Understanding the Relevance of Error Rates In A Digital World

ATSAIC James Darnell, U.S. Secret Service
Moderator

July 23, 2015

Abstract

- Digital evidence (DE) is prone to analyst errors, aka 'systematic errors'
- Proper QA helps systematic errors to be recognized and potentially mitigated
- Random errors = process produced error that can be evaluated by a statistical rate
- DE is not purely seeking if two artifacts are from the same source
- DE instead seeks to show or imply actions by an individual

As such, random errors are not necessarily appropriate as an evaluation tool in a digital evidence process.

Panelists – Issues and Mitigation Opportunities

Dr. James Lyle, National Institute of Standards
Mary Horvath, Federal Bureau of Investigation
Dr. Mark Pollitt, Digital Evidence Professional Services, Inc.
Clay Schilling, CACI International
Sam Brothers, Customs and Border Protection
Dr. Richard Vorder Bruegge, Federal Bureau of Investigation
James Holland, Walmart, Inc.

Dr. James Lyle

- Technical (in a statistical sense) meaning of the term 'error'
- Application of error in digital forensics
  - Inherent error in an algorithm
  - Software faults in an implementation
- Some tool functions have an error rate (e.g., hashing) but other functions cannot be characterized by an 'error rate'
- Sometimes there is no agreed definition of 'the correct tool behavior' e.g., file carving.

Considering the above factors, SWGDE published *Establishing Confidence in Digital Forensics Results by Error Mitigation Analysis*

Mary Horvath

- Error mitigation's impact on forensic examiner
- Testimonial and Daubert issues

Dr. Mark Pollitt

- Examination errors
  - Accuracy
  - Reliability
  - Validation
- Analytical errors
  - Technical analysis
  - Investigative analysis
  - Failure to consider alternative explanations

- Error Mitigation Techniques available to DE examiners
  - Equipment and tool testing/performance verification
  - Forensic process and tool training
  - Written policies and procedures
  - Examination documentation
  - Technical and management oversight
  - Technical/peer reviews
  - Use of a second tool
  - Awareness of past and current problems

Sam Brothers

- Error Mitigation Through Technical Peer Review Process
  - Process Documentation
    - 'If it is not written down, it never happened'
  - Identification
  - Result Documentation
  - Author Feedback
  - Root Cause Analysis
  - Process Feedback
  - Management Buy-in
  - Process Review

Dr. Richard Vorder Bruegge

- Examiner testing as a means of demonstrating the validity of different analytical processes
  - Example - black box testing as a way of defining the accuracy of opinion based conclusions
- Defining the questions that we can answer and the limits of those answers, such as:
  - Was this digital image direct from a camera or was it computer generated or otherwise manipulated?
  - Did this camera take that photo?
  - How tall was the person in the bank surveillance photo?

Adam Holland

- Quality management program impact on DE
- Validation of work, verification of evidence
- Most common needs from DE
  - Criminal culpability
  - Substantiating policy violations in the work place
  - Other civil/contractual issues outside of criminal courts

Questions / Comments?

ATSAIC James Darnell - james.darnell@usss.dhs.gov