2011 Sixth International Conference on IT Security Incident Management and IT Forensics

(IMF 2011)

Stuttgart, Germany
10 – 12 May 2011

IEEE Catalog Number: CFP1117I-PRT
ISBN: 978-1-4577-0146-7

6th International Conference on IT Security Incident Management and IT Forensics

IMF 2011

Table of Contents

Preface......vii

Committees......viii

Reviewers......x

Keynotes......xi

Workshops......xii

Sponsors......xiii

Technical Papers

Towards Forensic Data Flow Analysis of Business Process Logs 3
Rafael Accorsi, Claus Wonnemann, and Thomas Stocker

Security Aspects of Piecewise Hashing in Computer Forensics 21
Harald Baier and Frank Breitinger

Computational Documentation of IT Incidents as Support for Forensic Operations 37
Sebastian Kurowski and Sandra Frings

Forensics Investigations of Multimedia Data: A Review of the State-of-the-Art 48
Rainer Poisel and Simon Tjoa

Design and Implementation of a Documentation Tool for Interactive Commandline Sessions 62
Andreas Dewald, Felix C. Freiling, and Tim Weber

Usability of Forensics Tools: A User Study 81
Hanan Hibshi, Timothy Vidas, and Lorrie Cranor

A Common Scheme for Evaluation of Forensic Software 92
Mario Hildebrandt, Stefan Kiltz, and Jana Dittmann

Integrated Security Incident Management — Concepts and Real-World Experiences 107
Stefan Metzger, Wolfgang Hommel, and Helmut Reiser

Towards a Rapid-Alert System for Security Incidents 122
Stefan Rass

Automated Audit of Compliance and Security Controls 137
Gerhard Koschorreck

Use of Machine Learning Classification Techniques to Detect Atypical
Behavior in Medical Applications 149
Terrence Ziemniak

Author Index 163