Report from Dagstuhl Seminar 14092

Digital Evidence and Forensic Readiness

Edited by

Glenn S. Dardick[1], Barbara Endicott-Popovsky[2], Pavel Gladyshev[3], Thomas Kemmerich[4], and Carsten Rudolph[5]

1 **Longwood University – Farmville, US,** gdardick@dardick.net
2 **University of Washington, US**
3 **University College Dublin, IE,** pavel.gladyshev@ucd.ie
4 **Gjøvik University College, NO,** thomas.kemmerich@hig.no
5 **Fraunhofer SIT – Darmstadt, DE,** carsten.rudolph@sit.fraunhofer.de

Abstract

The seminar on Digital Evidence and Forensic Readiness provided the space for interdisciplinary discussions on clearly defined critical aspects of engineering issues, evaluation and processes for secure digital evidence and forensic readiness. A large gap exists between the state-of-the-art in IT security and best-practice procedures for digital evidence. Experts from IT and law used this seminar to develop a common view on what exactly can be considered secure and admissible digital evidence.

In addition to sessions with all participants, a separation of participants for discussing was arranged. The outcome of these working sessions was used in the general discussion to work on a common understanding of the topic. The results of the seminar will lead to new technological developments as well as to new legal views to this points and to a change of organizational measures using ICT. Finally, various open issues and research topics have been identified. In addition to this report, open research issues will also be published in the form of a *manifesto* on digital evidence.

One possible definition for *Secure Digital Evidence* was proposed by Rudolph et al. at the Eighth Annual IFIP WG 11.9 International Conference on Digital Forensics 2012. It states that a data record can be considered secure if it was created authentically by a device for which the following holds:

- The device is physically protected to ensure at least tamper-evidence.
- The data record is securely bound to the identity and status of the device (including running software and configuration) and to all other relevant parameters (such as time, temperature, location, users involved, etc.)
- The data record has not been changed after creation.

Digital Evidence according to this definition comprises the measured value and additional information on the state of the measurement device. This additional information on the state of the measurement device aims to document the operation environment providing evidence that can help lay the foundation for admissibility.

This definition provided one basis of discussion at the seminar and was compared to other approaches to forensic readiness.

Additional relevant aspects occur in the forensic readiness of mobile device, cloud computing and services. Such scenarios are already very frequent but will come to full force in the near future.

The interdisciplinary Dagstuhl seminar on digital evidence and forensic readiness has provided valuable input to the discussion on the future of various types of evidence and it has build the basis for acceptable and sound rules for the assessment of digital evidences. Furthermore, it has established new links between experts from four continents and thus has set the foundations for new interdisciplinary and international co-operations.

Digital Evidence and Forensic Readiness, *Dagstuhl Reports*, Vol. 4, Issue 2, pp. 150–190
Editors: Glenn S. Dardick, Barbara Endicott-Popovsky, Pavel Gladyshev, Thomas Kemmerich, and Carsten Rudolph
DAGSTUHL REPORTS
Dagstuhl Reports
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Seminar Februrary 23–28, 2014 – http://www.dagstuhl.de/14092
1998 ACM Subject Classification D.4.6 Security and Protection, K.4.2 Social Issues, K.5.2 Governmental Issues
Keywords and phrases digital evidence, forensic readiness, mobile forensic, trusted computing, Cyberlaw
Digital Object Identifier 10.4230/DagRep.4.2.150
Edited in cooperation with Günther Diederich (ifib GmbH – Bremen, DE)

1 Executive Summary

Carsten Rudolph

This summary briefly recapitulates the outcomes of our seminar on digital evidence and forensic readiness. The main focus of the seminar was to work on a common cross-discipline understanding of notions of digital evidence and forensic readiness. In particular, technical notions in the view of IT security experts and the legal view were considered. Furthermore, relevance of differences in jurisdictions in different countries was also discussed.

The participants of the seminar came from 4 continents (Europe, U.S., Africa and Australia) and 12 countries. The group was a mix of experts from digital forensics, IT security, cyber security, archival sciences, criminal law, civil law, and cyber law. Thus, all relevant disciplines for digital evidence and forensic readiness were represented in the seminar, creating a perfect group for the task, but also a challenging communication environment that required good leadership in the interaction and discussions.

The main focus of the seminar was to develop a common view on what exactly can be considered secure and admissible digital evidence. The seminar was a first attempt to achieve progress towards this goal and therefore, a comprehensive coverage of the topic was not to be expected. Nevertheless, the international interest in the topic as well as the intensive discussions in the seminar show the relevance of the topic. The results of the seminar identify open issues in the area of digital forensics, but also proposes first substantial steps in the direction of establishing strong and internationally useful notions for digital evidence and forensic readiness.

Initial talks and discussions quickly revealed some of the majour challenges:

- The growing variety of types of potential digital evidence increases the problem to define clear technical guidelines for the collection and evaluation of data records for forensic use. Examples include mobile devices, data stored and processed via cloud service, huge infrastructures with distributed data, or big data with many possible interpretations of data found.
- In many cases, digital evidence cannot be directly related to data on one device. In particular in cloud environments, stored data is distributed over different countries and digital processes easily cross borders. Thus, digital evidence becomes a cross-jurisdictional issue that needs rules on how to deal with differences and contradictions in jurisdiction.
- Teaching and education is another challenge. One cannot expect all lawyers, attorneys, or judges to become experts on technical issues. however, a basic understanding of the area of digital evidence is essential to be able to decide if expert witnesses are required and also to be able to achieve correct interpretations of the report by expert witnesses.

- forensic readiness can guide the development of systems that collect, store, and provide secure digital evidence. However, the applicability of forensically ready technical solutions is restricted by privacy and also economy. Here, processes need to be defined and adequate procedures and regulations (also internationally) need to be found.

Four discussion groups were formed in the seminar to discuss *digital forensic readiness processes and procedures for investigators*, *notions of digital evidence*, *a forensic readiness landscape*, and *forensic readiness: evidence in a digital world*. More details of the results of the discussions in the working groups can be found in the sections below.

As one of the major results of the seminar can be identified that all participants understood and agreed on the need to initiate future research activities in the area of digital evidence and forensic readiness. The results also clearly show that this research must be international and inter-disciplinary. Furthermore, the seminar has proven that technically oriented IT security experts and experts from law can co-operate to advance the state of the art. The seminar has established new inter-disciplinary and international contacts that are suitable to build a new community that will drive this strand of work in the field of forensic readiness.

2 Table of Contents

Executive Summary

Overview of Talks

Working Groups

3 Overview of Talks

3.1 Legal Processes for Cloud Forensic Investigations

Aaron Alva (University of Washington – Seattle, US)

Cloud forensics is an emerging field that addresses how to ensure cloud-based evidence can be used in courts of law. The US Federal Rules of Evidence were originally designed for paper documents, and updates to the rules have yet to consider the cloud-paradigm. This presentation discusses the legal challenges involved in cloud computing investigations, and the potential legal processes that can be adapted for the admissibility of cloud-based evidence.

References

1 A. Alva, and B. Endicott-Popovsky, *Legal Process and Requirements for Cloud Forensic Investigations, Cybercrime and Cloud Forensics: Applications for Investigation Processes*, IGI Global, 2013, pp.186–235; http://ssrn.com/abstract=2197978

3.2 Implementation guidelines for a harmonised digital forensic investigation readiness process model

Hein Venter (University of Pretoria, ZA)

Joint work of Valjarevic, Aleksandar;
Main reference A. Valjarevic, H. S. Venter, "Implementation guidelines for a harmonised digital forensic investigation readiness process model," in Proc. of the 2013 Information Security for South Africa Conf., pp. 1–9, IEEE, 2013.
URL http://dx.doi.org/10.1109/ISSA.2013.6641041

Digital forensic investigation readiness enables an organisation to prepare itself in order to perform a digital forensic investigation in a more efficient and effective manner. Benefits of achieving a high level of digital forensic investigation readiness include, but are not limited to, higher admissibility of digital evidence in a court of law, better utilisation of resources (including time and financial resources) and higher awareness of forensic investigation readiness.

The problem that this research addresses is that there exists no harmonised digital forensic investigation readiness process model. In addition, no implementation guidelines exist and, thus, there is a lack of an effective and standardised implementation of digital forensic investigation readiness measures within organisations.

Part of this research also involves the harmonasation and standardisation of the entire digital forensic investigation process. An ISO standard, ISO/IEC 27043, in this regard will be published in 2014 of which I am the main editor.

References

1 Aleksandar Valjarevic and Hein S. Venter. *Implementation guidelines for a harmonised digital forensic investigation readiness process model*. IEEE Xplore, Published in Information Security for South Africa, Johannesburg, South Africa, 2013, ISBN 978-1-4799-0808-0

3.3 Computer Forensics in Industrial Control Systems

Heiko Patzlaff (Siemens – Munich, DE)

This talk addresses the challenges of performing computer forensic investigations in industrial control systems (ICS). Starting with Stuxnet, the general lack of tools and procedures for analyzing security incidents in industrial settings has become apparent.

In this talk first an introduction to ICS systems is given. We discuss the challenges that arise when one needs to investigate security incidents in industrial products. In particular, what data is available in these systems, how to acquire this data, how to transfer and analyze it and what conclusions can be drawn from it. Some examples of real world cases are discussed. And the preliminary results of the Crisalis research project are presented that aims at developing tools and approaches for performing computer forensic investigations in IC systems.

3.4 The origin of digital evidence

Felix C. Freiling (Friedrich-Alexander-University Erlangen-Nürnberg, DE)

Joint work of Freiling, Felix C.; Dewald, Andreas
Main reference A. Dewald, F. C. Freiling, “Is Computer Forensics a Forensic Science?”, Presentation at the 2012 Current Issues in IT Security Conf., Freiburg, Germany, 2012.

The focus of forensic computing , i.e., forensic computer science, is digital evidence. Digital evidence is any digital data that has relevance to questions of law. In this sense, digital evidence is similar to physical evidence, a type of evidence that is in the focus of classical forensic sciences (like forensic biology or forensic medicine). Unlike physical evidence, digital evidence is not primarily tied to the physical matter (e.g., the magnetic tape) that stores the data. The value of digital evidence regularly lies in the *information* encoded within the stored data. In cases where the physical storage device is important (e.g., the hard disc of a particular computer seized in a particular place), we have a combination of physical and digital evidence.

The fact that digital evidence is a question of information rather than physical matter is not surprising, since digital data is always an *abstraction* of physical phenomena (e.g., magnetization of the surface of a hard disc). But this aspect is also not specific to *digital* evidence. Here we can also draw from insights in classical forensic sciences: The notion of digital evidence can draw almost fully from what is called *imprint evidence.* Examples of imprint evidence are tool marks or footprints where – at least theoretically – an exchange of physical matter does not have to happen. And while for a long time the transfer of physical matter was believed to be the basis for any form of evidence (due to Locard’s “exchange principle”), Inman and Rudin [1] developed the concept of “transfer of traits” to explain the origin of such evidence.

So digital evidence is not fundamentally new (as postulated by many authors, e.g., Casey [2]). The main difference between digital and physical evidence lies rather in the possibility to automatically gather and process it.

References

1 Keith Inman, Norah Rudin: *Principles and Practice of Criminalistics: The Profession of Forensic Science.* CRC Press, 2001.

2 Eoghan Casey: *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet.* Academic Press, 3rd ed., 2011

3.5 Cloud and mobile forensics

Kim-Kwang Raymond Choo (University of South Australia – Mawson Lakes, AU)

As the use of information and communications technologies (ICT) grows throughout society in general, so does their use by criminals, particularly in areas of serious and organised crime where ongoing secure communication and secure dissemination and storage of their data is critical for the operation of the criminal syndicate – similar to how cybercrime may be understood as a new way of committing traditional crimes ([5]; [7]).

There are various challenges and implications of emerging technologies for governments – particularly law enforcement and regulatory agencies – and other key stakeholders. For example, during investigations of crimes involving the use of cloud computing, there is usually some accumulation or retention of data on a digital device (e.g. mobile device used to access cloud services and cloud datacentres) that will need to be identified, preserved, analysed and presented in a court of law – a process known as digital forensics ([4]; [10]; [16]). Many conventional forensic tools have focused upon having physical access to the media that stores the data of potential interest. However, in a cloud computing environment it is often not possible or feasible to access the physical media that stores the user's data ([12]; [11]). In addition, [16] pointed out not all countries have legal provisions which allow for data to be secured at the time of serving a warrant, such as at the time of a search and seizure undertaking. Data fragmentation and distribution across the globe within numerous datacentres also present technical and jurisdictional challenges in the identification and seizure of (the fragile and elusive) evidential data by law enforcement and national security agencies in criminal investigations as well as by businesses in civil litigation matters ([7]; [14]; [15]). The technical and legal uncertainties surrounding these questions are, perhaps, why traditional boundaries are now blurred ([9]).

Existing digital forensic techniques are designed to collect evidential data from typical digital devices (e.g. where advanced security features and anti-forensic techniques are rarely exploited to their full extent). In contrast, serious and organised criminals often make use of secure services and devices specifically designed to evade legal interception and forensic collection attempts. Examples of devices designed to enable encrypted communications include the Android-based Blackphone ([3]; [19]) and the well-known BlackBerry. While the use of BlackBerry in the consumer market might be declining, Australian law enforcement agencies have suggested that these devices have become popular amongst serious and organised criminals – see interview by Acting CEO of Australian Crime Commission ([1]). For example, it was recently reported that

> *[t]housands of encrypted phones are believed to be in Australia and the officials say some of the phones are suspected of being used to send the most dangerous messages imaginable – those that lead to murder . . . [and] Police believe one*

> *of Australia's most violent outlaw bikers used uncrackable encrypted phones to order some of the shootings that have rocked Sydney ([2]).*

Therefore, the digital forensics 'space' can be seen as a race, not only to keep up with hardware and software/application releases (e.g. by cloud and mobile service providers), but also from software and hardware modifications made by end users, particularly serious and organised criminals, to complicate or prevent the collection and analysis of digital evidence. For example, although cloud computing may have attracted academic attention, including issues relating to data sovereignty and data confidentiality, and the inadequacy of our existing legislative and regulatory frameworks to protect the data from criminals and government's prying eyes (see [5]; [6]; [8]; [13]; [17]; [18]), research on security, privacy and forensics challenges associated with cloud computing is still in its infancy.

References

1 Australian Broadcasting Corporation 2014a *Questions arise despite crime task force grabbing $500 million haul.* Media transcript 23 January. http://www.abc.net.au/7.30/content/2013/s3931176.htm

2 Australian Broadcasting Corporation 2014b *Sydney shooting murders linked to uncrackable phones.* Media transcript 05 March. http://www.abc.net.au/7.30/content/2014/s3957610.htm

3 Boeing 2014 *Boeing black smartphone* http://www.boeing.com/assets/pdf/defense-space/ic/black/boeing_black_smartphone_product_card.pdf

4 Butler B and Choo K-K R n.y. *IT standards and guides do not adequately prepare IT practitioners to appear as expert witnesses: An Australian perspective.* Security Journal [In press, DOI: 10.1057/sj.2013.29]

5 Choo K-K R 2010 *Cloud computing: Challenges and future directions* Trends & Issues in Crime and Criminal Justice no 400:1–6

6 Gray A 2013 *Conflict of laws and the cloud* Computer Law & Security Review 29(1):58–65

7 Hooper C, Martini B and Choo K-K R 2013 *Cloud computing and its implications for cybercrime investigations in Australia* Computer Law & Security Review 29(2):152–163

8 Irion K 2012 *Government cloud computing and national data sovereignty* Policy & Internet 4(3-4):40–71

9 Jones D and Choo K-K R 2014 *Should there be a new body of law for cyber space?* In 22nd European Conference on Information Systems (ECIS 2014), Tel Aviv, Israel, 9–11 June [In press]

10 McKemmish R 1999 *What is forensic computing?* Trends and Issues in Crime and Criminal Justice 118:1–6

11 Martini B and Choo K-K R 2013 *Cloud storage forensics: ownCloud as a case study* Digital Investigation 10(4):287–299

12 Martini B and Choo K-K R 2012 *An integrated conceptual digital forensic framework for cloud computing* Digital Investigation 9(2):71–80

13 Maxwell, W., and Wolf, C. 2012 *A global reality: Governmental access to data in the cloud* http://www.cil.cnrs.fr/CIL/IMG/pdf/Hogan_Lovells_White_Paper_Government_Access_to_Cloud_Data_Paper_1_.pdf

14 Quick D and Choo K-K R 2013a *Digital Droplets: Microsoft SkyDrive forensic data remnants* Future Generation Computer Systems 29(6): 1378–1394

15 Quick D and Choo K-K R 2013b *Dropbox Analysis: Data Remnants on User Machines* Digital Investigation 10(1):3–18

16 Quick D and Choo K-K R 2013c *Forensic collection of cloud storage data: Does the act of collection result in changes to the data or its metadata?* Digital Investigation 10(3):266–277

17 Ryan P and Falvey S 2012 *Trust in the clouds* Computer Law & Security Review 28(5):513–521

18 Ter KL 2013 *Singapore's personal data protection legislation: Business perspectives* Computer Law & Security Review 29(3):264–273

19 Silent Circle 2014 *New smartphone to put privacy and control first* Media release 15 January. https://silentcircle.com/web/press-releases/1-15-14-PRNewswire/

3.6 Forensic readiness for smart mobile devices

Florian Junge (Universität Bremen, DE)

Smart mobile devices (SMD), such as smartphones or tablets, offer a wide range of computation and communication facilities. Even though the devices were initially targeted for the private customer market, business organizations nowadays use them more frequently for commercial purposes. With a higher rate of usage, the devices become a more attractive target for attackers. However, even their restricted operating system designs cannot enforce comprehensive protection for the data on the device. Thus after the occurrence of a security incident, computer forensics techniques are needed for an understanding of the details, clean up and especially for a judicial prosecution. To facilitate forensic investigations, the concept of Forensic Readiness was developed. Its comprises measures to collect credible digital evidence, which might help in forensic investigations, as well as staff training for special procedures needed to shorten the investigations.

As part of an ongoing research project "SAiM", I examined the adaptation of forensic readiness to SMDs. I call this concept "Mobile Forensic Readiness", which has been presented in this talk. The focus is on smartphones in business organizations, because these have the biggest need for regulatory compliance in their operations. Therefore they need a proper analysis of security incidents and an effective collaboration with law enforcement. The research revealed potential technical, operational and legal aspects which have be addressed in order to achieve mobile forensic readiness.

On the technical side, topics like logging overhead or secure storage and transportation have to be considered. Also, data handling and hand over operations done by interal staff must be taken into account and which laws regarding privacy of personal data apply. Furthermore, as the data is designated to be used in court, its usefulness in such cases must be evaluated. My work examines these topics and the mentioned aspects. The goal is to deliver an approach to handle the overall process, beginning from risc assessments inside an organization to the handling of the evidence in court.

The technical architecture of this research work extends the components developed in SAiM. The project provides a framework for dynamic malware analysis on SMDs. Pattern matching algorithms for strings are used on the device itself. These use as input discretized events that are generated by various sensors throughout the operating system. A central server generates the patterns, because the computational power of a handheld device is not strong enough for the creation. The overall goal of this bi-polar approach in combination with a light-weight transport protocol is the recognition of designated malware as well as attacked apps.

3.7 Hardware-based secure digital evidence

Nicolai Kuntze (Fraunhofer SIT – Darmstadt, DE)

Joint work of Kuntze, Nicolai; Rudolph, Carsten

Traditional approaches to digital forensics are concerned with the reconstruction of events within digital systems that often are not built for the creation of evidence. Various examples exist where devices are meant to provide certain evidence like precise farming, speed cameras, automotive black boxes or other process documentation equipment. In these cases, specialised equipment samples data that is meant to provide a non-reputable proof on a certain event.

The presentation focuses on the idea of incorporating requirements for forensic readiness designing-in features and characteristics that support the use of the data produced in these devices being used as evidence. This paper explores legal requirements that such evidence must meet as the basis for developing technical requirements for the design of such systems. An approach is proposed using state of the art security technology that could be used to develop devices and establish processes crafted for the purpose of creating digital evidence. The aim hereby is to add specific meta data to the evidence created that shows additional specifics of the device, software and processes in place needed to judge on the authenticity of the evidence created.

The presenter suggests that the legal view needs to be incorporated into the device design as early as possible to allow for the probative value required of the evidence produced by such devices.

3.8 Can an Integrated Model of Digital Forensics Practice and Digital Records Lifecycle Inform Forensic Readiness

Corinne Rogers (InterPARES Trust – Vancouver, CA)

Main reference C. Rogers, "Digital Records Forensics: Integrating Archival Science into a General Model of the Digital Forensics Process," in Proc. of the Second Int'l Workshop on Cyberpatterns: Unifying Design Patterns with Security, Attack and Forensic Patterns, pp. 4–21, Oxford Brookes University, 2013.
URL http://tech.brookes.ac.uk/CyberPatterns2013/

Both archival and digital forensics methods and principles evolved out of practice and grew into established professional disciplines by developing theoretical foundations, which then returned to inform and standardize that practice. An intersection of digital forensics and digital diplomatics increase our capacity to identify records in digital systems, assess their authenticity, and establish the requirements for their long-term preservation. This paper presents the Digital Records Forensics general process model (DRF model), developed as a tool to aid in meaningful comparison of digital forensics activities and archival preservation activities. The purpose is to assess the moments in which digital records as understood by archival science, and digital evidence as understood by digital forensics, may be identified, their authenticity assessed, their reliability and integrity managed and preserved, in order to satisfy laws of evidence and requirements for admissibility.

The Digital Records Forensics general process model offers a point of departure in a mutual discussion between records professionals and digital forensics professionals. By combining the technical expertise of digital forensics with the social and contextual analysis of records and data from archival science (and in particular the theory and methodology of archival diplomatics), a richer understanding of digital evidence is possible. This work continues in the research undertaken by the InterPARES Trust project (www.interparestrust.org) broadly, and in specific project within that research in which the author is involved that are studying metadata requirements for authenticity of digital material, and modeling of authenticity in the process of digital preservation of records and data in online environments.

3.9 Digital Evidence and Forensics in Australia and New Zealand – Recent Developments

Nigel Wilson (University of Adelaide, AU)

Recent cases in Australia and New Zealand demonstrate that digital evidence continues to present challenges at the pre-trial stage and also significant admissibility concerns. Discovery protocols have also had both procedural and trial impact as has inadequate compliance with digital evidence procedures. Most importantly, the role of expert evidence (and the increasing role of digital experts) has been paramount. Digital expert evidence faces a trio of challenges: its 'leading-edge' nature, the inherent complexity of the characteristics of digital evidence and the technical diversity of the sciences which constitute its specialised knowledge base. Future developments will involve issues arising from Australia's implementation of the European Convention on Cybercrime, cloud computing and human rights (principally privacy). As a result of the adoption of international cybersecurity obligations in Australia, mutual assistance will be required by law enforcement agencies and industry to expedite the interception, real-time collection, access to, preservation and disclosure of digital evidence.

3.10 Computational Forensics: Forensic Investigations in Cyberspace: what about big data?

Katrin Y. Franke (Gjøvik University Colledge, NO)

Information Society has become a reality with the establishment of the Internet. These ICT infrastructures are complex, rapidly growing, and constantly changing. Massive amounts of data are shared. The estimate for 2012 is 247 billion emails per, about 234 million websites and 5 billion mobile-phone users. The data volume is expected to increase by factor 44 within one decade only, i.e. from 800,000 petabyte in 2009 up to 35 zetabyte in 2020 (Gantz & Reinsel, 2010).

The reliance on the Internet creates increasing vulnerabilities. Cyber attacks from organized crime and terrorism pose severe threats to society. ICT infrastructures are constantly exposed to hostile and unwanted activities. In 2012 it was reported about 1 million victims of cyber crime with constant increase and expected losses of 297 billion Euros by 2017 (RAND, 2012).

The methods used to combat the increasing amount of high-tech crime and computer crime, must be improved. The amount of data and sharing of ICT resources through the cloud is so extensive and complex that current methods are incapable to cope. Proactive, ultra-large scale forensic investigations need to be researched and developed.

Computational forensics (CF) is an emerging interdisciplinary field of research. It unites expertise from computer science and forensic science. Data-science methods may establish decentralized, collaborative and independent investigation procedures. These require computing algorithms that are context- aware, adaptable and self-organizing. Typical challenges in investigations are about gathering evidence, search, ability to link various evidence and to visualize them.

In addition to the technological issues are the social and socio-technical, e.g. when it comes to culture, social behavior, law and policy rules in different countries. International cyber laws should be further improved so that international cooperation can strengthened. There is great demand to establish a legal framework for ICT (Sunde, 2006), and implement the law into ICT functionality, e.g. programming laws and regulations to automate the enforcement of them (Sunde, 2010).

The objective of this resentation is to provide an introduction to research methods through the increase of very large amounts of data, and to encourage discussion about the consequences thereof. Researchers in computer science and computer specialists be exposed with forensic sciences. Investigations related challenges that make it necessary to develop the next generation digital investigations, are pointed out. Researchers in forensics and case investigators are introduced to the basic techniques of digital computing and information technology.

Selected examples of successful methods adopted for data processing, and ongoing research will contribute to the understanding and confidence in the new technology. Examples include digital forensics through the cloud, i.e.

1. detection malicious PDF
2. the detection of malware when the malicious program operates, and
3. automatic linking evidence from multiple computers.

3.11 Models for Incorporating Forensic Readiness into Design as an Aspect of Resilience and Security

Barbara Endicott-Popovsky (University of Washington – Seattle, US)

Main reference B. Endicott-Popovsky, D. Ryan, D. Frincke, “The New Zealand Hacker Case: A post mortem,” in Proc. of the Oxford Internet Institute Cybersafety Conf. on Safety and Security in a Networked World: Balancing Cyber-Rights & Responsibilities, 9pp., 2005.
URL http://www.oii.ox.ac.uk/microsites/cybersafety/extensions/pdfs/papers/barbara_endicottpopovsky.pdf

A typical incident response pits technicians against networks that aren’t prepared forensically [1, 2]. If practitioners do consider collecting digital forensic data from networks, they face a choice between expending extraordinary effort (time and money) collecting forensically sound data, or simply restoring the network as quickly as possible. The latter means key evidentiary files most likely are altered in the process, limiting their forensic value. With limited interest in pursuing legal action, those administering networks most often make the expedient choice – responding to distraught users by restoring network function as soon as possible, ignoring the rigors of collecting and preserving forensically sound data [3].

In the interest of establishing evidence of having exercised reasonable care to protect data on their networks, legal counsel have begun urging organizations to invest in procedures and technology that will allow collection of forensically sound data defensible in a court of law [4].

There is an urgency to 're-think' our traditional models for incident response to include forensic readiness [1]. In this presentation a proactive and preventive approach as opposed to a reactive one. It includes recommendations for how to "operationalize" organizational forensic readiness and change our mental models for managing networks.

References

1 Rowlinson R. *Ten Steps to Forensic Readiness* International Journal of Digital Evidence, Winter 2004, Volume 2, Issue 3.

2 Tan J. *Forensic Readiness* Cambridge 2001, MA: Stake.

3 Dittrich D. *Basic Steps in Forensic Analysis of Unix Systems.* Retrieved October 28, 2004 from the World Wide Web http://staff.washington.edu/dittrich/misc/forensics/.

4 Simon M. *Seminar in Data Security* Preston Gates: Seattle, WA, March 2, 2005.

3.12 Exploring the space of digital evidence

Carsten Rudolph (Fraunhofer SIT – Darmstadt, DE)

Digital evidence is much more than what is acquired during forensic investigations. One approach towards defining the available space for digital evidence suggests three dimensions. First, and most obviously, is the time when data is collected, processed, retained and correlated for potential forensic use. This dimension includes data collected at runtime, data collected for particular transactions, in case of deviations, for incidents, "post-mortem" forensic investigations, and the digitalization of evidence for court procedures. The second dimension describes the goal for which digital evidence is produced. This can be either for showing compliance, i.e. for proving that somebody was not responsible for some incident or for for showing malicious events that happened and to find who did what. Finally, the third dimension consists of the actual information to be documented. Examples are the documentation of the normal system behaviour, compliance information, accidents, safety issues, malicious behaviour, identity informations and various relevant parameters.

3.13 New "E-Justice" Law in Germany since 2013 – A Temple Architecture for an "Agenda of Securitization"

Viola Schmid (TU Darmstadt – Darmstadt, DE)

This abstract summarizes inspirations and discussions of an ambitious Dagstuhl seminar. The talk (27.02.2014) was titled: "New 'E-Justice' Law in Germany since 2013 – A Temple Architecture for an 'Agenda of Securitization"'. The presentation provided and argued with

[1] Defined as 'maximizing the ability of an environment to collect credible digital evidence while minimizing the cost of an incident response' [2].

Anglo-Saxon as well as German **terminologies** – partly bilingually. The importance of transnational terminologies is also reflected in the ductus of this abstract, by using German and Anglo-Saxon terminologies and texts. Examples for the results of this terminological query are:

- "Recht" as part of "Ge(recht)igkeit";
- "E-Justiz" instead of "E-Justice" and
- "Rechtswissenschaft" in the German terminology as "creation of legal science ("Rechtswissen")" instead of "legal science" in the Anglo-Saxon terminology describing the status of knowledge (Latin: scientia – "Wissen"). In short: A literal interpretation of "Rechtswissenschaft" comprises the process of information gathering ("Schaffen"). This inclusion of the scientific process (and method) makes the German denomination noteworthy.

These insights can only be gained by using "transnational" terminologies and legal analysis.

E.g.: This research method led to a differentiated use of "E-Justice" in the German legal system.[2]

These questions of terminology prepare the groundwork for the presentation of the following content that was addressed in February 2014:

- On the one hand – first – the audience was informed about new "E-Justice" ("E-Justiz") legislation in Germany and the challenges arising from this endeavor.
- On the other hand – second – a research initiative at the Faculty of Law and Economics, Technical University Darmstadt, Germany, was introduced (the so called "LEXONOMICS")[3].

In addition to the presentation at Dagstuhl, this abstract provides a third aspect: The follow-up – third – of the ideas presented in February 2014 with *the judgment of the European Court (Grand Chamber), 8. April 2014, C-293/12 and C-594/12* (Digital Rights Ireland Ltd (C-293/12) v Minister for Communications, Marine and Natural Resources et al. and Kärntner Landesregierung (C-594/12) et al.).

First: New "E-Justice" Law in Germany and Challenges for "Securitization" (Versicherheitlichung). The international audience with technological and/or legal expertise learned that there is a new German Law[4] in 2013 containing a master plan for lawmakers, as well as courts, establishing milestones for "e-courts" and "e-lawyers" [5] (especially the so called "power users"[6]) until 2022. By then, the "power users" must submit their briefs and documents "electronically" – otherwise the courts and the "justice system" may not admit these documents to court proceedings ("Informationstechnologiezwang" [7]). In short: There will be a new jurisdiction – the electronic jurisdiction ("elektronischer Rechtsweg") for law professionals[8] in Germany. Especially from the perspective of a German legal scientist ("Rechtswissenschaftler/in"), this digitization of the justice system poses new challenges

[2] Soon to be published: V. Schmid, in: H. Sodan/J. Ziekow, Großkommentar zur Verwaltungsgerichtsordnung, 4th Edition 2014, § 173 marginal number 13.

[3] V. Schmid, in: H. Sodan/J. Ziekow, § 173 marginal numbers 10 and 57.

[4] Act to Promote Electronic Legal Transactions with the Courts (translation by the author) – Gesetz zur Förderung des elektronischen Rechtsverkehr mit den Gerichten ("FeRGG", acronym by V. Schmid, in: H. Sodan/J. Ziekow, § 173 marginal number 1) vom 10.10.2013, BGBI. I, S. 3786.

[5] And „e-administration“ (Gesetz zur Förderung der elektronischen Verwaltung (E-Government-Gesetz – EGovG) vom 25. Juli 2013 (BGBl. I S. 2749).

[6] V. Schmid, in: H. Sodan/J. Ziekow, § 55a marginal number 25.

[7] V. Schmid, in: H. Sodan/J. Ziekow, § 55a marginal number 28.

[8] Not for ordinary citizens if there is no statutory requirement to be represented by a lawyer ("Anwaltszwang").

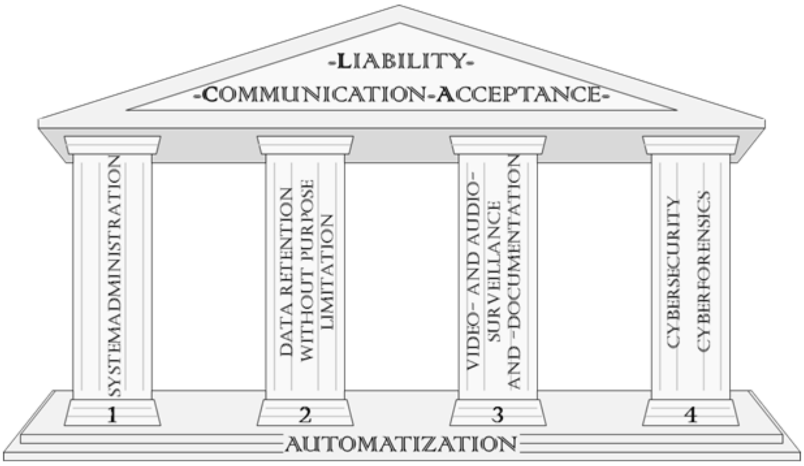

-LIABILITY-
-COMMUNICATION-ACCEPTANCE-
SYSTEMADMINISTRATION
DATA RETENTION WITHOUT PURPOSE LIMITATION
VIDEO- AND AUDIO- SURVEILLANCE AND -DOCUMENTATION
CYBERSECURITY CYBERFORENSICS
1
2
3
4
AUTOMATIZATION

Figure 1 Temple architecture of e-justice.

that need be mastered. The German language differentiates between "Recht" (law) and "Gerechtigkeit" (justice, justness) and the question arises: How does the digitization affect this distinction? What is the difference between a "justice system" and an "e-justice-system"? This is not only a challenge for the German Legal System as the wise deliberations of M. de Boer-Buquicchio have demonstrated:

> "E-Justice, in my view, can stand for equitable justice; it can stand for efficient justice, or even for enlightened justice, but certainly not for electronic justice. What makes justice just, after all, is human judgment, applying a democratically accepted set of abstract rules to a specific situation. This can be greatly helped, but cannot be replaced by information technology, so I would prefer to speak about e-courts, rather than e-justice."[9]

The presentation took these arguments into account by stipulating that, in Germany, we should write and speak about "E-Justiz" ("E-Rechtsstaat") instead of using the Anglo-Saxon term "E-Justice". The reason being that using the terminology "E-Justice" in the German legal system could be understood as "E-Gerechtigkeit". The queries of terminology prepare for further challenges. "E-Justiz" demands new scientific approaches including applied sciences as well as legally compatible pragmatism ("rechtserträglicher Pragmatismus"). There are new threats and challenges – as well as opportunities and advantages – for the judicial system that are connected with the use of information technology.[10] A systematic analysis of potential weaknesses is the first step to achieving an equal chance for justice in the traditional court system, as well as in an e-court (E-Justiz) system. This agenda is titled with the term "securitization" ("Versicherheitlichung") – knowing that there are other notions of "securitization" e.g. in political sciences or in economics.[11] In a nutshell: In order to use the advantages of information technology in such a data sensitive system as "E-Justiz" "we" should identify the homework for the lawmakers, as well as courts and lawyers. Hence, the temple architecture shown in Figure 1 was presented and its publication (with more detailed information than in this in short article) in May 2014 was announced:[12]

[9] V. Schmid, in: H. Sodan/J. Ziekow, § 173 marginal number 13 with further reference.
[10] E.g. "mobile justice" ("M-Justiz"), V. Schmid, in: H. Sodan/J. Ziekow, § 55a marginal number 9.
[11] Further research and publications are initiated.
[12] V. Schmid, in: H. Sodan/J. Ziekow, § 55a marginal number 106.

The roof of this temple needs jurisprudential deliberations (even if there should be regulation at all ("Grenzen des Rechts")) about the liability (accountability, responsibility) of "E-Justiz"-providers; about the communication of technological changes within the system (such as "Rechtsbehelfsbelehrung"[13], § 58 VwGO[14]) and about instruments that encourage and inform the "clients" (and in the future perhaps customers as well as patrons) of the "E-Justiz"-system (acceptance). The columns of this temple symbolize new challenges for technology as well as law: Such as challenges for (the law on) system administration, data retention without purpose limitation, video and audio surveillance and documentation and – last but not least – cybersecurity and cyberforensics. This last column is the inspiration for this presentation at a Dagstuhl seminar with the title: Digital Evidence and Forensic Readiness. And the underlying and fundamental question (in the literal sense of the temple metaphor) is: Which processes can be automated – and which do we reserve for human (inter)action? The identification of these challenges gave birth to the idea of a new cross-disciplinary approach and the creation of its name – the "LEXONOMICS"-perspective[15].

Second: LEXONOMICS. "LEXONOMICS" is the research motto and desired outcome of the future efforts of the Faculty of Law and Economics at the Technical University of Darmstadt, Germany (there the research formation on Governance, Compliance and Regulation with its speaker Prof. Dr. Dirk Schiereck). LEXONOMICS is a compound of the Latin "LEX" with the Anglo-Saxon "ECONOMICS". Latin "LEX“ also stands for the root of law in the history of law, and the Anglo-Saxon "ECONOMICS" refers to the interrelation of the legal and economic sciences in the future. From the "LEXONOMICS" perspective, the balancing test between "necessary effort" with "desired effect of protection" can be applied with new methods and insights. A first approach is § 9 BDSG[16] – the "Magna Carta" of IT security law in Germany – which has undergone firm establishment through new case law. A follow-up after the seminar exemplifies the potential and challenges for this "temple perspective" as well as "LEXONOMICS" regarding the second column:

Third: Follow-up of the seminar with the decision of the European Court of Justice from 8. April 2014. The second column of the temple architecture titled "Data retention without purpose limitation" was at dispute in the judgment of the *European Court (Grand Chamber), 8. April 2014, C-293/12 and C-594/12.* The court rendered the following decision:

> "Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC is invalid."[17]

A core area of (European Union) Cyberlaw, the law allocating chances and risks, rights and obligations in cyberspace, was "established" with this judgment. It is noteworthy that

[13] "Information on legal remedies available".

[14] V. Schmid, in: H. Sodan/J. Ziekow, § 55a marginal number 151 et seqq.

[15] V. Schmid, in: H. Sodan/J. Ziekow, § 173 marginal numbers 10 and 57.

[16] Federal Data Protection Act in the version promulgated on 14 January 2003 (Federal Law Gazette [Bundesgesetzblatt] Part I p. 66), as most recently amended by Article 1 of the Act of 14 August 2009 (Federal Law Gazette Part I p. 2814), in force from 1 September 2009. This Act serves to implement directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protec-tion of individuals with regard to the processing of personal data and on the free movement of such data (OJ EC no. L 281, p. 31 ff.); non authentic translations provided by the Language Service of the Federal Ministry of the Interior under http://www.gesetzeiminternet.de/englisch_bdsg/index.html.

[17] Judgment of the European Court (Grand Chamber), 8. April 2014, C-293/12 and C-594/12, marginal number 73.

all other member-states of the European Union (with the exception of Germany) might have acted unlawfully by implementing this European Directive.[18] The only member-state (still) not[19] implementing that Directive, the Federal Republic of Germany, even had to face an infringement proceeding[20] in 2012 (Art. 258 et seqq. Treaty on the Functioning of the European Union (TFEU)) instituted by the European Commission. This information sets up the importance of this judgment of the European Court of Justice in April 2014. Very rarely does the European Court of Justice declare European Union Law – here the *Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC*[21] – invalid. It is noteworthy that two organs of European Union Law (Art. 13 paragraph 1 Treaty on European Union (TEU)) had fundamentally different opinions concerning the European Union Law on data retention: The European Commission sued the Federal Republic of Germany for not implementing the Directive (Art. 258, 260 TFEU) whereas the European Court of Justice decided that the directive in dispute was unlawful. Not only the European Union Law was affected – "data retention law" also divided lawmakers and courts in Germany.

Moreover, in matters of IT Security Law (**"ITS-Law"**, acronym by the author) the European Court of Justice is in some aspects in line with the judgment of the highest German court, the Federal Constitutional Court, from March 2010. The legal issue in this decision was not European law, but German law, implementing the European directive (§ 113a, b TKG[22]. This Act serves to transpose the following Directives: Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) (OJ L 108 page 33); Directive 2002/20/EC of the European Parliament and of the Council of 7 March 2002 on the authori-sation of electronic communications networks and services (Authorisation Directive) (OJ L 108 page 21); , § 100g StPO[23]). Perhaps – that is remarkable from the "LEXONOMICS"-perspective – both courts declared IT-Security of **inestimable value** for digit(al)ization. In April 2014, the challenge is to compare and evaluate both approaches – the here so called "German" and the here so called "European Union" approach to IT-Security-Law (**"ITS-Law"**). The German Approach: The "magna carta" in German data-protection and IT-Security-Law is traditionally § 9 sentence 1 BDSG and annex and § 9 sentence 2 BDSG. This provision is so relevant that it is presented here:[24]

[18] Further research is initiated

[19] In retrospect in 2014: The German Government and Parliament tried to implement the Directive. A groundbreaking decision of the German Federal Constitutional Court in 2010 declared this implementation as unconstitutional.

[20] Action brought on 11 July 2012 – European Commission v Federal Republic of Germany (Case C-329/12).

[21] Official Journal L 105, 13/04/2006, P. 0054–0063.

[22] Telecommunications Act (Telekommunikationsgesetz – TKG) in the version promulgated on 22 June 2004 (Federal Law Gazette Part I p. 1190), as most recently amended by Article 4 subsection (108) of the Act of 7 August 2013 (Federal Law Gazette Part I p. 3154)

[23] Code of Criminal Procedure (Strafprozessordnung – StPO) in the version promulgated on 7 April 1987 (Federal Law Gazette Part I p. 1074, 1319), as most recently amended by Article 5 subsection (4) of the Act of 10 October 2013 (Federal Law Gazette Part I p. 3799); non authentic translations provided by the Language Service of the Federal Ministry of the Interior under http://www.gesetze-im-internet.de/englisch_stpo/.

[24] Accentuation by the author.

§ 9 BDSG [Technical and organizational measures]

Public and private bodies which collect, process or use personal data on their own behalf or on behalf of others shall take the necessary technical and organizational measures to ensure the implementation of the provisions of this Act, especially the requirements listed in the Annex to this Act. **Measures shall be necessary only if the effort required is in reasonable proportion to the desired purpose of protection.**

Annex (to § 9 sentence 1)

Where personal data are processed or used in automated form, the internal organization of authorities or enterprises is to be such that it meets the specific requirements of data protection. In particular, measures suited to the type of personal data or categories of data to be protected shall be taken

1. to prevent unauthorized persons from gaining access to data processing systems for processing or using personal data (access control),
2. to prevent data processing systems from being used without authorization (access control),
3. to ensure that persons authorized to use a data processing system have access only to those data they are authorized to access, and that personal data cannot be read, copied, altered or removed without authorization during processing, use and after recording (access control),
4. to ensure that personal data cannot be read, copied, altered or removed without authorization during electronic transfer or transport or while being recorded onto data storage media, and that it is possible to ascertain and check which bodies are to be transferred personal data using data transmission facilities (disclosure control),
5. to ensure that it is possible after the fact to check and ascertain whether personal data have been entered into, altered or removed from data processing systems and if so, by whom (input control),
6. to ensure that personal data processed on behalf of others are processed strictly in compliance with the controller's instructions (job control),
7. to ensure that personal data are protected against accidental destruction or loss (availability control),
8. to ensure that data collected for different purposes can be processed separately.

Traditionally, § 9 sentence 2 BDSG established that the level of IT-Security is the result of a balancing test between effort ("Aufwand") and effect ("angestrebter Schutzzweck"). In 2010, the German Federal Constitutional Court insisted for **German Constitutional Law** on a **particularly high standard of IT-Security** for the collection, storage, transmission and usage (processing) of telecommunication traffic data ("besonders hoher Sicherheitsstandard")[25], see also Press release no. 37/2008 of 19 March 2008, http://www.

[25] BVerfG, Urteil vom 02.03.2010, Az 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, http://www.bverfg.de/entscheidungen/rs20100302_1bvr025608.html, see also Press release no. 11/2010 of 2 March 2010, http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg10-011en.html; BVerfG, 1 BvR 256/08 vom 11.3.2008 (application for a temporary injunction in the matter of "data retention"), http://www.bverfg.de/entscheidungen/rs20080311_1bvr025608.html. BVerfG, Urteil vom 02.03.2010, Az 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08:
Leitsatz 4:
"Hinsichtlich der Datensicherheit bedarf es Regelungen, die einen **besonders hohen Sicherheitsstandard** normenklar und verbindlich vorgeben. Es ist jedenfalls dem Grunde nach gesetzlich sicherzustellen, dass sich dieser an dem Entwicklungsstand der Fachdiskussion orientiert, neue Erkenntnisse und Einsichten fortlaufend aufnimmt und nicht unter dem Vorbehalt einer freien Abwägung mit allgemeinen

bundesverfassungsgericht.de/pressemitteilungen/bvg08-037en.html.

In April 2014, the European Court of Justice insisted for **European Union Law** (Directive 2006/24/EC) also on a **particularly high standard of IT-Security** for the collection, storage, transmitting and usage (processing) of telecommunication traffic-data. Furthermore, the European Court explicitly **rejected the notion of a balancing test** between effort and effect:

> Moreover, as far as concerns the rules relating to the security and protection of data retained by providers of publicly available electronic communications services or of public communications networks, it must be held that Directive 2006/24 **does not provide for sufficient safeguards**, as required by Article 8 of the Charter, **to ensure effective protection** of the data retained against the risk of abuse and against any unlawful access and use of that data. In the first place, Article 7 of Directive 2006/24 does not lay down rules which are specific and adapted to (i) the vast quantity of data whose retention is required by that directive, (ii) the sensitive nature of that data and (iii) the risk of unlawful access to that data, **rules which would serve, in particular, to govern the protection and security of the data in question in a clear and strict manner in order to ensure their full integrity and confidentiality**. Furthermore, a specific obligation on Member States to establish such rules has also not been laid down.
>
> Article 7 of Directive 2006/24, read in conjunction with Article 4(1) of Directive 2002/58 and the second subparagraph of Article 17(1) of Directive 95/46, does not ensure that a particularly high level of protection and security is applied by those providers by means of technical and organisational measures, **but permits those providers in particular to have regard to economic considerations when determining the level of security** which they apply, as regards the costs of implementing security measures. [. . .][26]

As a consequence, the legal standards for IT-Security concerning telecommunication traffic-data have to be analyzed and discussed in the near future. There is the German model (§ 9 sentence 1 and annex and sentence 2 BDSG) and the hitherto European model of the legislation (see below) with the balancing test of effort and effect (“erforderlicher Aufwand und angestrebter Schutzzweck”) on one hand and new case law (“Rechtsprechung”) of the German Federal Constitutional Court and the European Court of Justice on the other hand – both postulating a very high standard of IT Security. There might be different IT Security Law (**“ITS-Law”**) perceptions in legislation and in judiciary. As mentioned above, the balancing test in European (Union) Law is established with the following articles:[27]

wirtschaftlichen Gesichtspunkten steht.“ (accentuation by the author).
Randnummer 222:
Angesichts des Umfangs und der potentiellen Aussagekraft der mit einer solchen Speicherung geschaffenen Datenbestände ist die Datensicherheit für die Verhältnismäßigkeit der angegriffenen Vorschriften von großer Bedeutung. Dieses gilt besonders, weil die Daten bei privaten Diensteanbietern gespeichert werden, die unter den Bedingungen von Wirtschaftlichkeit und Kostendruck handeln und dabei nur begrenzte Anreize zur Gewährleistung von Datensicherheit haben. Sie handeln grundsätzlich privatnützig und sind nicht durch spezifische Amtspflichten gebunden. Zugleich ist die Gefahr eines illegalen Zugriffs auf die Daten groß, denn angesichts ihrer vielseitigen Aussagekraft können diese für verschiedenste Akteure attraktiv sein. Geboten ist daher ein **besonders hoher Sicherheitsstandard**, der über das allgemein verfassungsrechtlich gebotene Maß für die Aufbewahrung von Daten der Telekommunikation hinausgeht. Solche Anforderungen der Datensicherheit gelten dabei sowohl für die Aufbewahrung der Daten als auch für deren Übermittlung; ebenso bedarf es effektiver Sicherungen zur Gewährleistung der Löschung der Daten.“ (accentuation by the author).

[26] Judgment of the European Court (Grand Chamber), 8. April 2014, C-293/12 and C-594/12, marginal numbers 66, 67.

[27] Accentuation by the author.

Article 7 DIRECTIVE 2006/24/EC[28][**Data protection and data security**]
Without prejudice to the provisions adopted pursuant to Directive 95/46/EC and Directive 2002/58/EC, each Member State shall ensure that providers of publicly available electronic communications services or of a public communications network respect, as a minimum, the following data security principles with respect to data retained in accordance with this Directive:

(a) the retained data shall be of the same quality and subject to the same security and protection as those data on the network;

(b) the data shall be subject to appropriate technical and organisational measures to protect the data against accidental or unlawful destruction, accidental loss or alteration, or unauthorised or unlawful storage, processing, access or disclosure;

(c) the data shall be subject to appropriate technical and organisational measures to ensure that they can be accessed by specially authorised personnel only;

and

(d) the data, except those that have been accessed and preserved, shall be destroyed at the end of the period of retention.

Article 4(1) DIRECTIVE 2002/58/EC[29][**Security**]

1. The provider of a publicly available electronic communications service must take**appropriate technical and organisational measures** to safeguard security of its services, if necessary in conjunction with the provider of the public communications network with respect to network security. Having regard to the state of the art and the cost of their implementation, these measures shall ensure **a level of security appropriate to the risk** presented.

Article 17(1) Directive 95/46/EC[30][**Security of processing**]

1. Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Having regard to the state of the art and the cost of their implementation, such measures shall ensure **a level of security appropriate to the risks** represented by the processing and the nature of the data to be protected.

These are prerogatives and prerequisites for digit(al)ization and therefore challenges that "LEXONOMICS" might master.

[28] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, Official Journal L 105, 13/04/2006, P. 0054–0063.

[29] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), Official Journal L 201 , 31/07/2002 P. 0037 – 0047.

[30] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the pro-tection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281 , 23/11/1995 P. 0031–0050.

References

German literature and references about "Informatisierung" (as at February 2014) can be found in *Schmid*, V., in: H. Sodan/J. Ziekow, Großkommentar zur Verwaltungsgerichtsordnung, 4th Edition 2014, §§ 55a and b (soon to be published).
The provided literature is German-language and not Anglo-Saxon. Nevertheless, three very renowned authors are recommended here (in alphabetic order):

- *Berlit, U.*, Elektronischer Rechtsverkehr – eine Herausforderung für die Justiz, JurPC Web-Dok. 173/2013, Abs. 1–50;
- *Herberger, M.*, Zehn Anmerkungen zum "Gesetz zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten", JurPC Web-Dok. 81/2013, Abs. 1–66;
- *Köbler, R.*, Der elektronische Rechtsverkehr kommt; Fahrplan bis 2022 steht, AnwBl 2013, 589.

3.14 ICT Policy in Norwegian Industries

Rhythm Suren Wadhwa (Gjøvik University College, NO)

This abstract discusses ICT policy in the Norwegian industrial context. Norway was able to move from an agro-based economy to an industrial one within a single generation. The public sector acted both as a facilitator and a pace-setter with the private sector driving the economic development. Since ICT accelerates information & knowledge development and consumption, ICT, by default, was seen as the key driver of future growth in all phases of work & life. In national development, ICT can be said to play a dual role; one, as a production sector to achieve development goals and value creation; and two as an enabler in moving towards knowledge society and knowledge economy. A migration strategy towards attaining the objective of attaining competitiveness and equity were identified to provide overall guidance for the development: ICT as a sector and information as a commodity; value creating knowledge products and services; and competitive knowledge economy. Two major initiatives to address issues of economic competitiveness and social equity were in taking ICT development as a sector and as an enabler. The policy framework delineates strategic, tactical and operational aspects of policy intervention. Some of the lessons learnt are that visionary leadership and championship are necessary to provide vision and motivation, and to see projects to the end; academia-industry partnership and innovation clusters are a must to move fast and a planned approach is a must. A top-down strategic intervention becomes imperative to attain a benchmark position.

4 Working Groups

4.1 Digital forensic readiness processes and procedures for investigators

Hein Venter (University of Pretoria, ZA)

Well-documented processes are required for digital forensic readiness. Such processes can help to define detailed procedures that can be used in the rest of the digital forensic investigation process as portrayed in ISO27043. Following is a non-exhaustive list of typical processes that can be included for digital forensic readiness:

- Creation of audit logs
- Retention of audit logs
- Processing of logs
- Presentation of the logs
- Correlation of logs
- Transmission of logs
- Validation of logs

For example, consider the following scenario. Suppose a bank implements the processes as discussed above. Further, suppose that it is alleged that an employee of the bank leaked confidential information to a competitor bank via email.

Assume that the bank had policies in place to implement the processes as defined above. For example, the email server of the bank retains all emails sent. The firewall logs all incoming and outgoing network traffic and logs that an email with an attachment was sent to an unusual email address – that of the competitor bank. Some log correlation between the email and firewall servers' logs are automatically done by a log correlation system. A flag is raised by the intrusion detection system of the bank, warranting for a potential investigation to follow.

With the digital forensic readiness processes in place, the above was possible. Assume that there is now an enquiry launched into the allegations. However, without the above information, a digital forensic investigator will have to follow the normal digital forensic investigation process as stated in ISO27043. This entails the following processes to be followed:

- Prepare for the investigation (e.g. obtain authorization, such as to obtain a search warrant)
- Seize the employee's PC
- Acquire the hard drive from the PC
- Analyze the data for potential evidence and continue with the rest of the processes described in ISO27043

Remember that the above processes have been followed as if there were no digital forensic readiness processes in place. Should these processes be in place, however, the investigator need not follow all of the processes in ISO27043 as described above. This is so because the evidence required would have already been logged and the investigator need only to get authorization after which he can already start with the analysis of the data already available in log correlation system. The obvious advantage is that much time and cost is saved in this situation. What is more, the investigator have access to several other logs created by the digital forensic readiness system. Detailed procedures should then be defined in order to enhance each of the digital forensic investigation processes found in ISO27043. For example, now that more log data is available, detailed procedures can be defined on how to access the particular logs in order to identify even more compelling evidence.

4.2 Notion of Digital Evidence

Isabel Taylor (Universiät Tübingen, DE)

4.2.1 Authorship

The editor of this abstract would like to thank Nigel Wilson, Carsten Momsen, Raymond Choo, Stefanie Gerdes, Rhythm Suren Wadhwa, Christian Moch, Lee Tobin and Nils-Peter Hercher, as well as the members of the Definitions and Concepts Working Group – Viola Schmid, Thomas Kemmerich, Barbara Endicott-Popovsky, Aaron Alva, and Günther Diederich – for their valuable contributions and insights during the writing of this section.

4.2.2 The definitional problem

Terminology determines the way we perceive the world. We cannot engage in a meaningful discourse if we cannot agree on the definitions of terms. The concept of definition is the filter through which our understanding of solutions and outcomes is defined, but definitions are inevitably contextual, language-based and fluid. Glossaries are an important means of collating consistent terminology, but there are often difficulties with over-definition, particularly by non- subject specialists and in non-dynamic environments. The same terms may be defined in subtly different ways across different disciplines, which can lead to confusion in interdisciplinary discussions. The differences between the definitions may in some cases be profound, such as (for example) the definition of 'data' in ICT versus its definition in the 1995 Data Protection Directive. However, we acknowledge the important glossary projects that are ongoing outside the scope of this project.

4.2.3 Legal terminology

The current definitions in the literature are specific to a local area, and this is acutely so in law, because it is procedural and jurisdiction based. For example, 'privacy', which is highly relevant in the German environment – in terms of admissibility and forensics – has different legal impacts in different jurisdictions, and differing definitions.

Evidence provides a particularly good example of different categorisations having different legal effects and outcomes. These categorisations have both substantive and procedural (adjectival) implications. Depending on the jurisdiction, the categories of evidence are defined differently and the breadth and significance of the categories also varies. For example, the common law system makes a conceptual distinction between real (traditionally, physical) evidence and documentary evidence. Digital evidence bridges both categories. By contrast, categories of evidence have less impact on admissibility in the German system, where digital records often fall into the Augenscheinsbeweis ("visual inspection") category, such as a USB stick, or Urkundenbeweis (documentary evidence), i.e. the documents on the USB stick.

Additionally, 'soft law' such as the ISO standards influences the manner in which terms are understood, both within the regulatory environment and in practice. For example,'information assurance' has been defined by ISO 27001.

4.2.4 ICT

Information and Communication Technologies (ICT) presents its own particular set of challenges: indeed, the foundation of ICT is "language-based." Coupled with this is the fast pace of technological change. The terminology needs to be updated constantly, since new terms and buzzwords are always emerging: for example, "big data," or the "Internet of things." Sometimes there is a lack of consensus on the meanings of terms, such as "digital". File location has a particular meaning in the ICT forensic context, and some expressions, like "hash," or "byte," only have meaning in this particular discipline, and require 'translation' to be understood by those in other disciplines. The magnitude and dimension of ICT terms pose a particular conceptual challenge for those outside the area: for example, the conception of a terabyte of information, often requiring explanation by means of (often unsatisfactory) analogy to lay audiences. This has particular relevance when regulations or standards are developed that impact the ICT field: a common problem is the lack of understanding, on the part of legal specialists, of ICT-specific terms.

4.2.5 Archival terms

Since archival science is concerned with the preservation of documents that can be shown to be authentic, reliable and accurate– a function which derives from its roots in the legal world– its concepts and terminology are helpful to discussions of digital evidence. In particular, archival theory provides a set of conceptual parameters which assist in identifying "records" within the digital environment, and a definition of "trustworthiness" (the authenticity, reliability and accuracy of a document) which can help to inform the assessment of digital evidence. Archival science shares terms with both the legal and ICT fields. For example, the archival idea of the chain of custody has an analogue in the similar legal concept, often applied to police exhibits, while ICT and archival science both share an emphasis on metadata. Archival science provides essential concepts which can inform system requirements for the preservation of records' evidential value: classical concepts such as provenance (the history of the custody of the records and the way this has changed over time) and respect des fonds (the management of records based on creator) continue to inform digital archivists and are clearly relevant to the new digital environment.

4.2.6 Research projects

The interdisciplinary work in this and other working groups was accompanied by a constant discussion on definitions, concepts and notions in digital evidence and forensic readiness. In addition to this working group, a dedicated working group on "Definitions and Concepts" aimed at defining the gap between the different areas of expertise. A summary of their intermediate results has been integrated into this report in order to present a whole view on notions, definitions and concepts.

In discussions concerning seemingly well-defined terms, the need for a unified glossary soon became evident. In order to start on this extensive task, the working group on "Definition and concepts" developed a methodology for input on glossary terms. First, they focused on collecting terms. Second, they differentiated between "clear" and "hard" cases for the terms collected. Third, they determined to do research in legal and technological sources. Fourth, they decided to refer to the "Origins of Evidence" group for a discussion of terms' history: adopting this coordination and cooperation strategy, they exchanged ideas with break-up teams on alternative perspectives and methods. Fifth, they proposed to start a matrix of legal sources, initially focusing on European Law, German Law, and Common

Law. Sixth, they pointed out that the methodology provides non-exhaustive research as a starting-point, but the community's input is needed to add depth and perspective from each area of expertise involved in forensic readiness.

With the differing area-specific definitions revealed in the discussion of the "Definitions and Concepts" working group, the need for a unified Glossary soon became evident. Therefore the "Notion of Digital Evidence" group recommends a commitment to definitively establishing the definition and parameters of the term "forensic readiness" and to this end:

- the development of a multi-regional glossary, including ICT, law and archives, to enable the identification of definitions relating to digital evidence that work across the disciplines and jurisdictions
- a multi-lingual collection of precedents that define relevant terminology, particularly those that sum up the state of the art, with a commentary in English.

4.2.7 Strategies

Increase consultation between the different disciplines and internationally. Begin an open dialogue between ICT and policy-makers, relevant industry, and government administration, so that policy-makers are informed of emerging technological challenges to the existing law. Develop catalogues of criteria for the creation, preservation and use of digital evidence, to increase certainty about the state of forensic readiness in a given situation.

4.3 Forensic readiness landscape

Hein Venter (University of Pretoria, ZA)

Joint work of Valjarevic, Aleksandar; Venter, Hein S.; Forte, Dario

There are, at the time of writing this paper, many standardization initiatives happening within many standardization bodies with regards to standardization of the digital forensic investigation process. Perhaps one of the most comprehensive standardization efforts currently happens within ISO. ISO27043 is the so-called umbrella standard, covering the width of the entire digital forensic investigation process.

ISO27043 provides guidelines that encapsulate idealized models for common digital forensic investigation processes across various investigation scenarios. This includes processes from digital forensic readiness up to and including investigation closure. A basic principle of digital forensic investigations is repeatability, where a suitably-skilled investigator should be able to obtain the same result as another similarly-skilled investigator, working under similar conditions. This principle is exceptionally important to any general investigation. Guidelines for many investigation processes have been provided in the standard in order to ensure that there is clarity and transparency in obtaining the produced result for each particular process.

Established guidelines covering digital forensic investigation principles and processes would expedite investigations, because they would provide a common order of the events that an investigation entails. Using established guidelines allows smooth transition from one event to another during an investigation. Such guidelines would also allow proper training of inexperienced investigators. The guidelines, furthermore, aim to ensure flexibility within an investigation due to the fact that many different types of digital investigations are possible, such as computer forensics (investigations on PCs), mobile phone (smart device) forensics, network forensics, cloud forensics (a kind of network forensics), and live forensics (i.e. volatile memory forensics).

By the time of writing, ISO27043 was still in a draft, yet nearly finalized, state. The need within the digital forensic investigation community is widely acknowledged for the establishment of a harmonized digital forensic investigation process model, however, both in a criminal prosecution setting and in other environments, such as corporate breaches of information security. Such harmonized incident investigation principles and processes are specified within the standard and indications are provided of how the investigation processes can be customized in different investigation scenarios.

The provided guidelines give succinct guidance on the exact process to be followed during any kind of digital forensic investigation in such a way that, if challenged, no doubt should exist as to the correctness of the investigation process followed during such an investigation.

Any digital investigation requires a high level of expertise. Those involved in the investigation should be competent, proficient in the processes used, and they should use processes which are compatible with the relevant policies and/or laws in various jurisdictions across the world.

Where the need arises to assign a process to a person, that person will take the responsibility for the process. Therefore, a strong correlation between a process responsibility and a person's input will determine the exact investigation process required according to the harmonized investigation processes provided as guidelines in ISO27043.

ISO27043 is intended to complement other standards and documents which give guidance on the investigation of, and preparation to investigate, information security incidents. It is not a comprehensive guide, but lays down certain fundamental principles which are intended to ensure that tools, techniques and methods can be selected appropriately and shown to be fit for purpose should the need arise. The standard also intends to inform decision-makers that need to determine the reliability of digital evidence presented to them. It is applicable to organizations needing to protect, analyze and present potential digital evidence. It is relevant to policy-making bodies that create and evaluate procedures relating to digital evidence, often as part of a larger body of evidence.

ISO27043 describes part of a comprehensive investigative process which includes, but is not limited to, the application of the following related standards. Note that, at the time of writing, all parts of this standard were in development, except for ISO27037, which was published in 2012.

- ISO27035: Information security incident management. This is a three part standard that provides organizations with a structured and planned approach to the management of security incidents. It is composed of three parts:
  - Part 1: Principles of incident management.
  - Part 2: Guidelines to plan and prepare for incident response.
  - Part 3: Guidelines for incident response operations.
- ISO27037: Guidelines for the identification, collection, acquisition and preservation of digital evidence.
- ISO27038: Specification for digital redaction.
- ISO27040: Storage security.
- ISO27041: Guidance on assuring the suitability and adequacy of incident investigation methods.
- ISO27042: Guidelines for the analysis and interpretation of digital evidence.
- ISO27044: Guidelines for Security Information and Event Management (SIEM).
- ISO27050: Electronic discovery.
- ISO30121: Governance of digital forensic risk framework.

The digital investigation processes of ISO27043 are multi-tiered, where each process would contain a set of sub-processes. Sub-processes can only be fully defined for a specific type of incident and investigation. Legal rules will also likely have a high impact on the definition of sub-processes. Digital investigation processes can be categorized into the following digital investigation process classes:

- readiness processes: That class of processes dealing with pre-incident investigation processes. This class deals with defining strategies which can be employed to ensure systems are in place, and that the staff involved in the investigative process are proficiently trained prior to dealing with an incident occurring. The readiness processes are optional to the rest of the digital investigation processes. Readiness processes include the following:
- planning and definition of system architectures for establishing digital forensic readiness;
- implementing digital forensic readiness system architecture;
- assessment of implementation;
- initialization processes: That class of processes dealing with the initial commencement of the digital investigation. Initialization processes include the following:
- incident detection;
- first response;
- planning;
- preparation.
- acquisitive processes: That class of processes dealing with the physical investigation of a case where potential digital evidence is identified and handled. Acquisitive processes include the following:
- potential digital evidence identification;
- potential digital evidence acquisition;
- potential digital evidence transportation;
- potential digital evidence storage.
- investigative processes: That class of processes dealing with uncovering the potential digital evidence. Investigative processes include the following:
- potential digital evidence examination and analysis;
- digital evidence interpretation;
- reporting;
- presentation;
- investigation closure.
- concurrent processes: That class of processes that continues concurrently alongside the other processes. This class of processes differ from the previous classes in the sense that they happen in tandem with the other processes instead of linear. In addition, the particular order in which the concurrent processes execute is irrelevant as opposed to the other non-concurrent processes. Concurrent processes include the following:
- obtaining authorization;
- documentation;
- managing information flow;
- preserving chain of custody;
- preserving digital evidence;
- interaction with the physical investigation.

The six concurrent processes are aimed at allowing the said processes to be executed as on-going processes. The reason for having the concurrent processes is mainly to ensure more effective admissibility of digital evidence into a legal system, since, in the case of not having such processes, any investigation may run the risk that the admitted potential evidence might not be suitable for litigation due to improper handling and documentation of potential digital evidence. These concurrent processes are, thus, based on principles that need to be followed throughout a digital investigation, alongside with the other classes of processes.

References

1 Hein S. Venter (Ed.). *ISO/IEC DIS 27043: Information technology – Security techniques – Incident investigation principles and processes.* ISO Draft International Standard

4.4 Forensic readiness: evidence in the digital world

Joe Cannataci (University of Malta, MT)

4.4.1 Landscape: the legal landscape for the treatment of evidence – Joe Cannataci

Evidence can take many forms: it may be a bullet or a blood-stained shirt or some such tangible three-dimensional object which is not digital but which may also be captured digitally whether through a two or 3D image or through a document which describes the artefact. It may be one or more documents which were created in a written or printed form most often on paper and which are also capable of being captured digitally in facsimile. It may also take the form of correspondence or publications or records of transactions which were "born digital" such as a word-processed document or e-mail or other user-generated content in an on-line environment or indeed digital photographs. Many "born digital" records would also largely consist of transactional data or traffic data such as telephone records or credit card records or electricity bills. Almost by definition most items which end up as evidence whether digital or non-digital were not intended to be used as evidence when they were created. Their use as evidence is secondary to their primary purpose, to their real "raison d'etre". Whether non-digital or digital evidence, the role of a bullet or a paper document or an e-mail as evidence is one which comes in at a later stage, when the artefact or record could help prove that an allegation about human behavior is true or false. In this sense historically there was no such thing as forensic readiness. Forensic sciences were developed to obtain information from artefacts and records which were most often never designed ab initio to in any way assist the forensic process in a court of law. Indeed an artefact or a record enters into the forensic process only if an incident, (criminal, civil or commercial) forces it to do so. Otherwise, for all of its natural lifespan the artefact or record will remain outside the forensic process and thus forensically irrelevant – though it may continue to be very relevant to its user or owner. The introduction of ICTs into the "forensic food chain" over the past forty years or so (much less in some countries) have led to more and more evidence being stored, transmitted and managed in a digital manner. It should be borne in mind that evidence is not only collected, processed and stored in those stages before a case is hear in court. More and more evidence is generated in the course of most court hearings with witnesses being recorded and their testimony entered into the official court record, irrespective of whether a case is criminal or civil. In a properly-organised e-justice or e-court system – indeed in most manual systems too – each new piece of testimony or evidence is allocated a new unique identifier which accompanies it and stays with it for the duration of the court proceedings and normally after these are completed too.

The ICT systems used by courts of law, administrative tribunals, land registries, public registries, public prosecutors, private law firms and solo law practitioners have grown organically over the years since they first started appearing in the 1970s. More often than not legal information retrieval systems and case management systems were not designed and developed according to some regional, national or international master-plan. Instead, most often, they grew higgledy-piggledy depending on the initiative, resources and resourcefulness of the actors in the local legal scene. Some courts and law firms in some countries computerized at a much faster rate than others in the same country or outside that country. Some forty years after "legal informatics" appeared on the scene in Europe the results and levels of computerization in different countries varies considerably. The disparity in the capability of different systems creates significant obstacles to the portability of evidence across different jurisdictions within and outside Europe thus contributing to delays and increase in costs of legal proceedings. This has led to a perceived need in the European Union context to have a Common Framework regulating the implementation of ICTs in the use, collection and exchange of evidence in criminal trials. However, legislation on criminal procedures in many European countries were enacted before these technologies appeared, thus taking no account of them and creating a scenario where criteria are different and uncertain, regulations are not harmonised and aligned and therefore exchange among EU countries jurisdictions, at transnational level, is very hard to be achieve in practice. What is also missing is a Common European Framework to guide policy makers, Law Enforcement Agencies (LEAs), judges/magistrates as well as lawyers and prosecutors when dealing with digital evidence treatment and exchange. From a European perspective this situation has led to the European Commission in 2014 making some limited funds available for the preliminary steps to be taken to create an evidence base and a roadmap for policy makers to attempt to find means to resolving the problems intrinsic to the fragmentation which characterizes legal informatics across the court systems in 28 EU member states. The EVIDENCE project sets out to plug part of the gap that is the missing common legal layer devoted to the regulation of electronic evidence in courts. A common guide identifying the value to be assigned to electronic evidence all over EU Member states, common criteria for reliability of electronic evidence independently from the country or LEA by which is gathered, reliability, validity and integrity of the electronic proof, and so forth. It also seeks to investigate the common background for all policy makers that must regulate the use of electronic evidence in their national scenario, for LEAs and other major actors in gathering electronic evidence, for judges, magistrates evaluating such electronic evidence in trials, for prosecutors and for lawyers, using electronic evidence for conducting someone's defence. Given the limited funding available, the EVIDENCE Project restricts itself to a number of basic initial steps: first of all at developing a road map (guidelines, recommendations, technical standards, research agenda) aimed at creating a Common European Framework for the systematic, aligned and uniform application of new technologies in the collection, use and exchange of evidence. By defining the Road map it will also discuss the treatment of evidence gathered by using new technologies, the specific rules and criteria for treatment of both digitized and born-digital evidence, what are the implications for privacy and ethical issues and finally, which are the conditions for a secure and consistent exchanging of evidence collected by means of new technologies. In the United States The Sedona Conference®, claims to be the pre-eminent thought leader in eDiscovery, and is in spring 2014 organising a regional program on Cross-Border Discovery and Data Protection Laws. The conference is being held in conjunction with Sedona's Working Group 6 on International Electronic Information Management, Discovery and Disclosure. Despite the International in the name it appears fair to say that Sedona remains a very US-centric affair with limited international impact. On the other hand it is reported that within the United States the guidelines published by Sedona in this field are widely respected and followed. The interdisciplinary specialists meeting within Dagstuhl Seminar 14092 together created the illustration of the iter of various categories of non-digital and digital evidence through the forensic process as illustrated in Fig 0. Onto this flow-chart they then mapped on existing efforts at introducing digital forensics standards such as ISO/IEC 27037, 27041, 27042 and 27043 in particular which are in the process of being created to promote good practice forensic investigation involving digital evidence. The extent to which the proposed new standard 27043 fitted legal realities is described in the section on ISO 27043 below. The quality of digital records was then also discussed from the perspective of archival sciences. In summary it was agreed that archival sciences may contribute to the treatment of digital and non-digital evidence in three main ways:

1. By optimizing the design of new corporate or public IT systems at the record-creation, management and preservation stages
2. By optimizing new e-court or e-justice systems and help them move to "ideal record form"
3. By maximising the utility of diplomatics – archival diplomatics may be useful in analysis in a retrospective way esp for existing records which were not designed to ideal record form.

The way that archival sciences may contribute to the process is described in more detail in the relative section below. Finally, the working group also discussed the current status quo from the perspective of It security professionals which is also briefly outlined in the relative section below.

4.4.2 Standardisation efforts and ISO – Hein S. Venter

There are, at the time of writing this paper, many standardization initiatives happening within many standardization bodies with regards to standardization of the digital forensic investigation process. Perhaps one of the most comprehensive standardization efforts currently happens within ISO. ISO27043 is the so-called umbrella standard, covering the width of the entire digital forensic investigation process. ISO27043 provides guidelines that encapsulate idealized models for common digital forensic investigation processes across various investigation scenarios. This includes processes from digital forensic readiness up to and including investigation closure. A basic principle of digital forensic investigations is repeatability, where a suitably-skilled investigator should be able to obtain the same result as another similarly-skilled investigator, working under similar conditions. This principle is exceptionally important to any general investigation. Guidelines for many investigation processes have been provided in the standard in order to ensure that there is clarity and transparency in obtaining the produced result for each particular process. Established guidelines covering digital forensic investigation principles and processes would expedite investigations, because they would provide a common order of the events that an investigation entails. Using established guidelines allows smooth transition from one event to another during an investigation. Such guidelines would also allow proper training of inexperienced investigators. The guidelines, furthermore, aim to ensure flexibility within an investigation due to the fact that many different types of digital investigations are possible, such as computer forensics (investigations on PCs), mobile phone (smart device) forensics, network forensics, cloud forensics (a kind of network forensics), and live forensics (i.e. volatile memory forensics). By the time of writing, ISO27043 was still in a draft, yet nearly finalized, state. The need within the digital forensic investigation community is widely acknowledged for the establishment of a harmonized digital forensic investigation process model, however, both in a criminal prosecution setting and in other environments, such as corporate breaches of information security. Such harmonized incident investigation principles and processes are specified within the standard and indications are provided of how the investigation processes can be customized in different investigation scenarios.

The provided guidelines give succinct guidance on the exact process to be followed during any kind of digital forensic investigation in such a way that, if challenged, no doubt should exist as to the correctness of the investigation process followed during such an investigation.

Any digital investigation requires a high level of expertise. Those involved in the investigation should be competent, proficient in the processes used, and they should use processes which are compatible with the relevant policies and/or laws in various jurisdictions across the world. Where the need arises to assign a process to a person, that person will take the responsibility for the process. Therefore, a strong correlation between a process responsibility and a person's input will determine the exact investigation process required according to the harmonized investigation processes provided as guidelines in ISO27043. ISO27043 is intended to complement other standards and documents which give guidance on the investigation of, and preparation to investigate, information security incidents. It is not a comprehensive guide, but lays down certain fundamental principles which are intended to ensure that tools, techniques and methods can be selected appropriately and shown to be fit for purpose should the need arise. The standard also intends to inform decision-makers that need to determine the reliability of digital evidence presented to them. It is applicable to organizations needing to protect, analyze and present potential digital evidence. It is relevant to policy-making bodies that create and evaluate procedures relating to digital evidence, often as part of a larger body of evidence. ISO27043 describes part of a comprehensive investigative process which includes, but is not limited to, the application of the following related standards. Note that, at the time of writing, all parts of this standard were in development, except for ISO27037, which was published in 2012.

- ISO27035: Information security incident management. This is a three part standard that provides organizations with a structured and planned approach to the management of security incidents. It is composed of three parts:
  - Part 1: Principles of incident management.
  - Part 2: Guidelines to plan and prepare for incident response.
  - Part 3: Guidelines for incident response operations.
- ISO27037: Guidelines for the identification, collection, acquisition and preservation of digital evidence.
- ISO27038: Specification for digital redaction.
- ISO27040: Storage security.
- ISO27041: Guidance on assuring the suitability and adequacy of incident investigation methods.
- ISO27042: Guidelines for the analysis and interpretation of digital evidence.
- ISO27044: Guidelines for Security Information and Event Management (SIEM).
- ISO27050: Electronic discovery.
- ISO30121: Governance of digital forensic risk framework.

Figure 2 shows typical activities surrounding an incident and its investigation. The numbers shown on this diagram (e.g. 27037) indicate the respective international standards listed above, and the shaded bars show where each is most likely to be directly applicable or has some influence over the investigative process (e.g. by setting policy or creating constraints). It is recommended, however, that all should be consulted prior to, and during, the planning and preparation phases. The process classes shown are defined fully in ISO27043 and the activities identified match those discussed in more detail in ISO27035, ISO27037, and ISO27042.

The digital investigation processes of ISO27043 are multi-tiered, where each process would contain a set of sub-processes. Sub-processes can only be fully defined for a specific type of incident and investigation. Legal rules will also likely have a high impact on the definition of sub-processes. Digital investigation processes can be categorized into the following digital investigation process classes:

- readiness processes: That class of processes dealing with pre-incident investigation processes. This class deals with defining strategies which can be employed to ensure systems are in place, and that the staff involved in the investigative process are proficiently trained prior to dealing with an incident occurring. The readiness processes are optional to the rest of the digital investigation processes. Readiness processes include the following:
- planning and definition of system architectures for establishing digital forensic readiness;
- implementing digital forensic readiness system architecture;
- assessment of implementation;
- initialization processes: That class of processes dealing with the initial commencement of the digital investigation. Initialization processes include the following:
- incident detection;
- first response;
- planning;
- preparation.
- acquisitive processes: That class of processes dealing with the physical investigation of a case where potential digital evidence is identified and handled. Acquisitive processes include the following:
- potential digital evidence identification;
- potential digital evidence acquisition;
- potential digital evidence transportation;
- potential digital evidence storage.
- investigative processes: That class of processes dealing with uncovering the potential digital evidence. Investigative processes include the following:
- potential digital evidence examination and analysis;
- digital evidence interpretation;
- reporting;
- presentation;
- investigation closure.
- concurrent processes: That class of processes that continues concurrently alongside the other processes. This class of processes differ from the previous classes in the sense that they happen in tandem with the other processes instead of linear. In addition, the particular order in which the concurrent processes execute is irrelevant as opposed to the other non-concurrent processes. Concurrent processes include the following:
- obtaining authorization;
- documentation;
- managing information flow;
- preserving chain of custody;
- preserving digital evidence;
- interaction with the physical investigation.

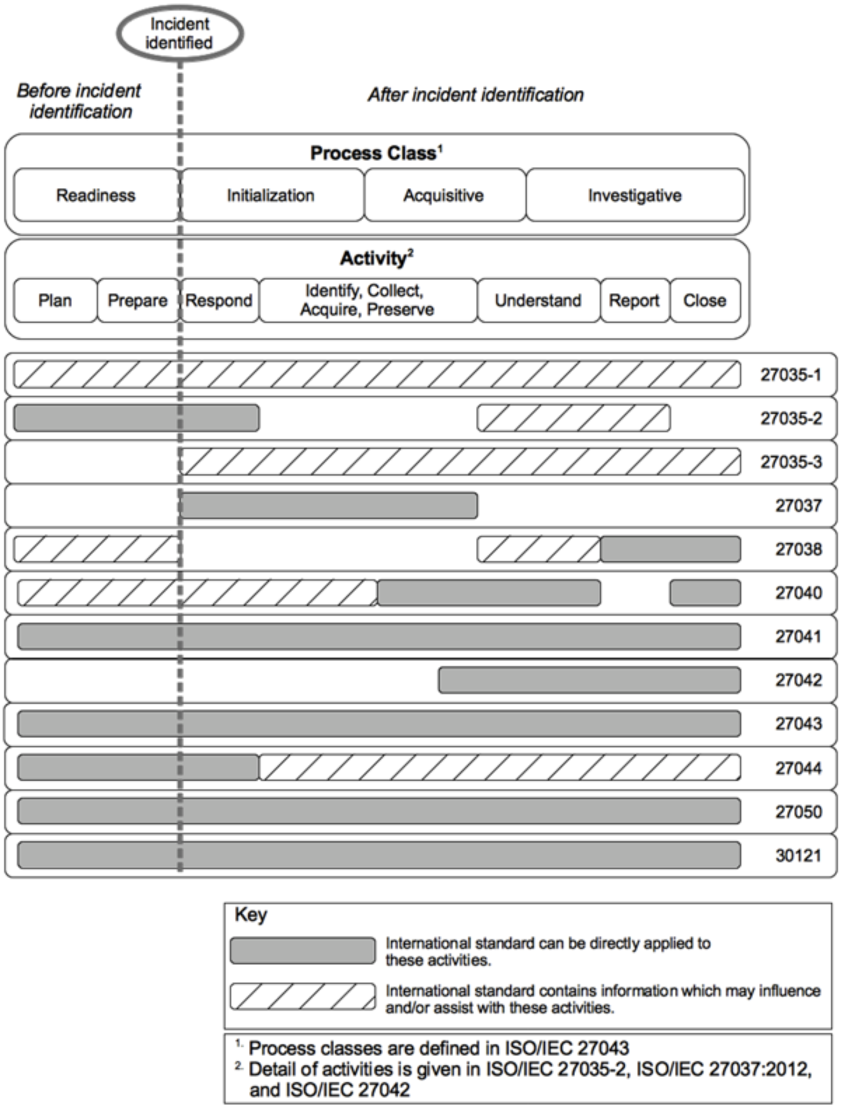

Incident identified
Before incident identification
After incident identification
Process Class[1]
Readiness
Initialization
Acquisitive
Investigative
Activity[2]
Plan
Prepare
Respond
Identify, Collect, Acquire, Preserve
Understand
Report
Close
27035-1
27035-2
27035-3
27037
27038
27040
27041
27042
27043
27044
27050
30121
Key
International standard can be directly applied to these activities.
International standard contains information which may influence and/or assist with these activities.
1. Process classes are defined in ISO/IEC 27043
2. Detail of activities is given in ISO/IEC 27035-2, ISO/IEC 27037:2012, and ISO/IEC 27042

Figure 2 Applicability of standards to investigation process classes and activities.

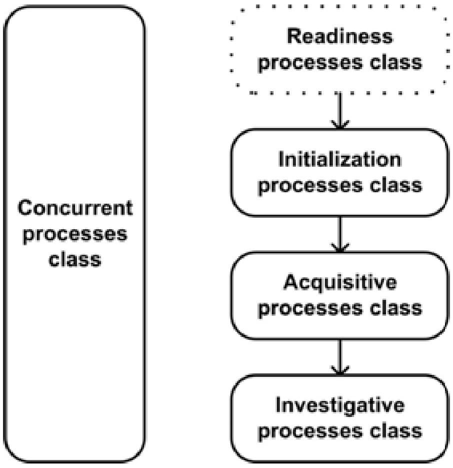

Concurrent processes class
Readiness processes class
Initialization processes class
Acquisitive processes class
Investigative processes class

Figure 3 The various classes of digital forensic investigation processes in ISO27043.

Figure 3 shows the relationships between the various classes of digital investigation processes. Note that the dotted lines around processes in all figures indicate that the particular process is optional.

The six concurrent processes are aimed at allowing the said processes to be executed as on-going processes. The reason for having the concurrent processes is mainly to ensure more effective admissibility of digital evidence into a legal system, since, in the case of not having such processes, any investigation may run the risk that the admitted potential evidence might not be suitable for litigation due to improper handling and documentation of potential digital evidence. These concurrent processes are, thus, based on principles that need to be followed throughout a digital investigation, alongside with the other classes of processes.

4.4.3 The contribution of the archival sciences – Corinne Rogers

The ease with which digital material can be altered, intentionally or accidentally, and the ease with which it can be disseminated, shared, combined, and repurposed, has driven security, privacy, and rights concerns across domains and disciplines. Two of the most challenging issues presented by digital technology to the law enforcement, records management, archival and legal professions, researchers, business, government and the public are the identification of "records" in digital systems, and the determination of their "authenticity" [2]. These issues may be addressed from the archival perspective, backed by archival theory and methodology, and specifically by digital diplomatics. They are also addressed from a technological perspective, by the methods and tools of digital forensics. At the most basic level, both digital archivists and digital forensics practitioners are concerned with discovering, understanding, describing and presenting information inscribed on digital media.

Shared theoretical perspectives of digital forensics and digital archival practice include: (1) authorship and identity (authenticity of origin and forgery), (2) informational pattern and change over time (reconstruction and relationships among extant traces and objects), (3) evidential reliability (provenance and integrity), and (4) digital materiality and ornament (contextual detail and interpretation). There are also common pressing challenges in finding, processing and sustaining digital information: (1) the volume of a person's life information spread across myriad devices, along with the exacerbating complexity of diverse applications and locations – local machines and media, network servers and remote cloud services; (2) the necessary versatility of tools, techniques and models required to capture and investigate digital information and to marshall metadata and description; (3) the forward looking process and activity required to ensure sustainability and long term digital preservation; and (4) the intensifying role of information assurance, data security planning, and protection of privacy and other digital rights [8].

The core archival functions are identified as appraisal and acquisition, arrangement and description, retention and preservation, management and administration, and reference and access. Furthermore, research may be considered the foundation of each archival activity [3]. Archival research has focused historically on records, defined as documents made or received in the course of practical activity, and set aside for further action or reference [4], as the primary objects of investigation. Archivists are concerned with establishing the evidentiary capacity of documents, and analyzing their evidential value, whether they are preserved primarily as records (as with a public organisation) or for their informational value as personal memory or legacy (as with a personal archive).

The science of diplomatics originated in the 17th century to establish the authenticity, and indirectly, the reliability, of archival documents, in order to determine rights and to identify and eliminate forgeries. It studies the genesis, forms, and transmission of records, the relationships of the records with associated actions, persons, and legal consequences [1]. Digital diplomatics has developed to provide a framework for assessing the authenticity of digital records and offers a powerful methodology for analyzing digital records. However, digital diplomatics alone may not be sufficient to understand the challenges posed to information inscribed by increasingly complex digital systems [2].

The lifecycle of authentic digital records, from the development of records systems through generation, maintenance, use, and preservation of records is captured in the Chain of Preservation (COP) model (Consultation draft – [5]). This model, developed through the research of the InterPARES Project (http://www.interpares.org), reflects archival theory and archival diplomatics, and complies with the requirements of the Open Archival Information System (OAIS) Reference Model, ISO 14721:2003 Space data and information transfer systems (see appendix for and example of key diagrams). The model identifies all the activities and actions that must be undertaken to ensure that digital records are properly generated in the first instance, maintain their integrity over time, and can be reproduced at any time throughout their existence. As well, it characterizes the metadata that must be gathered, stored and utilized throughout the lifecycle. Preliminary work has been done in mapping elements of the COP model to a general digital forensics process model [7]. Such an integration is intended to assist in establishing requirements for digital evidence and forensic readiness.

4.4.4 Digital forensics in IT security incident management

4.4.4.1 Historical perspective

The application of digital forensic methods for the investigation of security incidents grew out of the use of computer forensics in criminal investigations. Starting in the mid-1990, many organisations developed internal security incident response capabilities and the investigation of security breaches was an important part. While initially focused on the collection and analysis of digital traces from individual computer hard drives, with computers becoming network-centric the monitoring and analysis of network data became important and with it the field of network forensics. While in traditional computer forensics data is collected and analysed after and as a result of a security incident, in network forensics data is often collected and analysed with the specific aim to actively detect security intrusions. More recent developments focus on the capture and analysis of volatile computer data (memory forensics), the investigation of mobile devices (mobile device forensics) and the enterprise-wide investigation of security breaches (enterprise forensics). While digital forensic methods are regularly applied in the investigation of criminal cases, civil litigations also make use of the forensic analysis of digital data. This so called electronic discovery or e-dicovery process is often a part of internal compliance investigations in an enterprise context.

4.4.5 Forensics in IT security investigations and its relations to criminal and civil litigations – Heiko Patzlaff

There are specific differences in the application of digital forensic methods for the investigation of security breaches versus its use in litigation.

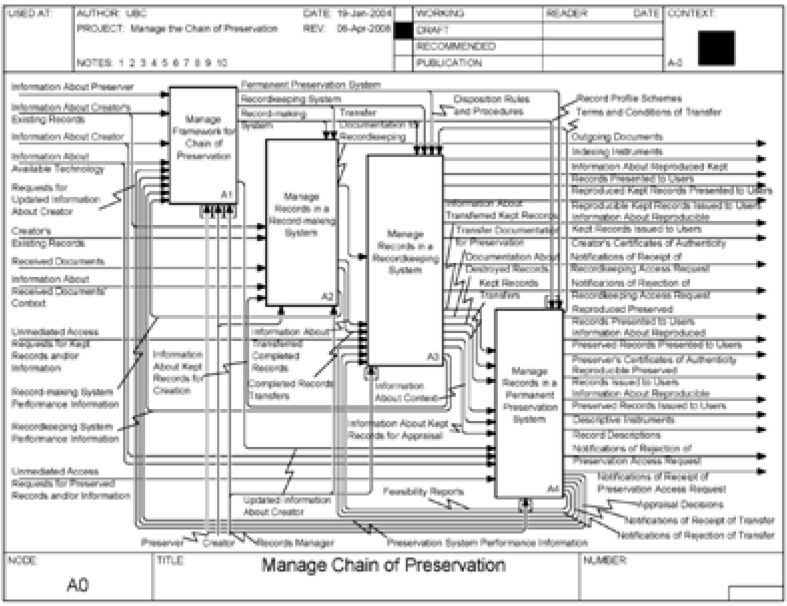
a. IT security investigations are usually not user centric Since the target of a security attack is usually a computer system inside a company and the attacker is an outsider, data produced by the user of the computer system is not relevant to the investigation. The aim is to reconstruct the activities of the attacker. The analysis of logs and timestamps plays a central role. While user activity traces might be important for and therefore part of the investigation, this has fewer data protection and data privacy implications than the analysis of user generated content such as emails or office documents.

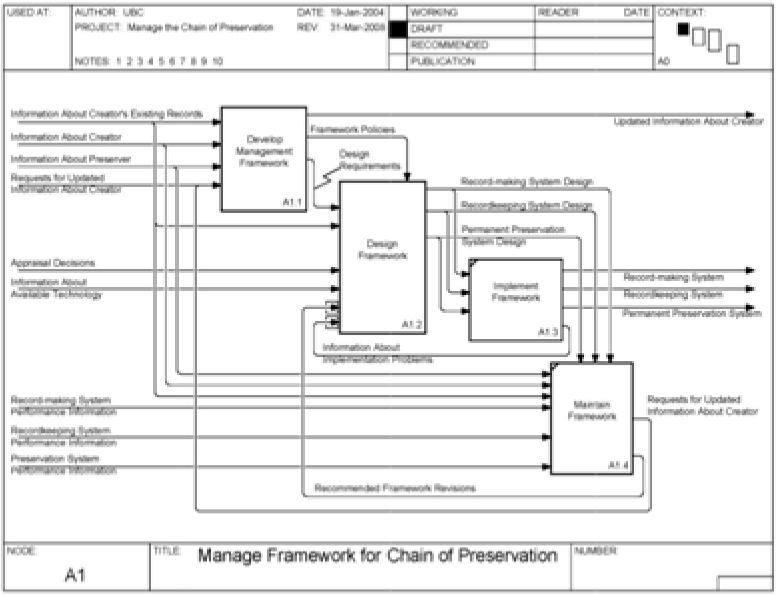
b. IT security investigations usually don't lead to litigation Even though typical security breaches are in most countries illegal, the investigation of those breaches usually does not lead to litigation. The reasons are practical since establishing the identity of the attacker is often not possible or cost prohibitive. There are therefore less stringent requirements with respect to the collection, analysis and preservation of data than in digital forensic investigations leading to criminal or civil lawsuits. The main aim of a security forensic investigation is therefore usually not to identify the attacker but to establish the root cause of why a security breach was possible and the damage that was done.

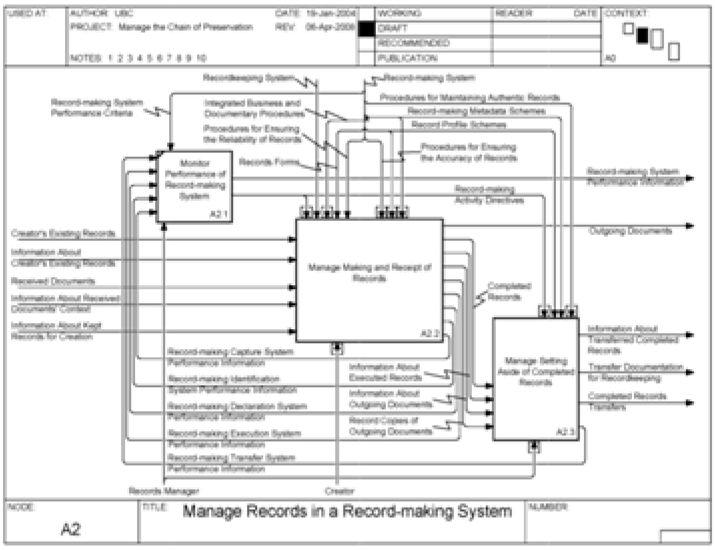
4.4.6 Current trends and challenges

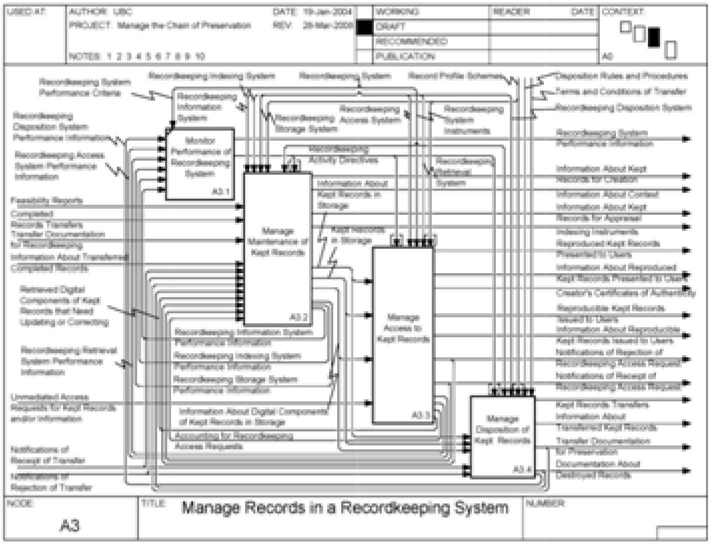
With the growing loss of effectiveness of traditional, signature-based security controls such as anti-virus and the advent of campaign style attacks against company intellectual properties (advanced persistent threats) in recent years, the need for new ways to conduct digital forensic investigations has become apparent. The need for large-scale investigations of hundreds or thousands of computers has lead to the field of enterprise forensics and brought the introduction of new pro-active methodologies such as malware hunting, where company-wide searches of computers for the presence of specific objects or anomalies are conducted in order to identify compromised computer nodes. This has lead to new legal questions related to the protection of user data and privacy. While traditional investigations of single computer nodes are both limited in scope and bound to specific indicators of a successful security breach of the computer in question, these new investigations are often conducted based on much less clear compromise indicators and with a much wider scope. They might also extend across multiple countries and jurisdictions. Another challenge arises with the new trend of user owned devices (bring your own device, BYOD) where company and user data are not well separated and again questions related to user data and privacy emerge.

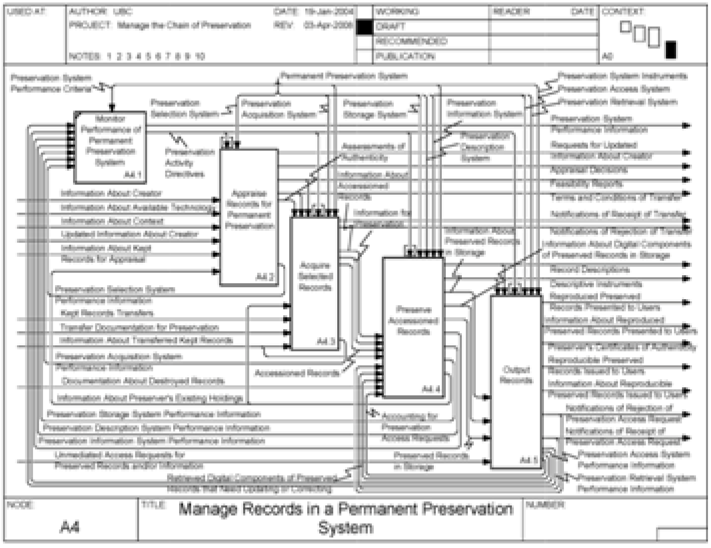
4.4.7 Appendix – Key diagrams from the COP Model


USED AT:
AUTHOR: UBC
PROJECT: Manage the Chain of Preservation
NOTES: 1 2 3 4 5 6 7 8 9 10
DATE: 19-Jan-2004
REV: 06-Apr-2008
WORKING
DRAFT
RECOMMENDED
PUBLICATION
READER
DATE
CONTEXT:
A-0
Information About Preserver
Information About Creator's Existing Records
Information About Creator
Information About Available Technology
Requests for Updated Information About Creator
Creator's Existing Records
Received Documents
Information About Received Documents' Context
Unmediated Access Requests for Kept Records and/or Information
Record-making System Performance Information
Recordkeeping System Performance Information
Unmediated Access Requests for Preserved Records and/or Information
Manage Framework for Chain of Preservation
A1
Permanent Preservation System
Recordkeeping System
Record-making System
Transfer Documentation to Recordkeeping
Manage Records in a Record-making System
A2
Disposition Rules and Procedures
Manage Records in a Recordkeeping System
A3
Information About Kept Records for Creation
Information About Transferred Completed Records
Completed Records Transfers
Information About Context
Information About Kept Records for Appraisal
Updated Information About Creator
Feasibility Reports
Information About Transferred Kept Records
Transfer Documentation for Preservation
Documentation About Destroyed Records
Kept Records Transfers
Manage Records in a Permanent Preservation System
A4
Record Profile Schemes
Terms and Conditions of Transfer
Outgoing Documents
Indexing Instruments
Information About Reproduced Kept Records Presented to Users
Reproduced Kept Records Presented to Users
Reproducible Kept Records Issued to Users
Information About Reproducible Kept Records Issued to Users
Creator's Certificates of Authenticity
Notifications of Receipt of Recordkeeping Access Request
Notifications of Rejection of Recordkeeping Access Request
Reproduced Preserved Records Presented to Users
Information About Reproduced Preserved Records Presented to Users
Preserver's Certificates of Authenticity
Reproducible Preserved Records Issued to Users
Information About Reproducible Preserved Records Issued to Users
Descriptive Instruments
Record Descriptions
Notifications of Rejection of Preservation Access Request
Notifications of Receipt of Preservation Access Request
Appraisal Decisions
Notifications of Receipt of Transfer
Notifications of Rejection of Transfer
Preserver
Creator
Records Manager
Preservation System Performance Information
NODE:
A0
TITLE:
Manage Chain of Preservation
NUMBER:


USED AT:
AUTHOR: UBC
PROJECT: Manage the Chain of Preservation
NOTES: 1 2 3 4 5 6 7 8 9 10
DATE: 19-Jan-2004
REV: 31-Mar-2008
WORKING
DRAFT
RECOMMENDED
PUBLICATION
READER
DATE
CONTEXT:
A0
Information About Creator's Existing Records
Information About Creator
Information About Preserver
Requests for Updated Information About Creator
Develop Management Framework
A1.1
Updated Information About Creator
Framework Policies
Design Requirements
Design Framework
A1.2
Record-making System Design
Recordkeeping System Design
Permanent Preservation System Design
Appraisal Decisions
Information About Available Technology
Implement Framework
A1.3
Record-making System
Recordkeeping System
Permanent Preservation System
Information About Implementation Problems
Record-making System Performance Information
Recordkeeping System Performance Information
Preservation System Performance Information
Maintain Framework
A1.4
Requests for Updated Information About Creator
Recommended Framework Revisions
NODE:
A1
TITLE:
Manage Framework for Chain of Preservation
NUMBER:


USED AT:
AUTHOR: UBC
PROJECT: Manage the Chain of Preservation
DATE: 19-Jan-2004
REV: 06-Apr-2006
NOTES: 1 2 3 4 5 6 7 8 9 10
WORKING
DRAFT
RECOMMENDED
PUBLICATION
READER
DATE
CONTEXT:
A0
Recordkeeping System
Record-making System
Record-making System Performance Criteria
Integrated Business and Documentary Procedures
Procedures for Ensuring the Reliability of Records
Records Forms
Procedures for Maintaining Authentic Records
Record-making Metadata Schemes
Record Profile Schemes
Procedures for Ensuring the Accuracy of Records
Monitor Performance of Record-making System
A2.1
Record-making System Performance Information
Record-making Activity Directives
Outgoing Documents
Creator's Existing Records
Information About Creator's Existing Records
Received Documents
Information About Received Documents' Context
Information About Kept Records for Creation
Manage Making and Receipt of Records
A2.2
Completed Records
Manage Setting Aside of Completed Records
A2.3
Information About Transferred Completed Records
Transfer Documentation for Recordkeeping
Completed Records Transfers
Record-making Capture System Performance Information
Record-making Identification System Performance Information
Record-making Declaration System Performance Information
Record-making Execution System Performance Information
Record-making Transfer System Performance Information
Information About Executed Records
Information About Outgoing Documents
Record Copies of Outgoing Documents
Records Manager
Creator
NODE:
A2
TITLE:
Manage Records in a Record-making System
NUMBER:


USED AT:
AUTHOR: UBC
PROJECT: Manage the Chain of Preservation
DATE: 19-Jan-2004
REV: 28-Mar-2006
NOTES: 1 2 3 4 5 6 7 8 9 10
WORKING
DRAFT
RECOMMENDED
PUBLICATION
READER
DATE
CONTEXT:
A0
Recordkeeping System Performance Criteria
Recordkeeping Indexing System
Recordkeeping System
Record Profile Schemes
Disposition Rules and Procedures
Terms and Conditions of Transfer
Recordkeeping Disposition System
Recordkeeping Information System
Recordkeeping Storage System
Recordkeeping Access System
Recordkeeping System Instruments
Recordkeeping Disposition System Performance Information
Recordkeeping Access System Performance Information
Monitor Performance of Recordkeeping System
A3.1
Recordkeeping Activity Directives
Recordkeeping Retrieval System
Recordkeeping System Performance Information
Information About Kept Records for Creation
Information About Context
Information About Kept Records for Appraisal
Indexing Instruments
Reproduced Kept Records Presented to Users
Information About Reproduced Kept Records Presented to Users
Creator's Certificates of Authenticity
Reproducible Kept Records Issued to Users
Information About Reproducible Kept Records Issued to Users
Notifications of Rejection of Recordkeeping Access Request
Notifications of Receipt of Recordkeeping Access Request
Kept Records Transfers
Information About Transferred Kept Records
Transfer Documentation for Preservation
Documentation About Destroyed Records
Feasibility Reports
Completed Records Transfers
Transfer Documentation for Recordkeeping
Information About Transferred Completed Records
Manage Maintenance of Kept Records
A3.2
Information About Kept Records in Storage
Kept Records in Storage
Manage Access to Kept Records
A3.3
Retrieved Digital Components of Kept Records that Need Updating or Correcting
Recordkeeping Information System Performance Information
Recordkeeping Indexing System Performance Information
Recordkeeping Storage System Performance Information
Recordkeeping Retrieval System Performance Information
Unmediated Access Requests for Kept Records and/or Information
Information About Digital Components of Kept Records in Storage
Accounting for Recordkeeping Access Requests
Manage Disposition of Kept Records
A3.4
Notifications of Receipt of Transfer
Notifications of Rejection of Transfer
NODE:
A3
TITLE:
Manage Records in a Recordkeeping System
NUMBER:


USED AT:
AUTHOR: UBC
PROJECT: Manage the Chain of Preservation
DATE: 19-Jan-2004
REV: 03-Apr-2006
NOTES: 1 2 3 4 5 6 7 8 9 10
WORKING
DRAFT
RECOMMENDED
PUBLICATION
READER
DATE
CONTEXT:
A0
Preservation System Performance Criteria
Permanent Preservation System
Preservation System Instruments
Preservation Access System
Preservation Retrieval System
Preservation Selection System
Preservation Acquisition System
Preservation Storage System
Preservation Information System
Monitor Performance of Permanent Preservation System
A4.1
Preservation Activity Directives
Preservation Description System
Assessments of Authenticity
Information About Accessioned Records
Information for Preservation
Preservation System Performance Information
Requests for Updated Information About Creator
Appraisal Decisions
Feasibility Reports
Terms and Conditions of Transfer
Notifications of Receipt of Transfer
Notifications of Rejection of Transfer
Information About Digital Components of Preserved Records in Storage
Record Descriptions
Descriptive Instruments
Reproduced Preserved Records Presented to Users
Information About Reproduced Preserved Records Presented to Users
Preserver's Certificates of Authenticity
Reproducible Preserved Records Issued to Users
Information About Reproducible Preserved Records Issued to Users
Notifications of Rejection of Preservation Access Request
Notifications of Receipt of Preservation Access Request
Preservation Access System Performance Information
Preservation Retrieval System Performance Information
Information About Creator
Information About Available Technology
Information About Context
Updated Information About Creator
Information About Kept Records for Appraisal
Appraise Records for Permanent Preservation
A4.2
Acquire Selected Records
A4.3
Information About Preserved Records in Storage
Preserve Accessioned Records
A4.4
Output Records
A4.5
Preservation Selection System Performance Information
Kept Records Transfers
Transfer Documentation for Preservation
Information About Transferred Kept Records
Preservation Acquisition System Performance Information
Accessioned Records
Documentation About Destroyed Records
Information About Preserver's Existing Holdings
Preservation Storage System Performance Information
Preservation Description System Performance Information
Preservation Information System Performance Information
Accounting for Preservation Access Requests
Unmediated Access Requests for Preserved Records and/or Information
Preserved Records in Storage
Retrieved Digital Components of Preserved Records that Need Updating or Correcting
NODE:
A4
TITLE:
Manage Records in a Permanent Preservation System
NUMBER:

References

1 Duranti, L. (1998). *Diplomatics: New Uses for an Old Science.* Lanham: Scarecrow Press.

2 Duranti, L. (2009). *From Digital Diplomatics to Digital Records Forensics.* Archivaria, 68(Fall), 39–66.

3 Duranti, L., & Michetti, G. (2012). *Archival method.* Vancouver, BC.

4 Duranti, L., & Thibodeau, K. (2006). *The Concept of Record in Interactive, Experiential and Dynamic Environments: the View of InterPARES.* Archival Science, 6(1), 13–68.

5 Eastwood, Terry, and Randy Preston. (2008). *Modeling Cross-domain Task Force Report: Chain of Preservation Model Narrative.* Available at http://www.interpares.org/ip2/display_file.cfm?doc=ip2_book_part_5_modeling_task_force.pdf.

6 John, J. L. (2012). *Digital Forensics and Preservation. Digital Preservation Coalition.* Retrieved from http://www.dpconline.org/component/docman/doc_download/810-dpctw12-03pdf

7 Rogers, Corinne. 2013. *Digital Records Forensics: Integrating Archival Science into a General Model of the Digital Forensics Process.* In Proceedings of the Second International Workshop on Cyberpatterns: Unifying Design Patterns with Security, Attack and Forensic Patterns, edited by Clive Blackwell, 4–21. Oxford, UK: Oxford Brookes University.

8 Rogers, Corinne, and JL John. 2013. *Shared Perspectives, Common Challenges: A History of Digital Forensics & Ancestral Computing for Digital Heritage.* In The Memory of the World in the Digital Age: Digitization and Preservation, 314–36. Vancouver, BC: UNESCO. http://www.unesco.org/webworld/download/mow/mow_vancouver_proceedings_en.pdf.

Participants

- Aaron Alva
University of Washington, US
- Carsten Bormann
Universiät Bremen, DE
- Joseph Cannatac
University of Malta, MT
- Raymond Choo
Univ. of South Australia, AU
- Glenn S. Dardick
Longwood University, US
- Günther Diederich
ifib GmbH – Bremen, DE
- Jos Dumortier
KU Leuven, BE
- Barbara Endicott-Popovsky
University of Washington, US
- Katrin Y. Franke
Gjøvik University College, NO
- Felix C. Freiling
Friedrich-Alexander-University
Erlangen-Nürnberg, DE
- Stefanie Gerdes
Universiät Bremen, DE
- Pavel Gladyshev
University College Dublin, IE
- Babak Habibnia
University College Dublin, IE
- Nils-Peter Hercher
Nagel Schlösser
Rechtsanwälte, DE
- Florian Junge
Universiät Bremen, DE
- Thomas Kemmerich
Gjøvik University College, NO
- Nicolai Kuntze
Fraunhofer SIT – Darmstadt, DE
- David Manz
Pacific Northwest National
Laboratory, US
- Christian Moch
Friedrich-Alexander-University
Erlangen-Nürnberg, DE
- Carsten Momsen
Leibniz University Hannover, DE
- Heiko Patzlaff
Siemens, DE
- Corinne Rogers
InterPARES Trust, CA
- Carsten Rudolph
Fraunhofer SIT, DE
- Viola Schmid
TU Darmstadt, DE
- Isabel Taylor
University Tübingen, DE
- Lee Tobin
University College Dublin, IE
- Hein Venter
University of Pretoria, ZA
- Rhythm Suren Wadhwa
Gjøvik University College, NO
- Nigel Wilson
University of Adelaide, AU
- Stephen Wolthusen
Royal Holloway University of
London, GB & Gjovik University
College, NO