Challenge Paper: Validation of Forensic Techniques for Criminal Prosecution

Robert F. Erbacher, *Member, IEEE*
Department of Computer Science, UMC 4205
Utah State University
Logan, UT 84322
Robert.Erbacher@usu.edu

Barbara Endicott-Popovsky,
Student Member, IEEE
University of Washington
Seattle, WA 98195-2840
endicott@u.washington.edu

Deborah A. Frincke,
Senior Member, IEEE
Pacific Northwest National Laboratory
Richland, WA 99352
deborah.frincke@pnl.gov

1. Introduction

As in many domains, there is increasing agreement in the user and research community that digital forensics analysts would benefit from the extension, development and application of advanced techniques in performing large scale and heterogeneous data analysis. Modern digital forensics analysis of cyber-crimes and cyber-enabled crimes often requires scrutiny of massive amounts of data. For example, a case involving network compromise across multiple enterprises might require forensic analysis of numerous sets of network logs and computer hard drives, potentially involving 100's of gigabytes of heterogeneous data, or even terabytes or petabytes of data. Also, the goal for forensic analysis is to not only determine whether the illicit activity being considered is taking place, but also to identify the source of the activity and the full extent of the compromise or impact on the local network. Even after this analysis, there remains the challenge of using the results in subsequent criminal and civil processes.

Given this enormous volume of data, new tools and techniques are needed in order to analyze and resolve this data in the form of a forensic analysis. Currently, much digital data goes completely unanalyzed due to the time requirements imposed by their analysis. Thus, many researchers are exploring novel techniques for the analysis of digital data to more efficiently and effectively understand the extent of cyber-crimes and cyber-enabled crimes. In addition to the analysis of the digital data itself, there is an equally pressing issue as to whether or not the techniques being developed are incorporating the capabilities needed for the application to criminal and civil processes. For instance, is the analysis process reproducible, demonstrable, and validatable? Is the analysis process following accepted forensic analysis requirements? When presented in court, will opposing council be able to successfully attack the credibility of the presented material, and the foundation for the evidence's construction, or will these materials pass muster of acceptability?

To achieve the full benefit of forensic analysis, then, the consideration of legal consequences must be tightly integrated with the process of designing and evaluating developed forensic techniques and the networks themselves. This derives from the work by Erbacher et al. [1] in which a proposed digital forensic process was presented, as well as work by Popovsky et al [2][3], proposing network forensic readiness and device calibration. In essence, development of forensic techniques are already designed, evaluated, and refined through an iterative process. Combining [1] and [2] we propose that evaluation of legal admissibility be incorporated at each

stage of this process and examined to incorporate needed capabilities in order to ensure legal admissibility and validity. This proposed process is much akin to the process of designing visualization techniques in which user evaluation must be considered at each stage in the development of the visualization techniques in order to ensure they are effective, meet the needs of the users, and are perceptually viable.

Part of the challenge: The full range of issues needing to be resolved for such forensic validation must be identified. An example of unresolved problems is in the acquisition of data related to network intrusions. While the system actually compromised can be forensically duplicated and analyzed, what of the other systems on the network, especially on the same subnet as the compromised system. Such systems may have valuable forensic information in their system logs. Must an organization remove from service *all* systems that *may* have relevant data or can a mechanism be developed that will create forensically valid repositories of system log data. This can be considered as a modification to the typical system log reporting facility which many organizations already use to collate system logs on a central repository. How can this system be made to be forensically valid for legal admissibility?

2. Conclusions

With the growing interest in developing techniques specifically geared towards digital forensic analysis we must begin considering requirements for legal admissibility in the design and development of these techniques. Doing so now will ensure that techniques and capabilities developed by the forensic research community have wide applicability validity.

3. References

1. Robert F. Erbacher, Kim Christensen, and Amanda Sundberg, "Visual Forensic Techniques and Processes," *Proceedings of the 9th Annual NYS Cyber Security Conference Symposium on Information Assurance*, Albany, NY, June 2006, pp. 72-80.
2. Popovsky, B. and D. Frincke. Network Device Calibration for Establishing Foundation for Expert Testimony, accepted for inclusioni in S. Shenoi, .Ed, book proceedings for 3rd Annual IFIP WG 1.9 International Conference, to appear 2007.
3. Popovsky, B. and D. Frincke. Embedding Forensic Capabilities into Networks: Addressing Inefficiencies in Digital Forensics Investigations, 7th Annual IEEE Information Assurance Workshop, West Point, June 2006