B13 Computer Forensic Bitmaps and Visualization for Data Identification

Shane A. Macaulay, Security Objectives Corporation, 1100 Dexter Avenue North, Suite 100, Seattle, WA 33487*

After attending this presentation, attendees will understand some of the principles of visualization techniques which can be applied to data identification.

This presentation will impact the forensic science community by discussing the components used to generate bitmaps from opaque data regions. Attendees will be presented visualized examples from several public data sources and understand how these can be applied toward forensic methods and tools.

These images are generated fundamentally by using variable block hashing combined with advanced search techniques (akin to an overlay network of a distributed hash table) and guaranteed binary clone detection.

Using established cryptographic algorithms, or "digital fingerprints", with scaled variable size, applied to an opaque data region, illustrates a domain of knowledge when extrapolated against what is currently known in an existing database. Database seed material would typically be data from sources such as National Institute of Standards and Technologies (NIST) National Software Reference Library (NSRL), or other similar collections.

Bitmap generation applications can be used for coverage analysis, isolation of unknown or new artifacts and also data recovery. Data

interpretation, comprehension, recovery, and analysis of many forms may not need to be visualized but do benefit from bitmaps without coloring for determining probability or even partial matches.

Results of some recent colorized (visual) bitmaps are of a gigapixel class. Measuring the overall process of generation in some tens of minutes is an encouraging sign for future terapixel scale images.

Forensic Visualization, Variable Block Hashing, Data Search

** Presenting Author*