Report from Dagstuhl Seminar 11401

Forensic Computing

Edited by

Felix C. Freiling[1], Dirk Heckmann[2], Radim Polcák[3], and Joachim Posegga[4]

1 **University of Erlangen-Nuremberg, DE,** `felix.freiling@cs.fau.de`
2 **University of Passau, DE,** `heckmann@uni-passau.de`
3 **Masaryk University, CZ,** `radim.polcak@law.muni.cz`
4 **University of Passau, DE,** `posegga@uni-passau.de`

Abstract

Forensic computing (sometimes also called *digital forensics*, *computer forensics* or *IT forensics*) is a branch of forensic science pertaining to digital evidence, i.e., any legal evidence that is processed by digital computer systems or stored on digital storage media. Forensic computing is a new discipline evolving within the intersection of several established research areas such as computer science, computer engineering and law.

Forensic computing is rapidly gaining importance since the amount of crime involving digital systems is steadily increasing. Furthermore, the area is still underdeveloped and poses many technical and legal challenges.

This Dagstuhl seminar brought together researchers and practitioners from computer science and law covering the diverse areas of forensic computing. The goal of the seminar was to further establish forensic computing as a scientific research discipline, to identify the strengths and weaknesses of the research field, and to discuss the foundations of its methodology.

The seminar was jointly organized by Prof. Dr. Felix Freiling (Friedrich-Alexander University Erlangen-Nuremberg, Germany), Prof. Dr. Dirk Heckmann (University of Passau, Germany), Prof. Dr. Radim Polčàk (Masaryk University, Czech Republic), Prof. Dr. Joachim Posegga (University of Passau, Germany), and Dr. Roland Vogl (Stanford University, USA). It was attended by 27 participants.

Seminar 03.–07. October, 2011 – www.dagstuhl.de/11401
1998 ACM Subject Classification K.4.1 [Computers and Society] Public Policy Issues
Keywords and phrases forensic teaching, practical experience in forensics and law, selective imaging, mobile phone forensics, cryptographic hash functions
Digital Object Identifier 10.4230/DagRep.1.10.1
Edited in cooperation with Michael Spreitzenbarth

1 Executive Summary

Felix C. Freiling
Dirk Heckmann
Radim Polcák
Joachim Posegga

After a brief introduction by the organizers, the seminar started off with a sequence of 3 slide/5 minute talks by all participants stating their research interests, their background and their expectations towards the seminar. In the afternoon, two introductory talks by

Forensic Computing, *Dagstuhl Reports*, Vol. 1, Issue 10, pp. 1–13
Editors: Felix C. Freiling, Dirk Heckmann, Radim Polcák, and Joachim Posegga
DAGSTUHL REPORTS Dagstuhl Reports
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Dieter Gollmann ("Access control — principles and principals") and Stig Mjolsnes ("ICT and forensic science") paved the way for a common understanding of the open questions in the area and the relation of forensic computing to computer security.

Wednesday morning commenced with a first introductory law talk by Focke Höhne ("Introduction to German IT Forensics Law"). It was followed by two insightful technical talks from presenters who had considerable practical experience in the area: Glenn Dardick and Kwok Lam.

The afternoon was spent on a pleasant hike to a nearby village where the Dagstuhl office had organized delicious traditional coffee and cake. On the way back to Schloss Dagstuhl a group of adventurers separated from the main party to explore the woods around Wadern. They only managed to return to Dagstuhl in time because of modern navigation technology (paper maps provided by the Dagstuhl office). Reasons for the failure of more traditional technology (iPhones, etc.) were discussed in the evening in the wine cellar.

Thursday saw a mix of legal and technical talks: Herbert Neumann raised many questions during his presentation of practical (law) case studies while Viola Schmid presented a proposal for a "Casebook on Cyber Forensics". Harald Baier discussed the deficits of forensic hash functions and Felix Freiling shared some of his experiences from teaching digital forensics. After lunch Michael Spreitzenbarth presented an overview over mobile phone forensics while Radim Polčàk gave some background on the issues of data retention relevant in different countries. Joshua James pointed out the necessity to overcome the traditional separation of sciences and encouraged more interaction between computer science and law.

Finally, Johannes Stüttgen introduced the method of "Selective Imaging" to improve the digital evidence collection process.

Friday morning hosted a series of three talks from computer science, law and practice. Stefan Kiltz spoke about techniques to seize transient evidence in networks, Sven Schmitt gave an overview of digital forensics at the German federal police (BKA), and Nicolas von zur Mühlen sparked many discussions during his presentation on transborder searches.

Conclusion

Overall, the seminar was well-received by the participants. They particularly liked the interdisciplinary approach, which is documented by the results of the final Dagstuhl survey: Almost all participants stated that the seminar led to "insights from neighboring fields or communities" and that they made "new professional contacts like an invitation to give a talk or to join an existing project or network".

The organizers also identified room for improvement: Only about one-third of the participants came from law. This points to a fundamental problem for future seminars since — similar to participants from industry — it is rather untypical for academics in law or for international practicioners to spend an entire week at a seminar or workshop.

In possible future seminars, the set of relevant topics should been broadened to include legal aspects of IT forensics in enterprises. This would substantially enlarge the set of interested international academics and further nourish community building which is currently vital to the field.

2 Table of Contents

Executive Summary

Overview of Talks

3 Overview of Talks

3.1 Deficiencies of (Cryptographic) Hash Functions in Digital Forensics

Harald Baier (University of Applied Science Darmstadt, DE)

Joint work of Baier, Harald; Breitinger, Frank
Main reference Harald Baier, Frank Breitinger, "Security Aspects of Piecewise Hashing in Computer Forensics," Proc. 6th Int'l Conf. on IT Security Incident Management & IT Forensics (IMF 2011), IEEE CS, pp. 21–36, 2011.
URL https://www.fbi.h-da.de/fileadmin/gruppen/FG-IT-Sicherheit/Publikationen/2011/2011_05_Baier_IMF2011.pdf

Hash functions are well-known methods in computer science to map arbitrary large input to bit strings of a fixed length that serve as unique input identifier/fingerprints. A key property of cryptographic hash functions is that even if only one bit of the input is changed the output behaves pseudo randomly and therefore similar files cannot be identified.

However, in the area of computer forensics it is also necessary to find similar files (e.g. different versions of a file), wherefore we need a similarity preserving hash function also called fuzzy hash function. In this talk we present use cases of cryptographic hash functions and discuss their drawbacks.

We come up with proposed approaches for fuzzy hashing and discuss the next steps.

3.2 Cyber Forensics Assurance Model

Glenn S. Dardick (Longwood University – Virginia, US)

Main reference Based on Model Previously presented in December 2010 at SECAU Conference

As the usage of Cyber Forensics increases, so does the potential for errors in the practice of applying Cyber Forensic. Errors in opinions derived from faulty practices have resulted in grievous miscarriages of justice. However, utilizing the foundations of Information Systems Assurance and Information Quality, a solid foundation for improving the quality and effectiveness of Cyber Forensics can be derived. The foundations of Information Systems Assurance and information Quality provide a solid foundation for improving the current efforts in Cyber Forensics. With increasing computer and network systems usage as well as the increasing frequency of attacks on information systems, the need for controlling risks in information systems have become more apparent. Meeting that need, Information Systems Assurance has continued to evolve: from the CIA (confidentiality, integrity, and availability) into variations such as the five pillars (confidentiality, integrity, availability, authenticity, and non-repudiation) and the Parkerian Hexad (confidentiality, integrity, availability, authenticity, possession, and utility). Also, with the continuing growth of information systems, the need for improving the quality of such systems has also evolved focusing on various components of information Quality (accuracy, relevance, consistency, timeliness and completeness).

Utilizing the foundations of Information Systems Assurance and information Quality a model has been derived for Cyber Forensics Assurance. However, there is still a need to increase the level of training among digital forensics experts in order to attain the assurance needed as defined by the Cyber Forensics Assurance Model.

3.3 Experiences from teaching forensic computing

Felix C. Freiling (Universität Erlangen, DE)

In the summer of 2004, I gave the first lecture on forensic computing to University students in Germany together with Maximillian Dornseif. Since then, the field of IT forensics has changed dramatically and many more Universities have started to teach the subject. This talk reviews the current European teaching landscape in IT forensics and relates past and future developments in the field to my own teaching experiences. Furthermore, the design of the first German Master degree programme in digital forensics is discussed.

3.4 Access Control – Principles & Principals

Dieter Gollmann (TU Hamburg-Harburg, DE)

The concepts and terminology for access control were developed in the 1970s and 1980s in the context of closed organizations. In the context it was natural that principals (active entities) security policies referred to were closely related to human users, as is evident from the research literature of that time. By the same measure, there was a close link between access control and accountability.

This paradigm is still highly influential on the perception of access control but it is a poor match for today‘s situation in Web 2.0 applications. In a world of services, the services become principals; principals have to be named and have to be "authenticated" when issuing access requests. For names, the convention of using host names from the Domain Name System (DNS) has been adopted. However, DNS was not designed as a system supporting access control; in particular, there are no inherent mechanisms that stop authoritative name servers from lying about name/IP address bindings. For authentication, traditional PKI-based solutions do no exist, probably will never exist on a global scale, and are arguably not necessary in the first place. Alternatives are "recognizing the same service as before" (P. Nikander: identification) or distinguishing own requests/scripts from requests/scripts forwarded on behalf of others.

In summary, principals are associated with services, not with persons, authentication (determining origin) may be replaced by different notions, and the close link between access control and accountability no longer exists.

3.5 A transparent bridge for forensic sound network traffic data acquisition

Stefan Kiltz (University of Magdeburg, DE)

Joint work of Kiltz, Stefan; Hildebrandt, Mario; Hoppe, Tobias; Dittmann, Jana
Main reference Stefan Kiltz, Mario Hildebrandt, Jana Dittmann, "A transparent bridge for forensic sound network traffic data acquisition," In Sicherheit 2010 – Sicherheit, Schutz und Zuverlässigkeit, 5. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.V. (GI) Berlin, 5–7 Oktober 2010. S. 93.

In this paper we introduce a prototype that is designed to produce forensic sound network data recordings using inexpensive hard- and software, the Linux Forensic Transparent Bridge (LFTB). It supports the investigation of the network communication parameters and the investigation of the payload of network data. The basis for the LFTB is a self-developed model of the forensic process which also addresses forensically relevant data types and considerations for the design of forensic software using software engineering techniques. LFTB gathers forensic evidence to support cases such as malfunctioning hard- and software and for investigating malicious activity. In the latter application the stealthy design of the proposed device is beneficial. Experiments as part of a first evaluation show its usability in a support case and a malicious activity scenario.

Effects to latency and throughput were tested and limitations for packet recording analyzed. A live monitoring scheme warning about potential packet loss endangering evidence has been implemented.

3.6 Forensic Computing: Objectives and Challenges

Kwok Lam (National University of Singapore, SG)

In this talk, we discuss the relationship of computing and forensics, and the role of computing in forensics. The objectives and challenges of forensic computing are also discussed. Specifically, the nature of digital evidences, where and how digital evidences may be collected for supporting forensic works in different types of scenario in which digital evidences are of crucial legal implications. We'll identify areas where computing techniques may be applied to support forensic activities and propose approaches for future development of methodologies for forensic computing. We conclude by sketching a proposed collaborative model for legal and computing researchers to contribute to the development of forensic computing methodologies.

3.7 ICT and Forensic Science

Stig Frode Mjølsnes (NTNU – Trondheim, NO)

Main reference Stig F. Mjølsnes (ed.), "A Multidisciplinary Introduction to Information Security," Chapman and Hall/CRC, 2011.

The term forensic is derived from the latin *forum*, denoting the public square of roman cities (foremost Forum Romanum), where all public matters including of judicial nature took place.

The proceedings of disputes and public trials were conducted orally, and the actual evidence supporting the claims were physically and methodically presented to a judge positioned on a tribunal.

The judicial evidence could take the form of testimony of witnesses, physical objects, or documents.

Evidence means what is clearly there for all to see.

The roles of computers and networks at the crime scene can be one or more of the following:

- The direct target of intentional incidents (information security).
- Technical tools and accomplices for crime (cybercrime).
- Instruments assisting the incident investigation process (digital forensics).
- Passive sources of evidence, and witnesses providing technical testimonies (digital evidence).

An after-the-fact investigation of an incident seek answers to the questions of what happened, the true explanation of how it happened, and the attribution to who did what. The judicial verdict must be founded on inculpatory and exculpatory evidence in criminal law. The evidence must be relevant and intelligible in the context of the judicial inquiry. Many disciplines of science are employed in this process of technical evidence.

Digital components and systems can be passive sources of information, or even regarded as witnesses that can provide technical testimonies about events. These informational objects are called digital evidence.

The evidence authenticity, both the origin and the integrity, must be assured by proper chain-of-custody/provenance. The current practice of the use of one-way hash function for verifying the integrity cannot become acceptable without some sort of commitment protocol.

The problem of forensic/court presentation of digital evidence is hard.

Can digital evidence be presented directly, or is it only possible to present indirect documentation about the digital evidence? For instance, US Federal Rules of Evidence distinguishes between original and duplicate.

Pragmatically, a paper printout shown to reflect the data accurately is called an "original". This presupposition of original is not future proof, and new definitions suitable for digital evidence are needed.

The Daubert Test constitutes four criteria for an acceptable forensic theory or method. Currently, there does not exist any theory or method in digital forensics that will satisfy all four soundness criteria. Some of the current analysis methods are image/mirror copy, keyword search, file type search, hash values of known files, timeline analysis using timestamps. The software tools and ad-hoc techniques developed for digital evidence extraction are often very specific to a device or software.

Any digital forensic detection tool will spur, with time, an anti-detection tool.

Are public or secret tools the best in practice? Remember that fingerprint analysis is used although gloves are easily available.

Finally, I list some promising research directions pertaining to digital forensics:

- Time line analysis using temporal logic for (partially) event ordering.
- Reverse engineering techniques of hardware, software, and systems.
- Bayesian causal graphs applied to digital evidence inferences assessing alternative hypotheses.
- Cryptanalysis models and methods from a forensic perspective.
- Shared cross-border investigation and aggregation of technical evidence from internet-based network infrastructures.

This Dagstuhl seminar presentation is based on Chapter 12 in the book *A Multidisciplinary Introduction to Information Security* [1].

References

1 Stig F. Mjølsnes (ed.) *A Multidisciplinary Introduction to Information Security*. Chapman and Hall/CRC, 2011. 348 pages. ISBN 978-1420085907

3.8 A small case of practical experience

Herbert Neumann (Anwaltskanzlei Neumann – Molfsee, DE)

The facts in catchwords: A 56 years old man, civil servant, married, two children (13 and 15) is accused of downloading and possessing child-pornographic photos. The police has searched through his home and confiscated the families entire it-equipment:

- father's PC and 3 laptops
- one external drive for backups
- 37 Original CD's and DVD's
- 9 blank CD's
- 2 photo- and one videocameras
- 29 video tapes
- the NTBA, splitter, DSL-modem and wifi-router

After nine months four child-pornographic photos were found on the PC named: *53896.jpg*, *89463.jpg*, *73346.jpg*, *1397.jpg*. But the defendant says: "I never did such a thing."

The background: The ISP had detected rapidly increasing traffic on 2 domains: *jh-desjn8.khbs23.de*, *jsbggg63.bgsvvr5c.de* hosted on his servers.

Content: 500 pornographic photos , 29 thereof clear child-pornographic. Prosecution was informed, the complete communication was monitored and stored.

Result: during one month over 300.000 accesses on the first server, over 92.000 accesses on the second.

Investigation: IP-address – customers name – suspects name. About 12.000 preliminary investigations by public prosecution. Distribution to the local responsible prosecution (i.e. Köln 500).

The prosecutors duty: to investigate not only the inculpatory facts but also the exculpatory ones. (Word-for-word written down in the German Code of Criminal Procedure Art. 160 Ch 2) The attorney has to be the most objective person in the world.

The most important rules of evidence in Criminal Law:

- In doubt in favor of the defendant
- The court has to prove the defendants guilt and not the defendant has to prove his innocence.

Procedure by the public prosecution according to how long the suspects looked at the pictures or downloaded some, the investigations were:

- adjusted instantly (dwell “a few” i.e. 45 seconds only thumbs) or continued (minutes or even downloaded photos)
- search warrants
- prosecution of the sever cases

The Experts duty: The expert is bound to furnish the opinion to the best of his knowledge i.e. to explain about conflicted opinions.

The Courts duty: to exclude all possibility of reasonable doubt otherwise to acquit.

Problem: what are reasonable doubts? at any rate not: the green manikins from Mars

The Court issues the following order: Mr(s) O. is appointed to an expert of Forensic Computing. The expert is assigned to answer the following questions:

- How secure is the investigation of the customer on the basis of the ip-address? resp. is it possible, that an error occurs in the log ? i.e. a wrong ip-address, date or time is stored
- If yes:
  - are there any science-based findings, how often this happens?
  - would an error be noticeable anyway?
- Is it possible to modify the content of a log file?
- If yes, would a manipulation be discoverable anyway?
- Could a site by Firefox be accessed (prefetched) without assistance by the user?
- If yes, is it also automatically downloaded then?
- If yes, would this be discoverable anyway? i.e. stored in ISP’s or users log files or browser-cache
- Could anyhow a photo be stored on the users hdd without his assistance and knowledge?
- If yes, would this be discoverable anyway? i.e. stored in ISP’s or users log files or browser-cache

3.9 Proportional Cybersecurity

Radim Polcák (Masaryk University, CZ)

Securing national cyberspace always requires at least marginal infringement of distributive (individual) rights in favor of non-distributive (common) goods. The key issue in this case is to proportionally balance between various constitutionally grounded rights depending on recent state of social and technical development. If a system of national cybersecurity is to be somewhat efficient, it always has to combine gathering information with efficient competences including ultimate ones like blocking. That obviously collides with a set of individual information rights that the German Constitutional Court originally named as the right to information self-determination as well as with various procedural rights together named as the right for fair trial.

Compared to traditional security issues, there are multiple specific features also in securing of internal information infrastructure of a state and in gathering of respective evidence. Strict centralized security measures always represent an issue as to basic principle of distinction of powers; this applies namely in the case of judicial infrastructure as well as in the case of information space of state offices that are to be treated independently of the rest of state administration.

The note will discuss most recent constitutional issues in developing of efficient national cybersecurity solutions taking into account not just leading constitutional doctrine and recent constitutional case-law (namely those in data retention cases), but also technical features and specifics of various European national laws (like extraordinary strength of principle of legal evidence in the Czech Republic).

3.10 Casebook on Cyber Forensics (CCF) – a proposal for discussion

Viola Schmid (TU Darmstadt, DE)

URL http://www.cylaw.tu-darmstadt.de/home_2/forschung_4/onlinepublikationencylawreports_1/online_publikationen_cylaw_reports.de.jsp

Dagstuhl inspired the idea of a "Casebook on Cyber Forensics" (CFF) from a legal perspective. A lot of questions are connected with this endeavour. First the question of terminology: why not name it casebook on "digital forensics", "forensic informatics", or "forensic computing"? The title "cyber forensics" was chosen because these forensics are essential for cyberlaw, the law allocating chances and risks, rights and obligations in cyberspace. Moreover, not only digital data but also data written on paper comes into play.

The second question is: How should such a casebook be structured? Two prototypes — one regarding the format of such a casebook, one regarding the content of such a case book — were presented. The link between format and content is the formula: "form follows function". First, a "Cylaw Report" of the department of Public Law, Technical University of Darmstadt, on the topic of "Subscription Decoys" (Strafbarkeit von "Abo-Fallen"-Betreibern am Beispiel der "kostenpflichtigen" Vermittlung des Zugriffs auf eigentlich kostenlose Software (Freeware)?) was presented as a paradigm for the potential format[1] of such a CCF.

Members of the Computer Science community could contribute to the description of the facts of the case. Then another "Cylaw Report" on the topic of "Online Searches or Remote Acqusition" (Verdeckte Online-Durchsuchungen — zur IT-(Un)Sicherheit in Deutschland)[2] was offered for discussion and a an example for the potential content of a CCF. In this case, the federal constitutional court of Germany accepted online searches even if they do not guarantee authenticity and integrity of the data in every case. And also the US-American case Heckenkamp was cited as an example that online searches are a transatlantic phenomenon.

A potential table of contents for a CCF would divide the casebook in two parts:

- Part one: Scenarios that are distinguished by the information technology that is analyzed.

[1] http://tuprints.ulb.tu-darmstadt.de/2201/
[2] http://tuprints.ulb.tu-darmstadt.de/1357/

- Part two: Legal Principles such as the exclusionary rule.

Summa summa rum: a lot of work has to be done until this proposal becomes reality.

3.11 Mobile Phone Forensics with the help of ADEL

Michael Spreitzenbarth (University of Erlangen-Nuremberg, DE)

Joint work of Spreitzenbarth, Michael; Schmitt, Sven; Freiling, Felix
URL http://forensics.spreitzenbarth.de/?page_id=258

Due to the ubiquitous use of smartphones, these devices become an increasingly important source of digital evidence in forensic investigations. Thus, the recovery of digital traces from smartphones often plays an essential role for the examination and clarification of the facts in a case. Although some tools already exist regarding the examination of smartphone data, there is still a strong demand to develop further methods and tools for forensic extraction and analysis of data that is stored on smartphones. In this paper we describe specifications of smartphones running Android. We further introduce a newly developed tool –called ADEL– that is able to forensically extract and analyze data from SQLite databases on Android devices. During our evaluation we found that in contrast to data retained by the network operator, location data stored on the mobile device in many cases offers much more precise information than the rather coarse-grained data from the network operator. However, the availability of data shows a much higher variability on the mobile phone than at the network operator. Finally, a detailed report containing the results of the examination is created by the tool. The whole process is fully automated and takes account of main forensic principles.

3.12 Selective Imaging

Johannes Stuettgen (University of Erlangen-Nuremberg, DE)

Main reference M. Baecker, F.C. Freiling, S. Schmitt, "Selektion vor der Sicherung," in: Datenschutz und Datensicherheit – DuD, Volume 34, Number 2, 2010.
URL http://www1.cs.fau.de/filepool/thesis/diplomarbeit-2011-stuettgen.pdf

In an increasingly computerized world, the amount of digital evidence in criminal investigations is constantly growing. In parallel, storage capacities of digital devices scale up every year, to a point where current forensic procedures meet inherent limitations. Furthermore, digital evidence acquisition standards are often unable to comply to data protection regulations, forcing investigators to violate the principle of commensurability frequently, to be able to seize any evidence at all.

Our work aims at streamlining the forensic acquisition process, to enable forensic examiners to selectively acquire only those data objects that are of relevance to the investigation. This approach greatly enhances the scalability of data acquisition methods and enables investigators to respect data protection principles without sacrificing important evidence.

3.13 Legal Challenges of transborder Searches

Nicolas von zur Muehlen (MPI für ausländ. u. internat. Strafrecht-Freiburg, DE)

Transborder Searches have been an issue since the early days of the Internet and are still one of the biggest challenges for law enforcement agencies when obtaining digital evidence over the internet. This talk aims to explain the basics of the principle of territoriality. It will address the question of wether the violation of this principle –such as the accessing of data stored on a computer outside national territory– is even justified. Furthermore, the basics of mutual assistance are explained. Finally, this talk deals with the problem that traditional legal concepts can reach their functional limits in global cyberspace, especially when the territorial location of data cannot be pinpointed, as for example in cloud systems.

Participants

- Harald Baier
Hochschule Darmstadt, DE
- Glenn S. Dardick
Longwood Univ. – Virginia, US
- Andreas Dewald
Universität Mannheim, DE
- Felix C. Freiling
Universität Erlangen, DE
- Dieter Gollmann
TU Hamburg-Harburg, DE
- Daniel Hammer
Hochschule Offenburg, DE
- Focke Höhne
Universität Passau, DE
- Joshua James
University College – Dublin, IE
- Stefan Kiltz
Universität Magdeburg, DE
- Kwok Lam
National Univ. of Singapore, SG
- Martin Mink
TU Darmstadt, DE
- Stig Frode Mjolsnes
NTNU – Trondheim, NO
- Christian Moch
Universität Erlangen, DE
- Herbert Neumann
Anwaltskanzlei Neumann – Molfsee, DE
- Radim Polcák
Masaryk University, CZ
- Joachim Posegga
Universität Passau, DE
- Viola Schmid
TU Darmstadt, DE
- Sven Schmitt
Bundeskriminalamt – Wiesbaden, DE
- Thomas Schreck
Siemens – München, DE
- Andreas Schuster
Deutsche Telekom – Bonn, DE
- Michael Spreitzenbarth
Universität Erlangen, DE
- Johannes Stüttgen
Universität Erlangen, DE
- Stefan Vömel
Universität Erlangen, DE
- Nicolas von zur Mühlen
MPI für ausländ. und internat. Strafrecht – Freiburg, DE
- Christian Winter
Fraunhofer SIT – Darmstadt, DE