

# **2009 Fifth International Conference on IT Security Incident Management and IT Forensics**

**(IMF 2009)**

**Stuttgart, Germany  
15-17 September 2009**



**IEEE Catalog Number: CFP0917I-PRT  
ISBN: 978-1-4244-5168-5**

# Table of Contents

## 2009 Fifth International Conference on IT Security Incident Management and IT Forensics

IMF 2009

### Workshops

Digital Discovery with Bootable CDs

Ralf Moll, *Federal Police Baden-Wuerttemberg, Germany,*

Michael Prokop, *grml Solutions, Austria,* Holger Morgenstern, *gutachten.info, Germany*

### Keynotes

Thilo Weichert

Privacy Commissioner of Schleswig-Holstein, Germany

Independent Centre for Privacy Protection Schleswig-Holstein, Germany

Overcast: Forensic Discovery in Cloud Environments..... 3  
Stephen D. Wolthusen, Royal Holloway, University of London, UK

### Presentations

Experiences with the NoAH HoneyNet Testbed to Detect new Internet Worms..... 13  
*Jan Kohlrausch*

Botnet Statistical Analysis Tool for Limited Resource Computer Emergency Response Team..... 27  
*Kamol Kaemarungsi, Nawattapon Yoskamtorn, Kitisak Jirawannakool, Nuttapong Sanglerdsinlapachai, and Chanin Luangingkasut*

Semi-autonomous Link Layer Vulnerability Discovery and Mitigation Dissemination ..... 41  
*Ziyad Al-Salloum and Stephen Wolthusen*

From the Computer Incident Taxonomy to a Computer Forensic Examination Taxonomy..... 54  
*Robert Altschaffel, Stefan Kiltz, and Jana Dittmann*

Fast User Classifying to Establish Forensic Analysis Priorities .....	69
<i>Antonio Grillo, Alessandro Lentini, Gianluigi Me, and Matteo Ottoni</i>	
The Forensic Image Generator Generator (Forensig2) .....	78
<i>Christian Moch and Felix C. Freiling</i>	
Safe-Keeping Digital Evidence with Secure Logging Protocols: State of the Art and Challenges .....	94
<i>Rafael Accorsi</i>	
Technique to Interrogate an Image of RAM111 .....	111
<i>Mark Wozar</i>	
An Automated User Transparent Approach to log Web URLs for Forensic Analysis .....	120
<i>Muhammad Kamran Ahmed, Mukhtar Hussain, and Asad Raza</i>	
Self-Forensics through Case Studies of Small-to-Medium Software Systems .....	128
<i>Serguei A. Mokhov and Emil Vassev</i>	
Analysis of Download Accelerator Plus (DAP) for Forensic Artefacts .....	142
<i>Muhammad Yasin, Muhammad Arif Wahla, and Firdous Kausar</i>	
A Comprehensive and Comparative Analysis of the Patching Behavior of Open Source and Closed Source Software Vendors .....	153
<i>Guido Schryen</i>	

## **Author Index**