

From the Editors

When we started this endeavor, we believed that there was a need for a niche journal in the emerging field of digital forensics. However, we grossly underestimated the interest and needs of the digital forensics community. The latest statistics indicate that we have reached 125 countries and have had over 177,000 downloads since the journal was launched in spring 2002. We thank you for your interest and support.

Because of the increase in submissions, we have decided to include five articles in this issue. The articles are demonstrative of our continued efforts to introduce innovative concepts which we hope will provoke further discussion, encourage additional research, and help advance digital forensics methods.

The Gao, Richard, and Rousev article, *Bluepipe: A Scalable Architecture for On-the-Spot Digital Forensics*, argues for the need for on-the-spot digital forensics tools that supplement lab methods. The authors discuss the specific user and software engineering requirements for such tools, present their *Bluepipe* architecture and the *Bluepipe* remote forensics protocol, and discuss some of the details of their ongoing prototype implementation.

The Abouzakhar and Manson article, *Evaluation of Intelligent Intrusion Detection Models*, discusses an evaluation methodology that can be used to assess the performance of intelligent techniques designed to detect, as well as predict, unauthorized activities in networks.

Stephenson in his article, *The Application of Formal Methods to Root Cause Analysis of Digital Incidents*, presents the need for a structured and formal approach to root cause analysis following the recovery from such incidents. In light of regulations and standards mandates, the author proposes a methodology based upon formal modeling of the security processes in an enterprise under attack.

In *Process Forensics: A Pilot Study on the Use of Checkpointing Technology in Computer Forensics*, Foster and Wilson introduce a new area of computer forensics, process forensics. The authors define process forensics as the extracting of information "from a process's address space for the purpose of finding digital evidence pertaining to a computer crime." They make the case that an accurate and reliable checkpointing tool could create a new source of evidence for the forensic investigator.

The Ó Ciardhuáin article, *An Extended Model of Cybercrime Investigations*, proposes a comprehensive model of cybercrime investigations which incorporates and extends existing models to address certain activities not included in them. The model focuses on the information flows in an investigation, thus capturing the full scope of an investigation, rather than only the processing

of evidence. The evaluation of the model by practicing cybercrime investigators is presented, as well as an application to a real investigation.

The IJDE editors would like to thank the DFRWS (<http://www.dfrws.org/>), Digital Forensics Research Workshop, for its continued efforts to advance the field and for hosting its annual conference. Some of the papers for this issue and the next were submitted or presented at the August 2004 Baltimore conference.

In February 2004, a second journal in the field, *Digital Investigation*, was launched (<http://www.compseconline.com/digitalinvestigation/>). We welcome the journal as another resource for the digital forensics community. We have met with Eoghan Casey, Editor-in-Chief, to discuss ways that the two journals can complement each other.

We are actively soliciting articles for future issues. To be considered for the Fall issue, articles must be submitted by November 1, 2004 to provide time for the peer review process.

Gary R. Gordon, Editor
Utica College

John J. Leeson, Editor
University of Central Florida