Editorial

Systematic Approaches to Digital Forensic Engineering: Moving from Art to Disciplines

Ming-Yuh Huang
The Boeing Company
Ming-yuh.huang@boeing.com

Deborah A. Frincke
Pacific Northwest National Laboratory
Deborah.frincke@pnl.gov

Abstract

This paper introduces the SADFE 2007 conference, including a discussion of challenge areas in Forensics in general and for Forensics 2007.

1. Welcome

Welcome to SADFE 2007! The second SADFE (Systematic Approaches to Digital Forensic Engineering) International Workshop will be held April 2007 in Seattle. SADFE is a workshop intended to promote systematic approaches to cyber crime investigation, by furthering the advancement of digital forensic engineering as a disciplined practice. Unlike ad-hoc computer forensics, digital forensic engineering is characterized by the application of scientific and mathematical principles to the investigation and establishment of facts or evidence, either for use within a court of law or to aid understanding of cyber crimes or cyber-enabled crimes. Advancing digital forensics engineering requires the expertise of technologists, analysts, and legal experts to produce sound computer systems and sound forensic practices which will meet the needs of courtroom presentation as well as minimizing negative effects on the cyber-system original purpose. As with the first year, the 2007 SADFE workshop brings together top digital forensic researchers, advanced tool/product builders, and expert law enforcement representatives from around the world for information exchange and R&D collaboration.

2. Why a workshop on forensics?

There are many challenges involved in establishing a true engineering discipline in digital forensics, including scale, scope and presentation or reintegration of primarily technical information and conclusions into a non-technical societal framework. At the early stages of the development of applied disciplines, it is important to bring together a gamut of stakeholders and developers. In forensics it is especially important that efforts focus on work that is applicable to society’s needs and grounded in strong scientific and engineering principles, Hence SADFE’s emphasis on integration of backgrounds within a workshop format.

3. Digital forensic evidence: current and future challenges

Why is the digital aspect of forensics such a challenge? Digital information useful in understanding cyber-crimes and cyber-enabled crimes involves the gamut of possible scales in time, volume, and location: it may be available for only nanoseconds, or over the course of several years; it may involve only a single bit that has been modified, or huge volumes of data; it may be found within the smallest components of a system, or spread globally throughout a variety of
infrastructures. It may even be legal for some analysts to collect and observe and share, but not others. Correlating large amounts of digital information, establishing their relevance in the context of crime scenario construction, as well as presenting the complete picture in a court of law, are all challenges worthy of significant research.

Early forays into use of digital forensic evidence tended to be based on tool application and evidence gathering, with little foresight or consideration of sound engineering and legal principles. They were developed to meet pressing current needs, and served that purpose very well. However, perhaps due to the early need to get “something” working even if it was not comprehensive, many of the earlier approaches are no longer effective. Common criticisms are that early tools for gathering and analyzing data fail to scale up to the performance needed for very large enterprises or when high bandwidth is involved; that the use of the tools are burdensome from a societal and from a technological perspective, and can be ineffective, especially when it comes to newer or highly distributed tasks. In response, the SADFE community was formed, to identify systematic approaches that would yield effective solutions meeting future needs as well as current ones. Therefore, this and previous SADFE meetings have identified and focused on four critical areas where advances are needed:

- **Digital Evidence Management**: advanced digital evidence discovery, collection, and storage.
- **Principle-based Digital Forensic Processes**: systematic engineering processes supporting digital evidence management which are sound on both technical and legal grounds.
- **Digital Evidence Analytics**: Advanced digital evidence analysis, correlation, and presentation.
- **Forensic Support Technologies**: forensic-enabled and proactive monitoring/response.
### Figure 1 Challenges in Systematic Approaches to Digital Forensics

**Digital Evidence Management**: *advanced digital evidence discovery, collection, and storage*
- Identification and collection of digital evidence
- Post-collection handling of evidence
- Evidence preservation and storage
- Forensic-enabled architectures and processes
- Managing geographically, politically and/or jurisdictionally dispersed data

**Principle-based Digital Forensic Processes**: *systematic engineering processes supporting digital evidence management which are sound on both technical and legal grounds*
- Legal and 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

**Digital Evidence Analytics**: *advanced digital evidence analysis, correlation, and presentation*
*Advanced search, analysis, and presentation of digital evidence*
- Progressive cyber crime scenario analysis and reconstruction technology
- Legal case construction & digital evidence support
- Cyber-crime strategy analysis & modeling
- Combining digital and non-digital evidence
- Supporting qualitative or statistical evidence

**Forensic-support technologies**: *forensic-enabled and proactive monitoring/response*
*Forensics of embedded or non-traditional devices (e.g. digicams, cell phones, SCADA)*
- Innovative forensic engineering tools and applications
- Forensic-enabled support for incident response
- Forensic tool validation: methodologies and principles
- Legal and technical collaboration
- Digital Forensics Surveillance Technology and Procedures
4. Setting the focus of SADFE 2007

Our SADFE07 call for papers in the areas outlined yielded interesting results in several areas related to the challenges, particularly the use of models in forensics, gathering and understanding of digital forensic data, Forensic Analysis Tools, and Education/Training.

An area of particular importance to this year’s presenters involves the development and utilization of forensic models. In their paper *Towards Models for Forensic Analysis*, Peisert, Bishop, Karin and Marzullo discuss the need for a rigorous model of forensics. Andrew, in *Defining a Process Model for Forensic Analysis of Digital Devices and Storage Media*, addresses the importance of accuracy and provides a process model for the analysis phase of the digital forensic process. Cardenas and Herreras, in *A Log Correlation Model to Support the Evidence Search Process in a Forensic Investigation*, provide a model comprised of a set of agents that can collect, filter, normalize and correlate events coming from a broad range of log files, with the purpose of supporting an analyst engaged in evidence search. Finally, the workshop includes an invited paper from Pollitt, *An Ad Hoc Review of Digital Forensic Models*, in which he reviews a broad collection of diverse approaches illustrating the development of digital forensic models.

Another area that drew attention was the phase of gathering and understanding digital forensic data. With respect to gathering data, an especially difficult issue involves identification of data types embedded within a file. Erbacher and Mulholland received SADFE’s best paper award for their approach to this issue with *Identification and Localization of Data Types within Large-Scale File Systems*. In *The Rules of Time on NTFS File System*, Chow, Frank, Kwan and Lai advance an approach utilizing temporal analysis to support reconstruction of events or crimes. Finally, in *Data Hiding in SIM/USIM Cards: A Steganographic Approach*, Savoldi analyzes a SIM/USIM card file system, focusing primarily on what can be detected using existing tools, and newer methods that extend data collection to concealed parts of the file system. This section concludes with a panel discussion moderated by Losavio. This panel -- *Lawyers, Judges and Digital Forensics: Evaluating Situational Awareness and Evidentiary Skills with Electronic Evidence* -- gets at the new skills that are needed if lawyers and judges are to work effectively with the new media. In a similar vein, Attfield presents a panel on the *Courtroom Implications of Presenting Digital Evidence*.

On day two of the workshop, we begin by considering Forensic Analysis Tools, and whether they are performing as they should. Our first paper in this session, *X-Online: An Online Interface for Digital Decryption Tools*, is written by Aggarwal, Beech, Das, de Medeiros, and Thompson. X-Online is a Web application designed to interface with a password-recovery and/or decryption tools such as AccessData’s Distributed Network Attack (DNA™), and is an example of the kind of web-service based e-Forensic tools that the authors believe will become increasing common. Another paper in this category is written by Pan and Batten: *A Lower Bound on Effective Performance Testing for Digital Forensic Tools*. The authors observe that the “increasing complexity and number of digital forensic tasks required in criminal investigations demands the development of an effective and efficient testing methodology, enabling tools of similar functionalities to be compared based on their performance”, and provide support for identifying how many test cases might be needed. Finally, in *Establishing Tap Reliability in Expert Witness Testimony: Using Scenarios to Identify Calibration Needs*, Endicott-Popovsky, Fluckiger, and Frincke consider several scenarios involving a forensic tap, using their model for calibration development to illustrate how a calibration regime might be developed in each.

Our next session includes two challenge papers, or papers emphasizing challenges for the forensic community, intended to foster discussion. The first challenge, led by Losavio, involves *Construction of an Adequate Digital Forensics Testbed*. The second challenge, led by Erbacher, addresses issues in the *Validation of Forensic Tools and Approaches*.

Finally, a short session on Education and Training is represented by a paper from Taylor, Endicott-Popovsky, and Phillips. Their article, *Forensics Education: Assessment and Measures of Excellence*, seeks to define quality attributes for forensic programs. Included in this session is also
a panel led by Losavio, where a broad cross-section of the academic and practitioner communities discuss *Education and Interdisciplinary Issues in Digital Forensics, Computer Science and Judicial Process*.

5. What lies ahead?

We do not anticipate that the challenges raised in SADFE 2007 or other forensic forums will become any easier with time. The complexity and scope of cyber crimes and cyber-enabled crimes is increasing, and the objectives of the cyber-criminal are broad. While the cyber equivalent of breaking and entering may be the public perception of cyber criminal activity, more subtle and better organized crimes such as click-fraud, DDoS based extortion; illegal intercept and identity theft are all far more damaging than a typical web site defacement or compromise. These cyber crimes originate from multiple hosts involving multiple countries and may combine multiple crimes against multiple targets in a single act.

As well as having technological challenges, digital forensic evidence has a human side. Legal and technical teams must work together, and the result of their efforts normally will be presented to non-specialists who render a decision within the societal framework of a court of law. Regulatory and societal issues, from corporate to local through national to international, often drive the forensic process and the use of forensic results as much as technological issues. None of this is easy. Societal give-and-take as well as technological research is needed if the practice of digital forensics is to catch up with the requirements about to be placed upon it. It is our hope that communities such as SADFE will continue as a useful way to support interactions between all stakeholders, and in that way, support systematic approaches that suit both society and technology.

It has been a pleasure to work with the program committee and the authors in preparing for this meeting – and now we welcome you, the attendees, to SADFE 2007!