B28 Reliability of Computer Forensic Tools: Application of Chain of Custody Principles

Daniel Ayers, MSc, and Ricard Kelly, forensic-validation.com, PO Box 97651, Manukau City, Auckland, 2241, NEW ZEALAND*

After attending this presentation, attendees will understand limitations of the reliability of current computer forensic tools, protocols, and results. Attendees will then be able to consider what modifications to their computer forensic analysis protocols may be required, and will be better informed as to the types of validation tests that should be carried out on computer forensic tools and results.

This presentation will impact the forensic science community by encouraging the forensic community to require that tool vendors improve their products to better account for how data is handled and how computations are performed. These factors will in turn improve the reliability of computer forensic evidence presented in court.

"Chain of Custody" protocols are widely used to establish that a physical exhibit uplifted from a crime scene is the same exhibit produced in court and that the exhibit has not been tampered with in any way. The chain of custody comprises every person responsible for handling the exhibit, from the person who collected it through to the person producing the exhibit in court. Each person must be able to give evidence as to from whom (or where) they obtained the exhibit, to whom the exhibit was relinquished, what happened to the exhibit whilst in their custody, and what steps were taken to ensure the integrity of the exhibit was preserved.

Computers, hard drives, and other electronic media are physical exhibits for which the chain of custody must be maintained in the usual way. However, when computer forensic analysis tools are used to examine electronic evidence the traditional chain of custody protocols may not be adequate to establish that analysis results presented in court are reliable and have not been subject to tampering.

This presentation demonstrates how inadvertent errors and deliberate tampering can adversely affect the reliability of widely used computer forensic tools in ways that may not be easily detected. The problem is illustrated using a recent case study involving multiple flaws in a widely used computer forensic tool.

Current practice and tools do not effectively address the problem are illustrated. It is argued that, with current tools and practices, the chain of custody in respect of computer forensic analysis results is often broken. It will be proposed that the issue could be addressed by adapting traditional chain of custody protocols to provide assurance over the internal processes employed by tools to read, interpret and display data.

The concept of judicial notice, the *Daubert* test and statutory provisions as to reliability of evidence are briefly discussed in the context of computer forensic tools.

Computer, Reliability, Validation

* *Presenting Author*