

ISS Summer Research Award Final Report

A Comprehensive Survey on the Status of Digital Forensics and Its Preparedness against Anti-Terrorism

November 30, 2007

Principal Investigator: Ju-Yeon Jo, PhD
Assistant Professor
School of Informatics
University of Nevada, Las Vegas 89154 - 4054

ABSTRACT

Digital forensics is an essential field in combating crimes and terrorism. This report presents the collective viewpoint of the digital forensics investigators and researchers on its current status. It is intended to provide the investigators an overview on the training requirements, certifications, nature of the cases, relation to terrorism, and challenging issues so that they can better utilize the valuable investigation resources. This is the most comprehensive study conducted so far in digital forensics in terms of the scope. The survey was comprehensive consisting of over 50 questions and requiring about 25 minutes to complete. 106 contact points were collected mostly from the US while 10% was from other countries. They were personally invited to the survey via e-mail and 24 people responded, achieving a 22.6% response rate. The invitation email for the survey was sent out in September 2007 and again in November 2007 to those who didn't respond to the first invitation. No more survey instruments were distributed due to zero responses from the second one. The respondents' average experience in the digital forensics field ranged from 10 to 15 years and many of them held advanced degrees or certificates. Although the results may not have had a statistical significance due to the petite sample size, it still offers valuable insights through the collective opinion of the active practitioners in this field.

The ultimate questions we wished to answer through this survey were "How well are we prepared for digital forensics needs, what are the challenges, and what improvements should we make?" Supplementing that, we were interested in: 1) Are there enough number of trained investigators? What training is needed to produce them and how do we evaluate them? 2) What is the nature of investigation cases in terms of target systems, OS, applications, and encryptions? 3) What investigation tools are available and used favorably? 4) How complex are the cases in terms of difficulty, number of hours required and foreign language requirement? and 5) Are we well prepared to handle homeland security cases? To elicit the opinions on those questions, the survey contained several sections, some requiring technical information and some asking questions related to homeland security.

Overall, the results indicate that the digital forensics industry as a whole in the United States is hardly prepared for the current digital forensics' needs. The greatest challenge is the lack of the workforce. We are clearly in shortage of investigators in the civilian sector, and the workload in homeland security area is growing, too. The job demand is increasing, but finding the right people is difficult. It is agreed that the greatest strength of an investigator is the on-the-job experience, not a university degree or a certificate. But it takes several years of experience to be a proficient investigator. This gives universities a unique opportunity. With more realistic projects, state-of-the-art techniques, and interactions with active practitioners, universities can shorten the length of training greatly and advance the students to more complex cases. Some of the areas in this study are not conclusive and we suggested several areas for further investigation. The preliminary results presented in this report should serve as a roadmap for those future studies.