

2018 11th International Conference on IT Security Incident Management & IT Forensics (IMF 2018)

**Hamburg, Germany
7-9 May 2018**



**IEEE Catalog Number: CFP1817I-POD
ISBN: 978-1-5386-6633-3**

**Copyright © 2018 by the Institute of Electrical and Electronics Engineers, Inc.
All Rights Reserved**

Copyright and Reprint Permissions: Abstracting is permitted with credit to the source. Libraries are permitted to photocopy beyond the limit of U.S. copyright law for private use of patrons those articles in this volume that carry a code at the bottom of the first page, provided the per-copy fee indicated in the code is paid through Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923.

For other copying, reprint or republication permission, write to IEEE Copyrights Manager, IEEE Service Center, 445 Hoes Lane, Piscataway, NJ 08854. All rights reserved.

****** This is a print representation of what appears in the IEEE Digital Library. Some format issues inherent in the e-media version may also appear in this print version.***

IEEE Catalog Number:	CFP1817I-POD
ISBN (Print-On-Demand):	978-1-5386-6633-3
ISBN (Online):	978-1-5386-6632-6

Additional Copies of This Publication Are Available From:

Curran Associates, Inc
57 Morehouse Lane
Red Hook, NY 12571 USA
Phone: (845) 758-0400
Fax: (845) 758-2633
E-mail: curran@proceedings.com
Web: www.proceedings.com

CURRAN ASSOCIATES INC.
proceedings
.com

2018 11th International Conference on IT Security Incident Management & IT Forensics **IMF 2018**

Table of Contents

Preface .vii.....	
Conference Organization .viii.....	
Acknowledgements .x.....	

IMF 2018 Papers

On the Robustness of Random Walk Algorithms for the Detection of Unstructured P2P Botnets .3.....	
<i>Dominik Muhs (Technische Universität Dresden), Steffen Haas (Universität Hamburg), Thorsten Strufe (Technische Universität Dresden), and Mathias Fischer (Universität Hamburg)</i>	
Exploring the Processing of Personal Data in Modern Vehicles - A Proposal of a Testbed for Explorative Research to Achieve Transparency for Privacy and Security .15.....	
<i>Alexandra Koch (Otto-von-Guericke University of Magdeburg), Robert Altschaffel (Otto-von-Guericke University of Magdeburg), Stefan Kiltz (Otto-von-Guericke University of Magdeburg), Mario Hildebrandt (Otto-von-Guericke University of Magdeburg), and Jana Dittmann (Otto-von-Guericke University of Magdeburg)</i>	
Linux Memory Forensics: Expanding Rekall for Userland Investigation .27.....	
<i>Johannes Stadlinger (Friedrich-Alexander University Erlangen-Nürnberg), Andreas Dewald (ERNW Research GmbH, Friedrich-Alexander University Erlangen-Nürnberg), and Frank Block (ERNW GmbH, Friedrich-Alexander University Erlangen-Nürnberg)</i>	
mrsh-mem: Approximate Matching on Raw Memory Dumps .47.....	
<i>Lorenz Liebler (University of Applied Sciences Darmstadt, Germany) and Frank Breitingner (University of New Haven, USA)</i>	
Principles of Secure Logging for Safekeeping Digital Evidence .65.....	
<i>Felix Freiling (Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU)) and Edita Bajramovic (Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU) / Framatome GmbH)</i>	
Defeating the Secrets of OTP Apps .76.....	
<i>Philip Polleit (Friedrich-Alexander-Universität Erlangen-Nürnberg) and Michael Spreitzenbarth (Friedrich-Alexander-Universität Erlangen-Nürnberg)</i>	

Introducing Anti-Forensics to SQLite Corpora and Tool Testing .89.....	
<i>Sven Schmitt (Friedrich-Alexander-University Erlangen-Nuremberg (FAU), Germany)</i>	
Complexities in Investigating Cases of Social Engineering: How Reverse Engineering and Profiling can Assist in the Collection of Evidence .107.....	
<i>Christina Lekati (Cyber Risk GmbH)</i>	
Swimming in the Monero pools .110.....	
<i>Emilien Le Jamtel (CERT-EU)</i>	
The -Time-to-Compromise Metric for Practical Cyber Security Risk Estimation .115.....	
<i>Andrej Zieger (HAW Hamburg), Felix Freiling (FAU Erlangen-Nürnberg), and Klaus-Peter Kossakowski (HAW Hamburg)</i>	
Author Index 135.	