2014 47th Hawaii International Conference on System Science

Introduction to HICCS-47
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

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, and now to international cloud environments. This year, we accepted three papers for presentation in the Digital Forensics - Education and Research Minitrack which should promote an interesting discussion on anti-forensics as well as the opportunity to demonstrate some new educational techniques to stimulate our next generation of digital forensic researchers. The papers in this session represent much of the ongoing work in the forensics community and 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.

While mobile devices continue to grow in their complexity and widespread use, their vulnerabilities increase. As digital forensics techniques are developed, anti-forensic techniques also evolve in an ongoing "arms race." This year two papers address the important concept of anti-forensics.

In *Mobile Phone OS Anti*-Forensics by Karlsson and Glisson, they discuss how Android mobile devices inherently create opportunities to present environments that are conducive to anti-forensics activities. This paper will stimulate discussion on the viability of operation system modifications in an anti-forensics context and provides a direction for future research in this area.

In *iOS Anti-forensics: How Can We Securely Conceal, Delete, and Insert Data?* D'Orazion, Ariffin and Choo consider some of the same issues, but as applied to an iOS environment. They propose three techniques: concealment, deletion, and insertion, which may be challenging to detect during a forensics investigation.

Our final paper, *Teaching Digital Forensics Techniques for Process Identification within Linux Environments*, describes an intriguing digital forensics Honeynet Project Challenge that can be adapted for educational purposes in a lab-lecture format. McDaniel and Hay address some of the challenges that complicate the design and presentation of traditional digital forensics exercises and provide in-depth discussion of a proven example that can be used and extended by digital forensics educators.

978-1-4799-2504-9/14 $31.00 © 2014 IEEE
DOI 10.1109/HICSS.2014.592