MITRE: Proposal to Formalize Test and Evaluation Activities Within the Forensic and Law Enforcement Communities

By

Mark Hirsh

From the proceedings of

The Digital Forensic Research Conference

DFRWS 2004 USA

Baltimore, MD (Aug 11th - 13th)

Proposal to Formalize Test and Evaluation Activities Within the Forensic and Law Enforcement Communities

Background

The American Society of Crime Laboratory Director (ASCLD) has recently defined criteria for accrediting forensic crime laboratories that process, examine, and evaluate digital evidence. ASCLD is pursuing this objective because the organization believes laboratory accreditation is an essential component of the forensic process. Benefits of accreditation are multifaceted - Examiners will be able to better articulate the procedures of the laboratory on the witness stand; Examiners will have more information ensuring the quality of their work; Examiner findings will be more readily accepted by the court because standard, widely accepted processes and procedures have been followed in examining the evidence; and lastly, the laboratory will be open to inspection by independent experts who will measure it against national standards. One of the primary requirements of accreditation is that the lab use technical procedures that have been scientifically validated.

In an attempt to address issues inherent in the validation process, the Department of Defense Cyber Crime Institute (DCCI) is proposing the initiation of a broad-based, community-wide effort to test and evaluate the forensics soundness of products that are or can potentially be used by digital forensics examiners. The test and evaluation process and procedures should be formal and repeatable. The objective is to ensure to the maximum extent possible that the findings resulting from the use of tested, validated products are accurate and irrefutable in a court of law.

Business Need

The electronic forensic process includes a myriad of tools and activities. For example, it includes activities related to supporting and carrying out search and seizure operations, evidence collection and tagging, chain of custody processes and procedures, imaging and extraction, evidence examination and analysis, the creation of documents and reports detailing the examination process and findings, and the presentation of expert testimony in a court of law. The tools used to support these activities are varied and in many cases quite complex. Ensuring that the tools operate as advertised or as expected is an important part of the forensic process because these assurances lend creditability to overall findings. A broad-based, community-wide test and evaluation (T&E) process will not only support the selection of useful, effective tools, but will also provide the needed and required assurances that the tools provide accurate, reliable, and consistent results whenever they are used.

Current State

Within the law enforcement and forensic communities, the testing of forensic products is uneven, inconsistent, and fragmented. Many organizations implement test and evaluation activities, but there are wide variations in the processes and procedures used. Some of the testing is not adequately documented and therefore not repeatable. Documentation

that has been produced is not always readily obtainable by any organization except the one producing the documents. Because of variances in processes and methods, two or more organizations testing the same product may produce inconsistent results. To apply rigor and meaning to the digital forensics laboratory accreditation process, it is essential that the processes and procedures used to test and evaluate the products used within the community be normalized and coordinated.

Vision

The forensics and law enforcement communities need to establish a centralized "Consumer Reports" library. The library should be a repository where community members can go to review the results of T&E activities for a particular product. One difference between the information contained in this library and the well-known "Consumer Reports" publication is that the Forensic T&E Repository will not contain product ratings. The library will contain information that documents the results of T&E activities, provides guidance on the use of particular products, and identifies the organization that performed the tests. The library will provide guidance for individuals involved in the procurement process and will provide background and support material for individuals involved in litigations.

Service

At a high level, the steps needed to implement a rigorous, formalized T&E process, which is designed to support the broad forensics and law enforcement communities, are as follows:

- Identify the organization(s) that is (are) willing to take the lead in defining and promoting a broad-based T&E process
- Identify the organizations that are willing to test and evaluate forensic products
- Identify areas of expertise and configure the independent test labs accordingly
- Establish the processes and procedures by which consumers and vendors can submit T&E requests for products considered useful to the electronic forensic community
- Establish the necessary funding and contractual vehicles to run the test labs
- Define the T&E high level processes and procedures that are to be followed by the test labs
- Perform beta testing to validate the thoroughness and completeness of the test processes and procedures
- Review the findings from all independent test labs
- Create the documentation library
- Establish procedures by which DoD and law enforcement organizations can access the library
- Maintain a web presence, which will serve as the primary source of information related to the status of ongoing T&E activities

Customers

The T&E process addresses requirements of individuals involved in any and all aspects of computer crime investigations. In other words, the customer base includes any person or organization that is responsible for directing and overseeing electronic forensic

activities, everyone who is involved in the computer crime examination and investigation process, and any person or organization that is developing a product that can be or is intended to be used to support activities related to electronic forensic examinations and investigations.