The SADFE (Systematic Approaches to Digital Forensic Engineering) International Workshop is intended to further the advancement of computer forensic engineering by promoting innovative & leading-edge systematic approaches to cyber crime investigation. The workshop brings together top digital forensic researchers, advanced tool/product builders, and expert law enforcement from around the world for information exchange and R&D collaboration.

Today’s cyber investigation faces many difficult challenges. In the 2001 US v. Gorshkov case, the hackers employed a wide array of distributed Perl scripts that transcend across national boundaries to trigger massive numbers of coordinated online auctions, email confirmations, and other fake transactions to accomplish fraudulent electronic fund transfers on numerous stolen credit card records. Under such a reality, the foremost daunting challenge is the discovery and collection of voluminous and often globally distributed digital evidence. At the same time, increasing sophistication of modern cyber crimes further adds to the difficulty of correlating and piecing together physical and digital evidence for scenario reconstruction. Criminal suspects must also be identified, located and apprehended often within a legally challenging international context. Additionally, both legal and technical teams must work closely together to build a court-admissible case toward eventual conviction. This frequently implies that the strategy and the direction of the investigation may not be entirely technically driven at times. Issues such as privacy, admissibility and international laws often require careful consideration.

Modern digital forensic engineering needs to go beyond mere tool application and evidence gathering. Such an ad hoc approach is becoming increasingly limited in effectiveness and scalability. Therefore, in addition to advanced digital evidence discovery, gathering and correlation, SADFE recognizes the value of solid digital forensic engineering processes based on both technical and legal grounds. SADFE further recognizes the need of advanced forensic-enabled and proactive monitoring/response technologies. SADFE 2005 addresses broad-based, innovative digital forensic engineering technology, practical experience & process areas:

- Systematic engineering processes & methodologies for computer forensic
- Advanced techniques in evidence collection, search, analysis, correlation, handling and preservation
- Progressive cyber crime scenario analysis and reconstruction technology
- Legal case construction & digital evidence support
- Legal and technical collaboration
- Legal and technical aspects of tool validation
- Courtroom expert witness and case presentation
- Intrusion detection systems (IDS) for computer forensic
- Forensics of embedded devices (e.g. digicams, cell phones)
- Innovative forensic engineering tools and applications
- Attack strategy analysis & modeling
- Privacy, legal and legislation issues
- Monitoring and incident response
- Forensic-enabled architectures and processes
- Advanced system and application log analysis
SADFE’s vision was made possible only by the warm support from the below listed organizations. We deeply appreciate their generosity and the willingness to work with us and the international digital forensic community to advance this critical technology benefitting the global cyber security and law enforcement communities.

- Ministry of Education, Taiwan, Republic Of China
- National Science Council, Taiwan, Republic of China
- Taiwan Information Security Center, Taiwan, Republic of China
- National Cheng Kung University
- National Taiwan University of Science and Technology (NTUST)
- Chinese Cryptology and Information Security Association (CCISA)

Der-Tsai Lee (Honorary Chair), Taiwan Information Security Center
Chi Sung Laih (General Chair), National Cheng Kung University
Ming-Yuh Huang (Program Co-Chair), The Boeing Company
Jung-Shian Li (Program Co-Chair), National Cheng Kung University
Tzong-Chen Wu (Treasure Chair), National Taiwan University of Science and Technology

September 7, 2005