Measuring Systematic and Random Error in Digital Forensics

Alexander Nelson and Simson Garfinkel
NIST

International Symposium on Forensic Science Error Management – Detection, Measurement and Mitigation
July 20-24, 2015

Recognized sources of error in digital forensics include systematic errors arising from implementation errors, and random errors resulting from faulty equipment. But as digital forensic techniques expand to include statistical machine learning, another source of error will be statistical errors that arise because of chance disagreements between a statistical model and subject systems examined with that model. We consider two digital forensics systems with these different types of measurable error.

First, we show a mechanism for comparing the numerous and nuanced results of parsing a file system. Multiple storage system parsers were designed for or adapted to analyze a game console with a custom file system. However, it was initially unknown whether any of the parsers would produce a perspective of the storage system that was correct in reporting the files present and their characteristics. We adapted the parsers to produce an in-common, machine-differentiable format, and used a storage differencing algorithm to measure the relative incorrectness of each of the parsers. Discrepancies summarize errors in implementation or specification, an important report when any reverse-engineering is necessary. We discuss advantages and challenges in adopting this practice.

Second, we show how to construct a classifier using the hard drive from a multi-user computer that can determine the user responsible for creating a file. The classifier is constructed using allocated files and its accuracy determined with take-one-out cross-validation. Once created, the classifier can be used to predict the creator of files that can only be recovered with carving.