B9 Applying Advanced Search Techniques to Digital Forensics

Brian D. Carrier, PhD, Basis Technology, One Alewife Center, Cambridge, MA 02140*

After attending this presentation, attendees will have a better understanding of what search techniques exist, but are not yet being applied to digital forensics. Attendees will see an example of how these techniques can be applied to digital forensics tools.

This presentation will impact the forensic science community by discussing and talking about how research advances in other fields (namely information retrieval) can be applied to digital forensics to help an investigator more quickly locate evidence.

Keyword searching is common in a digital investigation, but primitive methods are currently being used. Keywords are entered and a list of files with the keyword is given. The files could be listed by file name, by the order the search tool found them in, or something else. It is similar to searching the web 10 years ago. There have been many advances in search techniques that could be applied to digital investigations to help find evidence more quickly. Examples of advances include faceted search, clustering search results by topic, generating automated summaries of documents, and improved ranking. These techniques would allow the investigator to more quickly review search results and ignore the false positives. This presentation will provide an overview of these technologies and demonstrate how they can be used in an investigation.

Digital Evidence, Search, Analysis Tools

** Presenting Author*