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 very forward-thinking, addressing issues that are challenging and which have not yet received adequate attention. All three papers will challenge the audience to change the status quo and help to evolve the practice of digital forensics.

In *Investigating the Impact of Global Positioning System Evidence*, by Berman, Glisson, and Glisson, they discuss how the increasing amalgamation of global positioning systems (GPS) into our daily technology-enhanced lives is leading to a growing contribution of these devices as evidence in legal proceedings of all types. This paper presents some interesting cases from the United Kingdom and Europe to demonstrate how the presentation of GPS evidence has increased in the past decade.

In *Utilizing Network Science and Honeynets for Software Induced Cyber Incident Analysis*, researchers from the Naval Research Laboratory and Arizona State University introduce a network science-based framework to conduct incident analysis on datasets through construction and analysis of communications within a population. They evaluate this framework by applying it to BlackEnergy, a malware network. This paper should lead to some interesting discussions of this new alternative to malware analysis.

Our final paper, *Building a Forensics Computing Language*, present an innovative idea for the development of a domain-specific language (DSL) focused on the requirements of forensic and security analysis. Roussev, from the University of New Orleans, discusses the deficiencies in our traditional methodology and presents an initial design sketch for a forensic DSL to illustrate the ideas behind the approach. Discussion of new ideas, such as this, by the digital forensics community is important if we wish to continue to move our practice forward to meet the challenges that we are currently facing.