Digital & Multimedia Sciences
Section - 2013

B18 Computer Forensics Tool Catalog: Connecting Users With the Tools They Need

Benjamin R. Livelsberger, MS, 100 Bureau Dr, Mail Stop 8970, Gaithersburg, Maryland 20899-8970*

After attending this presentation, attendees will be introduced to the Tool Catalog website, a website that provides users with an easily searchable catalog of forensics tools. The secondary goal is to provide a map of the computer forensics tool landscape, showing where there are gaps (i.e., functions for which there are no tools). The attendees of this presentation will become familiar with the Tool Catalog website and the benefits it offers the forensics community.

This presentation will impact the forensic science community by: (1) the forensics practitioner will have a better, more efficient way of connecting with the tools and technologies they require to do their work; and, (2) the law enforcement community will gain the ability to better identify and communicate the functionalities and features they need to the development community. This is facilitated by the map of forensics functions—the Tool Taxonomy.

There are many forensics tools available. These tools perform a wide variety of functions (e.g., imaging or memory reconstruction) and work on a wide variety of technologies (from PCs to Macs, to disposable phones, to iPhones). What is missing is an effective way of connecting practitioners to the tools that meet their specific requirements. The computer forensics tool lists currently available to the community have limitations in how they are populated, and in the level of detail of information they provide about tool capabilities. Maintaining a list is time consuming and lists easily become outdated. Also, while these lists generally connect practitioners to tools, they lack specificity. For instance, a typical tool list entry for a disk imaging tool might tell a practitioner that a tool supports USB, FireWire, and SCSI drives, but will not specifically address if this support is for the tool's evidence interfaces, target interfaces, or both. It will not uniformly list the specific capabilities of similar tools, such as for a disk imaging tool: the hash algorithms and image file types they support; supported acquisition methods (disk-to-disk or disk-to-file); whether it can encrypt data; if it supports block hashing, etc. Such specifics are important for connecting practitioners to the tools they require but are very time consuming to collect.

The website has three major sections. First, there is a description of forensic functionalities and technical parameters. This is the Tool Taxonomy. Currently, eight functionalities are defined, along with associated technical parameters and technical parameter values. These allow a tool's capabilities to be characterized. Example forensic functionalities are disk imaging, deleted file recovery, and mobile device acquisition and analysis. Example technical parameters for disk imaging include runtime environment, evidence interfaces, target interfaces, supported image file formats, hash algorithms, and acquisition methods. New functionalities will be added to the Tool Catalog based on the work of the Computer Forensics Tool Testing project.

Second is a search feature to find tools. Users can select their requirements in terms of functionality needed as well as specific technical parameter values. A list of tools that match the search criteria is returned. For example, a user might formulate a search for "all disk imaging tools that have support for acquisition to a networked file system, support the dd, E01, and AFF image file formats and support the SHA256 hash algorithm."

The third section of the Computer Forensics Tool Catalog site is a set of pages for vendors to input information about their tools and for public feedback. Unlike traditional tool lists, the Tool Catalog is not populated by a single entity or via crowd sourcing; the website is populated with tools by tool vendors. Tool submissions are reviewed at NIST prior to being posted to the website. Two advantages of this approach are that it takes the pressure off the single person or entity of keeping abreast of the latest tool developments and it leaves the task of populating the tool's specific capabilities to the party who knows them best, the vendor. Comments and feedback from both vendors and the forensics community are welcomed and are key for improving and keeping the Tool Catalog current.

Digital Forensics, Tool Taxonomy, Website

** Presenting Author*