Introduction to
Digital Forensics - Education, Research and Practice Minitrack

Kara Nance  
Department of Computer Science  
University of Alaska Fairbanks  
klnance@alaska.edu

Matt Bishop  
Department of Computer Science  
University of California Davis  
bishop@cs.ucdavis.edu

Amelia Phillips  
CIS and CS Departments  
Highline Community College  
aphillip@highline.edu

The field of digital forensics has evolved to allow security professionals to examine evidence from the increasing plethora of digital devices to help determine what individuals might have done in the past. The evidence collected is used in a wide variety of settings: from corporate server farms to police raids on criminals' houses to the modern battlefield. The primary goals are twofold: to determine what happened and to determine who might be responsible.

Work in digital forensics covers a wide variety of areas. Some work in digital forensics is largely procedural. Different organizational entities have unique requirements for forensic results. For example, law enforcement needs to produce compelling and legally recognized evidence to prosecute crimes; corporations might need to identify and mitigate an insider threat, requiring a lower standard of proof; and military intelligence needs might require quick action based on a limited amount of information. Papers in this session begin to delve deeper into the challenges that continue to grow in this emerging field. What type of person is attracted to cyber crime? Who has an interest in the outcome of the investigations and how does that affect the approach taken?

Other forensic work is more technical. The advent of new technologies, such as the rapid proliferation of mobile devices and related malware, means that forensics researchers must develop new techniques for acquiring and analyzing data from the new devices that they encounter in their cases. Cutting-edge research efforts on Android applications in this session are representative of these efforts. The issue of anti-forensic methods that can be used to thwart investigators is also explored.

This year, five papers were selected to be presented in the Digital Forensics - Education and Research Minitrack. They provide good coverage of the wide range of topics described above.

In Including Stakeholder Perspectives in Digital Evidence Programs, Colin Armstrong examines the methodology of how to teach evaluation of the worldview of the various stakeholders in a forensic investigation.

Cybercrime Assessment and Offender Profiling by Stephenson and Walter gets stimulate thought about the characteristics of a cyber criminal. While popular TV shows illustrate it, this paper examines how profiling techniques could potentially be applied to digital forensics.

While mobile devices continue to grow in their complexity and widespread use, their vulnerabilities increase. This year, several papers address these important and timely issues. In Android: Static Analysis Using Similarity Distance, Anthony Desnos examines the proliferation of Android products on the market which may have been tampered with. He addresses the problem of the high number of applications available and how similarity distance can be used to identify characteristics of the applications to identify malware injections, piracy, and to distinguish these from patches and updates.

In STAAF: An Efficient Distributed Framework for Performing Large-Scale Android Application Analysis, Smith and Pridgen delve more deeply into the ever-increasing number of applications and malware targeting the Android. They present a method to analyze malware and new Android apps in a collaborative manner that attempts to safeguard the user choosing from the pool of over 50,000 apps that are currently available.

In Novel Anti-forensics Approaches for Smart Phones, Azadegan et al. from Towson University present methods to use anti-forensics techniques against the most widely used commercial forensics tools. The Android wins again as they use an Android phone to demonstrate the techniques.

The papers in this session represent much of the ongoing work in the forensics community. They are an exciting sample of a larger body of work dedicated to ensuring that digital evidence remains available and useful for the good of the public.