

2013 Seventh International Conference on IT Security Incident Management and IT Forensics

(IMF 2013)

**Nuremberg, Germany
12 – 14 March 2013**



**IEEE Catalog Number: CFP1317I-POD
ISBN: 978-1-4673-6307-5**

2013 Seventh International Conference on IT Security Incident Management and IT Forensics

IMF 2013

Table of Contents

Preface.....	vii
Organizing Committee.....	ix
Program Committee.....	x
Reviewers	xi
Keynotes	xii
Workshops.....	xiii
Sponsors.....	xv

Technical Papers

Forewarned is Forearmed: Indicators for Evaluating Information Security Incident Management	3
<i>Karin Bernsmed and Inger Anne Tøndel</i>	
Identifying a Shared Mental Model Among Incident Responders	15
<i>Robert Floodeen, John Haller, and Brett Tjaden</i>	
A Case Study: Preparing for the Smart Grids - Identifying Current Practice for Information Security Incident Management in the Power Industry	26
<i>Maria B. Line</i>	
mvHash-B - A New Approach for Similarity Preserving Hashing	33
<i>Frank Breitingner, Knut Petter Astebøl, Harald Baier, and Christoph Busch</i>	
Selective Imaging Revisited	45
<i>Johannes Stüttgen, Andreas Dewald, and Felix C. Freiling</i>	
Developing a Cloud Computing Based Approach for Forensic Analysis Using OCR	59
<i>Matthias Trojahn, Lei Pan, and Fabian Schmidt</i>	

On Bayesian Trust and Risk Forecasting for Compound Systems	69
<i>Stefan Rass and Sebastian Kurowski</i>	
Anti-forensics: The Next Step in Digital Forensics Tool Testing	83
<i>Martin Wundram, Felix C. Freiling, and Christian Moch</i>	
Forensic Application-Fingerprinting Based on File System Metadata	98
<i>Sven Kälber, Andreas Dewald, and Felix C. Freiling</i>	
Statistical Pattern Recognition Based Content Analysis on Encrypted Network: Traffic for the TeamViewer Application	113
<i>Robert Altschaffel, Robert Clausing, Christian Kraetzer, Tobias Hoppe, Stefan Kiltz, and Jana Dittmann</i>	
Visualizing Indicators of Rootkit Infections in Memory Forensics	122
<i>Stefan Vömel and Hermann Lenz</i>	
Author Index	140