Systematic Approaches to Digital Forensic Engineering (SADFE)

Preliminary CFP

Together with

2018 IEEE Security and Privacy

The 12th International Conference on Systematic Approaches to Digital Forensic Engineering (SADFE) is calling for paper submissions in the broad field of Digital Forensics from both practitioner and researcher's perspectives. With the dynamic change and rapid expansion of the types of electronic devices, networked applications, and investigation challenges, systematic approaches for automating the process of gathering, analyzing and presenting digital evidence are in unprecedented demands. The SADFE conference aims at promoting solutions for related problems.

Past speakers and attendees of SADFE have included computer scientists, social scientists, forensic practitioners, lawyers and judges. The synthesis of hard technology and science with social science and practice forms the foundation of this conference. Papers focusing on any of the system, legal, or practical aspects of digital forensics are solicited.

Topics to be Addressed

Potential topics to be addressed by submissions include, but are not limited to:

- Digital Data and Evidence Management: advanced digital evidence discovery, collection, management, storage and preservation
  - Identification, authentication and collection of digital evidence
  - Extraction and management of forensic data/metadata
  - Identification and redaction of personally identifying information and other forms of sensitive information
  - Post-acquisition handling of evidence and the preservation of data integrity and admissibility
  - Evidence and digital memory preservation, curation and storage
  - Architectures and processes (including network processes) that comply with forensic requirements
  - Managing geographically, politically and/or jurisdictionally dispersed data artifacts
  - Data, digital knowledge, and web mining systems for identification and authentication of relevant data
  - Botnet forensics
- Digital Evidence, Data Integrity and Analytics: advanced digital evidence and digitized data analysis, correlation, and presentation
  - Advanced search, analysis, and presentation of digital evidence
  - Cybercrime scenario analysis and reconstruction technologies
  - Legal case construction and digital evidence support
  - Cyber-crime strategy analysis and modeling
  - Combining digital and non-digital evidence
  - Supporting both qualitative and statistical evidence
  - Computational systems and computational forensic analysis
  - Digital evidence in the face of encryption
  - Forensic-support technologies: forensic enabled and proactive monitoring/response

- Forensics of embedded or non-traditional devices (e.g. digicams, cell phones, SCADA, obsolete storage media)
  - Innovative forensic engineering tools and applications
  - Proactive forensic-enabled support for incident response
  - Forensic tool validation: methodologies and principles
  - Legal and technical collaboration
  - Digital forensics surveillance technology and procedures
  - "Honeypot" and other target systems for data collection and monitoring
  - Quantitative attack impact assessment
  - Comprehensive fault analysis, including, but not limited to, DFE study of broad realistic system and digital knowledge failures, criminal and non-criminal, with comprehensive DFE (malicious/non-malicious) analysis in theory, methods, and practices.
- Forensic and digital data integrity issues for digital preservation and recovery, including
  - Technological challenges
  - Legal and ethical challenges
  - Economic challenges
  - Institutional arrangements and workflows
  - Political challenges and
  - Cultural and professional challenges
- Scientific Principle-Based Digital Forensic Processes: systematic engineering processes supporting digital evidence management which are sound on scientific, technical and legal grounds
- Legal/technical aspects of admissibility and evidence tests
  - Examination environments for digital data
  - Courtroom expert witness and case presentation
  - Case studies illustrating privacy, legal and legislative issues
  - Forensic tool validation: legal implications and issues
  - Legal and privacy implications for digital and computational forensic analysis
  - Handling increasing volumes of digital discovery
  - New Evidence Decisions, e.g., United States v. Jones, _ U.S._ (2012) and United States v. Kotterman, _ F.3d _(9th Cir. 2013)
  - Computational Forensics and Validation
  - Transnational Investigations/Case Integration under the Convention on Cybercrime of the Council of Europe
  - Issues in Forensic Authentication and Validation.
- Legal, Ethical and Technical Challenges
  - forensic, policy and ethical implications of The Internet of Things, The "Smart City," "Big Data" or Cloud systems

Review Process

Papers will be double-blind reviewed using the EasyChair Submission system. Each paper will received no less than three professional peer reviews with results used for acceptance determination.

Workshop Planning Schedule

Important dates:

- Deadline for full papers and "SADFE Challenge" papers: 1/16/2018
- Deadline for panel proposals: 2/28/2018
- Notification of acceptance or rejection: 2/10/2018
- Deadline for final paper camera ready copy: 3/5/2018
- Deadline for poster session abstracts: 2/28/2018
- IEEE/SADFE-2018 workshop dates: 5/24/2018