Digital Media Sector Hashing for Evidence Correlation

Law enforcement entities collect and process large volumes of digital evidence in the course of conducting investigations. However, previously examined digital evidence may not be identified by investigators as relevant to an ongoing investigation. A CINA effort led by Dr. Jim Jones (George Mason University) proposed a project that will demonstrate that digital content relevant to a current investigation is present on previously acquired digital media, to provide the basis for re-examining such media, without reexamining previously acquired digital evidence.

The proposed solution includes a primary repository of evidence hashes (not actual evidence), and a lightweight field deployable component. The prototype developed in the project can be used to search found hard drives, phones, and other devices for evidence much more quickly than previously possible, as well as detecting fragments of files that have been deleted.

The prototype will reduce the time spent locating digital evidence and determine the probability that a deleted piece of evidence was present on a device, and allow agents in the field and at regional centers to quickly establish that previously collected evidence may contain evidence relevant to a new investigation.

To request more information or a demo of the prototype, please contact cina@gmu.edu.