## B27 The Application of Known Sample Searching to Digital Forensics

*Robert Monsour, BA*, Forensics3, PO Box 79134, Corona, CA 92877*

After attending this presentation, attendees will gain an understanding of the potential benefits and challenges of applying known sample searching to the field of digital forensics.

This presentation will impact the forensic science community by discussing how the application of known sample searching to digital forensics can allow examiners to search for and identify thousands of potentially important artifacts, including artifacts which examiners may not otherwise recognize. It will also assist examiners in confirming the origin of artifacts identified during investigations, and in more precisely understanding the activity that led to the creation of specific artifacts. Finally, the presentation may aid in generating interest, debate, and additional work in the application of known sample search techniques to digital forensics.

The forensic sciences have long used databases of known samples to assist in the identification of a wide range of physical evidence items. In this methodology, items such as paint chips or shoe prints are digitally quantified and searched against a database of known samples in order to identify the origin of an evidence item.

Surprisingly, the field of digital forensics has yet to generate a government or commercial solution for comparing digital evidence against a large collection of known samples in order to pinpoint artifacts that might be of evidentiary significance.

Forensic examiners typically learn to recognize and understand common digital artifacts through training, research, and experience. It can take several years for a forensic examiner to be able to recognize and understand even a few hundred common artifacts. The development of an automated system for screening evidence for thousands of known artifacts has the potential to allow examiners to identify many more digital artifacts than is currently possible through traditional training methods.

A year-long research effort aimed at developing the first comprehensive solution for screening digital evidence for known artifacts was started. The resulting solution allows forensic examiners to search digital evidence for over 2,000 artifacts left by popular websites and applications. This product is currently being tested by law enforcement and corporate digital forensic examiners in the United States.

Using this research effort as a case study, the potential benefits and practical issues involved in applying known sample searching to digital forensics will be discussed. Many artifacts not generally known in the forensic community were identified through the effort to develop this solution, indicating a known sample methodology may have the potential to allow investigators to locate artifacts that might otherwise go unnoticed. The benefits of using a keyword-based approach to known sample screening versus relying on more complex scripting will be discussed, which can allow development of known sample search solutions to keep pace with the constant changes associated with website and application artifacts. Finally, potential pitfalls and challenges of applying known sample search methods to digital forensics will be discussed.

**Digital Artifacts, Keyword Searches, Known Sample Searching**

 ** Presenting Author*