information are ad hoc, inconsistent, and inefficient. Where standardized structures are used, they are typically focused on only an individual portion of the overall cyber-investigation process, they do not integrate well with each other, or they lack coherent flexibility. Many existing information-sharing activities involve conversion of proprietary formats and are human-to-human exchanges of unstructured or semi-structured descriptions of cyber-investigation traces and analysis. Correlating results from digital forensic tools can be a time-intensive and error-prone process, largely due to the inconsistent export formats.

This presentation details a community-driven standard format to support interoperability between organizations, jurisdictions, investigations, and tools. This initiative is called Cyber-investigation Analysis Standard Expression (CASE). The intended benefits for this standard format include increased efficiency when combining and deduplicating output from multiple tools and reduced linkage blindness between investigations and jurisdictions.

Core features of this standard are presented, including how traces, actions, relationships, and provenance are represented. Examples are provided of the initial JavaScript™ Object Notification (JSON) serialization of the underlying information model. Use cases for the standard format are discussed, including collaboration and sharing, correlation and analysis, and tool comparison and interoperability. An initial proof-of-concept implementation of CASE is demonstrated using the open source "plaso" forensic framework.

Attendees are invited to join this community effort, using the standard in their organizations and tools, and proposing improvements to the standard.

Digital Evidence, Cyber-Investigation, Information Sharing