Tenth International Conference on Systematic Approaches to Digital Forensics Engineering

SADFE 2015

http://sadfe.org

September 30th – October 2nd, 2015, Málaga, Spain

Preliminary Call for Papers

Digital forensics engineering and the curation of digital collections in cultural institutions face pressing and overlapping challenges related to provenance, chain of custody, authenticity, integrity, and identity. The generation, analysis and sustainability of digital evidence require innovative methods, systems and practices, grounded in solid research and understanding of user needs. The term digital forensic readiness describes systems that are build to satisfy the needs for secure digital evidence.

SADFE-2015 investigates requirements for digital forensic readiness and methods, technologies, and building blocks for digital forensic engineering. Digital forensic at SADFE focuses on variety of goals, including criminal and corporate investigations, data records produced by calibrated devices, as well as documentation of individual and organizational activities. Another focus is on challenges brought in by globalization and cross-legislation digital applications. We believe digital forensic engineering is vital to security, the administration of justice and the evolution of culture.

Conference Topics

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

Important Deadlines

Paper submission: **July 14th, 2015**

Accept/Reject Notification: **August 15th, 2015**

Camera-ready papers: **September 1st, 2015**

Conference: **Sept. 30th – Oct. 2nd, 2015**

Publication

SADFE-2015 papers will be published in the Journal of Digital Forensics, Security and Law (JDFSL) and will undergo a double-blind review process.

Best paper award

A Best Paper Award will be made for the final papers.

Contact Information

Detailed submission instructions and additional details about the workshop can be found at **http://sadfe.org.** For any other question related to the submission please contact the SADFE 2015 PC chairs: Carsten Rudolph (rudolphc@web.de); Nicolai Kuntze (nicolai.kuntze@gmail.com); and Barbara Endicott-Popovsky (endicott@u.washington.edu).

For questions related to the organization of SADFE 2015 please use the following contacts:

Antonio Maña, University of Malaga
amg@lcc.uma.es
+34 951 952 940

Michael Losavio, University of Louisville
michael.losavio@louisville.edu
+1 502 852 3509