Introduction to HICCS-49
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
mabishop@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 some interesting discussions in some emerging areas of digital forensics. The papers in this session represent much of the ongoing work in the forensics community and are an exciting representation of a larger body of work dedicated to ensuring that digital evidence remains available and useful for the good of the public.

The papers this year are diverse in topic including Android, educating the judiciary, and file matching based on content similarity rather than hashing. The diversity in topics provides a well-rounded view of the current state of digital forensics and some focus areas that need additional attention.

In *Do Multimedia Presentation Enhance Judiciary's Technical Understanding of Digital Forensic Concepts? An Indonesian Case Study,* by Cahyani, Martini, and Choo of the University of South Australia, they discuss the challenges associated with using digital evidence in courts. It has long been observed that the members of the judiciary and law enforcement agencies need to understand digital evidence. This case study analyzes the effects of educating the participants to determine if their understanding of some technical concepts was improved through the utilization of multimedia-based training in the specific concepts. The methodology and results provide an excellent foundation for discussion on the potential expansion of this case study to other populations.

In *Text-based Document Similarity Matching Using sdtext,* Shields of Georgetown University discusses an alternative to the traditional approach of hashing to identify duplicate files. He introduces a tool, sdtext, which has shown success in comparing files with similar content, despite differing file formats. This novel approach to determining file duplicate provides some interesting options for digital forensics investigators.

Our final paper, *An Android Social App Forensics Adversary Model*, by Azfar, Choo, and Liu presents an adaptation of a popular adversary model from cryptography to the collection and analysis phases of mobile device forensics. The model is demonstrated using popular Android social applications including Twitter, POF Dating, Snapchat, Fling, and Pinterest. As digital forensics investigations increasingly involve mobile devices, the model is likely to stimulate further research and discussion about the recreation and analysis of social profiles.