Doctoral Dissertations 2014-current

INFERENCE-BASED FORENSICS FOR EXTRACTING INFORMATION FROM DIVERSE SOURCES

Robert J. Walls, *University of Massachusetts - Amherst*

Follow

Date of Award
Summer 9-1-2014

Document Type
Open Access Dissertation

Degree Name
Doctor of Philosophy (PhD)

Degree Program
Computer Science

First Advisor
Brian Neil Levine

Keywords
Digital Forensics

Subject Categories
Computer Security

Abstract
Digital forensics is tasked with the examination and extraction of evidence from a diverse set of devices and information sources. While digital forensics has long been synonymous with file recovery, this label no longer adequately describes the science's role in modern investigations. Spurred by evolving technologies and online crime, law enforcement is shifting the focus of digital forensics from its traditional role in the final stages of an investigation to assisting investigators in the earliest phases — often before a suspect has been identified and a warrant served. Investigators need new forensic techniques to investigate online crimes, such as child pornography trafficking on peer-to-peer networks (p2p), and to extract evidence from new information sources, such as mobile phones.

The traditional approach of developing tools tailored specifically to each source is no longer tenable given the diversity, volume of storage, and introduction rate of new devices and network applications. Instead, we propose the adoption of flexible, inference-based techniques to extract evidence from any format. Such techniques can be readily applied to a wide variety of different evidence sources without requiring significant manual work on the investigator's part. The primary contribution of my dissertation is a set of novel forensic techniques for extracting information from diverse data sources. We frame the evaluation using two different, but increasingly important, forensic scenarios: mobile phone triage and network-based investigations.

Via probabilistic descriptions of typical data structures, and using a classic dynamic programming algorithm, our phone triage techniques are able to identify user information in phones across varied models and manufacturers. We also show how to incorporate feedback from the investigator to improve the usability of extracted information.

For network-based investigations, we quantify and characterize the extent of contraband trafficking on peer-to-peer networks. We suggest various techniques for prioritizing law enforcement's limited resources. We finally investigate techniques that use system logs to generate and then analyze a finite state model of a protocol's implementation. The objective is to infer behavior that an investigator can leverage to further law enforcement objectives.

We evaluate all of our techniques using the real-world legal constraints and restrictions of investigators.

Recommended Citation

Walls, Robert J., "INFERENCE-BASED FORENSICS FOR EXTRACTING INFORMATION FROM DIVERSE SOURCES" (2014). *Doctoral Dissertations 2014-current.* Paper 265.
http://scholarworks.umass.edu/dissertations_2/265