Digital Forensics

Dr. Bhavani Thuraisingham
The University of Texas at Dallas

Evidence Correlation

November 2011

Papers to discuss

- Forensic feature extraction and cross-drive analysis
  - http://dfrws.org/2006/proceedings/10-Garfinkel.pdf
- A correlation method for establishing provenance of timestamps in digital evidence
  - http://dfrws.org/2006/proceedings/13-%20Schatz.pdf

Abstract of Paper 1

- This paper introduces Forensic Feature Extraction (FFE) and Cross-Drive Analysis (CDA), two new approaches for analyzing large data sets of disk images and other forensic data. FFE uses a variety of lexigraphic techniques for extracting information from bulk data; CDA uses statistical techniques for correlating this information within a single disk image and across multiple disk images. An architecture for these techniques is presented that consists of five discrete steps: imaging, feature extraction, first-order cross-drive analysis, cross-drive correlation, and report generation. CDA was used to analyze 750 images of drives acquired on the secondary market; it automatically identified drives containing a high concentration of confidential financial records as well as clusters of drives that came from the same organization. FFE and CDA are promising techniques for prioritizing work and automatically identifying members of social networks under investigation. Authors believe it is likely to have other uses as well.