

Towards a Capability Maturity Model for Digital Forensic Readiness

Günther Pernul, Ludwig Englbrecht and Stefan Meier
Department of Information Systems, University of Regensburg



Universität Regensburg

Agenda

- 1. Introduction to Digital Forensics**
2. Digital Forensics in Enterprises
3. Need for Digital Forensic Readiness
4. Capability Maturity Model for Digital Forensic Readiness

Motivation – Why do we need digital forensics?

Multiple banks hit: 3.2 mill... X +

indianexpress.com/article/explained/multiple-banks-hit-3-2-million-debit-cards-comp- Suchen

The Indian EXPRESS

Nation World Opinion Sports Entertainment Lifestyle Technology Viral Photos Videos Blogs ePaper Insurance

Latest News Karan Johar's Rs 5 cr is 3 times what Army welfare fund got in 2 months


Home > Explained > Multiple banks hit: 3.2 million debit cards compromised; how it happened, what happens now?

Multiple banks hit: 3.2 million debit cards compromised; how it happened, what happens now?

Indian Express explains one of the biggest data security breaches in Indian banking, situates it in the context of the rising threat from cyber crime.

324 SHARES

Written by **Khushboo Narayan** | Updated: October 21, 2016 7:09 pm



BEST OF EXPRESS

Business
Ratan Tata appointed interim Chairman of Tata Sons, Cyrus Mistry sacked

India
Don't politicise Triple Talaq, it's not just a Hindu-Muslim issue: PM Modi

NEWS

Technology

Massive ransomware infection hits computers in 99 countries

13 May 2017



follow the instructions!

WEBROOT

The ransomware has been identified as WannaCry - here shown in a safe environment on a security researcher's computer

A massive cyber-attack using tools believed to have been stolen from the US National Security Agency (NSA) has struck organisations around the world.

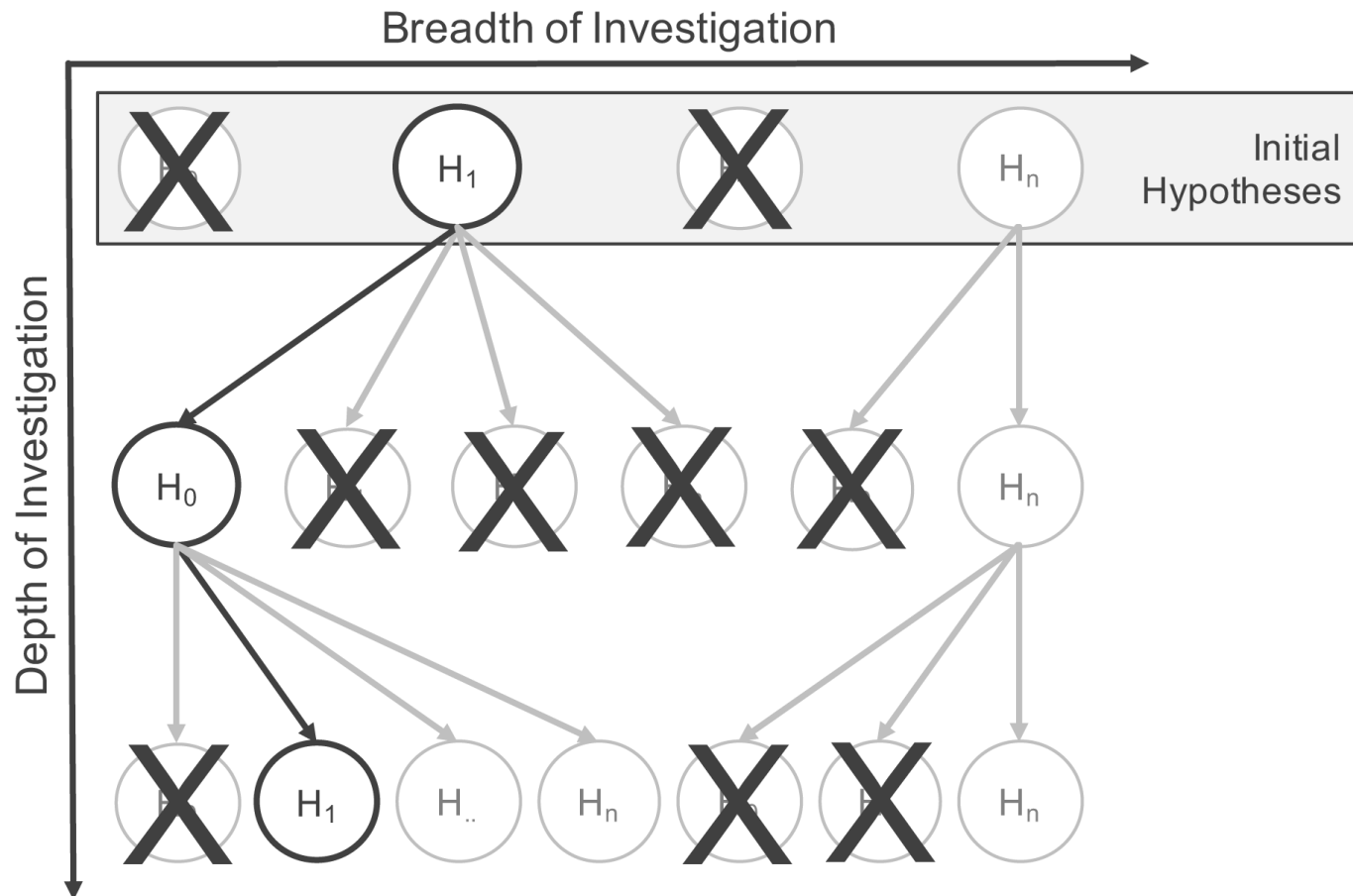
Cyber-security firm Avast said it had seen 75,000 cases of the ransomware - known as WannaCry and variants of that name - around the world.

Digital Forensics Definitions

Digital forensics deals with scientific methods from computer science to provide legitimate and correct digital evidence in a court of law / or the legal system.

- **E.g. cases of computer misuse**
- **To clarify fraud and computer related crime**

Scientific Method: Hypothesis Testing



Digital Evidence

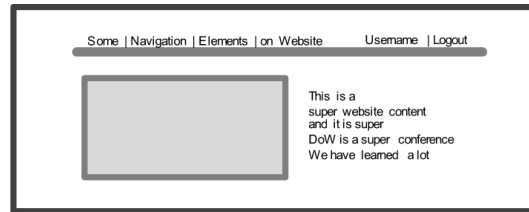
- **Any data stored or transmitted using a computer that support or refute a theory of how an offense occurred or that address critical elements of the offense such as intent or alibi.**

(Casey2011, p.7)

- **Digital evidence is also physical evidence in the first place**
 - Magnetization on the surface of a hard disk
 - Electromagnetic waves on a data cable
 - Transistor's state of charge

Digital Evidence Abstraction Layers

Application



File System



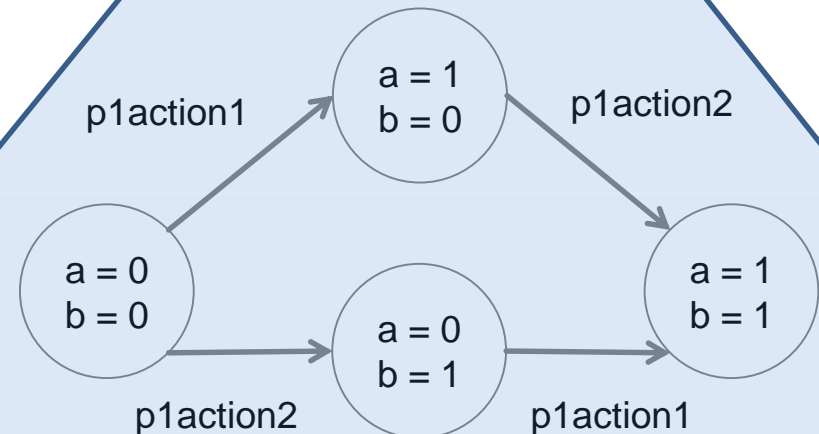
Media Management



Physical Media



Digital Evidence Model



**What is the basis to infer certain actions
in real life computer systems?**

Basic Forensic Principles in the Digital World

Question: Did computer A visit website B?

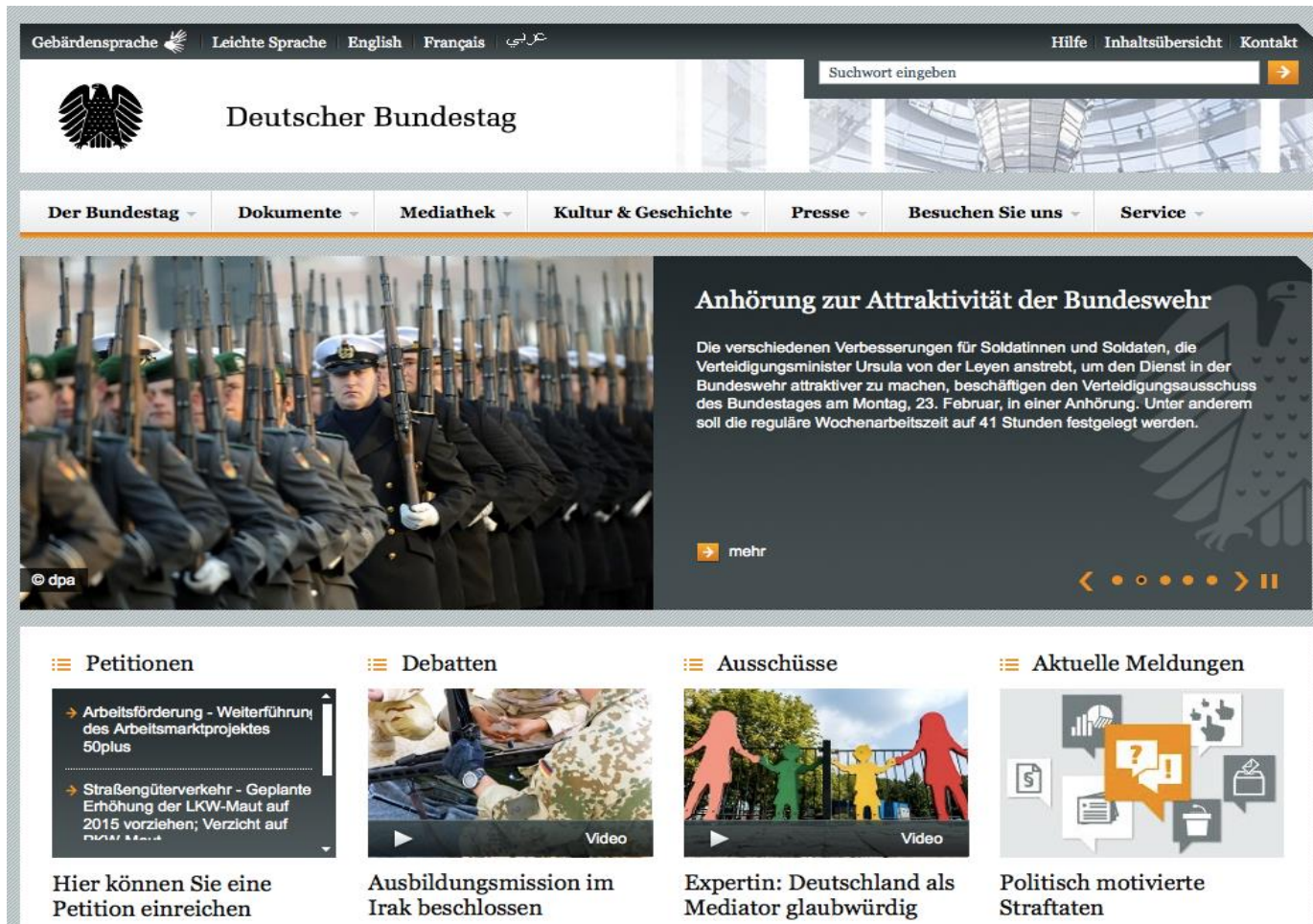
1. **Identify** files which might potentially be useful
2. **Classify** preserved files as browser cache files
3. Analyze content of cached files to find **individual** characteristics like cached user name, specific site, content of sites, timestamp of files, ...
4. Establish an **association** between the website B and the computer A based on the outcomes of the previous step.

Digital Evidence Problems

- Generally not tamper resistant
- Easy alterable
- Digital Evidence is not directly linkable to a natural person



DDoS-Attack on www.bundestag.de



The screenshot shows the homepage of the German Bundestag website. The header includes language options (Gebärdensprache, Leichte Sprache, English, Français, عربي) and a search bar. The main navigation menu contains links to Der Bundestag, Dokumente, Mediathek, Kultur & Geschichte, Presse, Besuchen Sie uns, and Service. The main content area features a large image of German soldiers in uniform, with a text block titled 'Anhörung zur Attraktivität der Bundeswehr' (Hearing on the attractiveness of the Federal Armed Forces). Below this, there are four sections: Petitionen (Petitions), Debatten (Debates), Ausschüsse (Committees), and Aktuelle Meldungen (Current News). Each section has a thumbnail image and a brief description of the topic.

Header: Gebärdensprache | Leichte Sprache | English | Français | عربي | Suche: Suchwort eingeben

Navigation: Der Bundestag | Dokumente | Mediathek | Kultur & Geschichte | Presse | Besuchen Sie uns | Service

Main Content:

- Anhörung zur Attraktivität der Bundeswehr**
Die verschiedenen Verbesserungen für Soldatinnen und Soldaten, die Verteidigungsminister Ursula von der Leyen anstrebt, um den Dienst in der Bundeswehr attraktiver zu machen, beschäftigen den Verteidigungsausschuss des Bundestages am Montag, 23. Februar, in einer Anhörung. Unter anderem soll die reguläre Wochenarbeitszeit auf 41 Stunden festgelegt werden.

Footer Sections:

- Petitionen:** Arbeitsförderung - Weiterführung des Arbeitsmarktpaketes 50plus; Straßengüterverkehr - Geplante Erhöhung der LKW-Maut auf 2015 vorziehen; Verzicht auf...
- Debatten:** Ausbildungsmission im Irak beschlossen
- Ausschüsse:** Expertin: Deutschland als Mediator glaubwürdig
- Aktuelle Meldungen:** Politisch motivierte Straftaten

(Basic) Forensic investigation process



Acquisition

Secure and collect
digital evidence
from the crime
scene

Examination

Decide which
evidence/data is
relevant to the case

Analysis

Interpretation of
data

Correlate evidence

Handle uncertainty

Assess likelihood of
events

Presentation

Write a Report

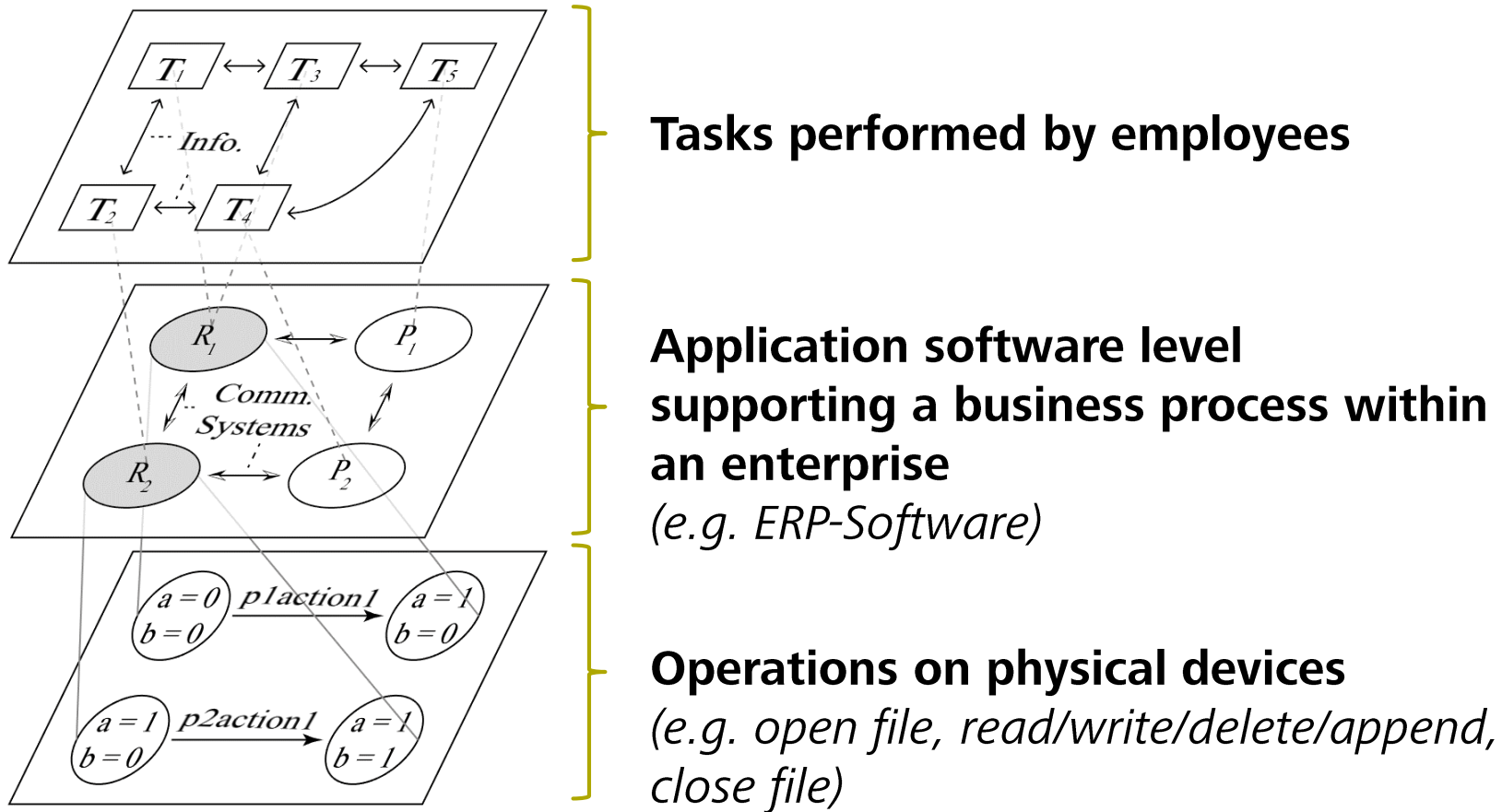
Present evidence in
a court of law

Agenda

1. Introduction to Digital Forensics
- 2. Digital Forensics in Enterprises**
3. Need for Digital Forensic Readiness
4. Capability Maturity Model for Digital Forensic Readiness

Digital Forensics in Enterprises

Relationships between the task, the application software level and operations on physical devices



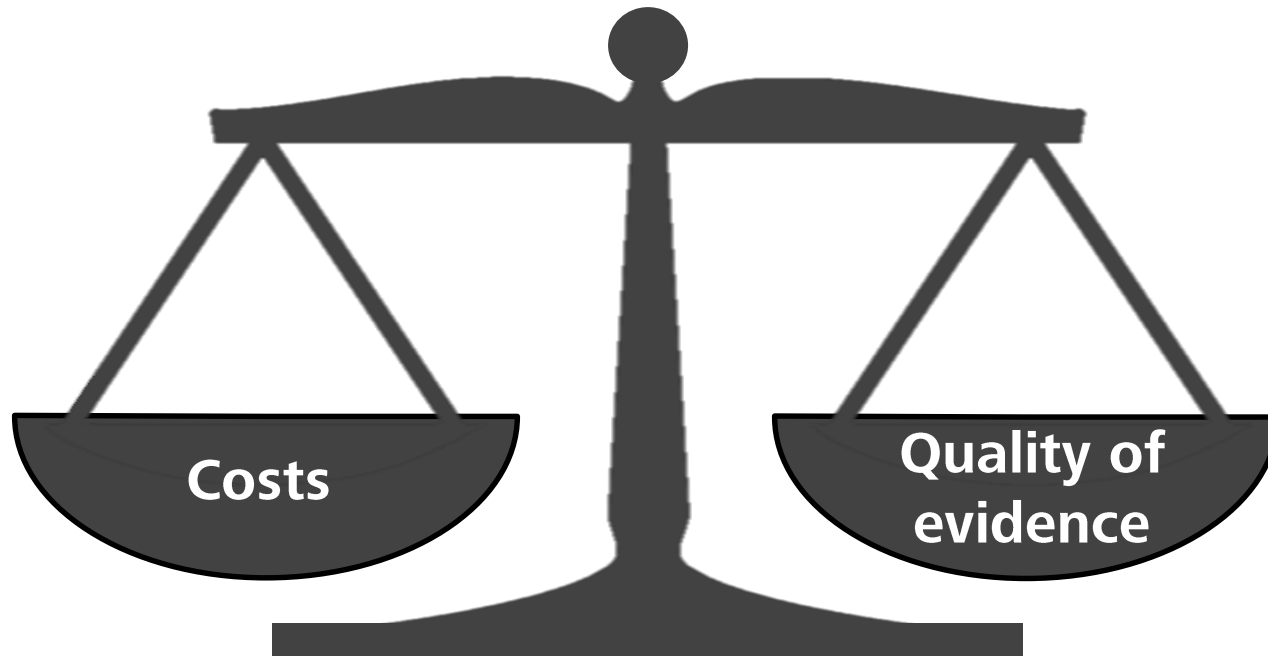
Agenda

1. Introduction to Digital Forensics
2. Digital Forensics in Enterprises
- 3. Need for Digital Forensic Readiness**
4. Capability Maturity Model for Digital Forensic Readiness

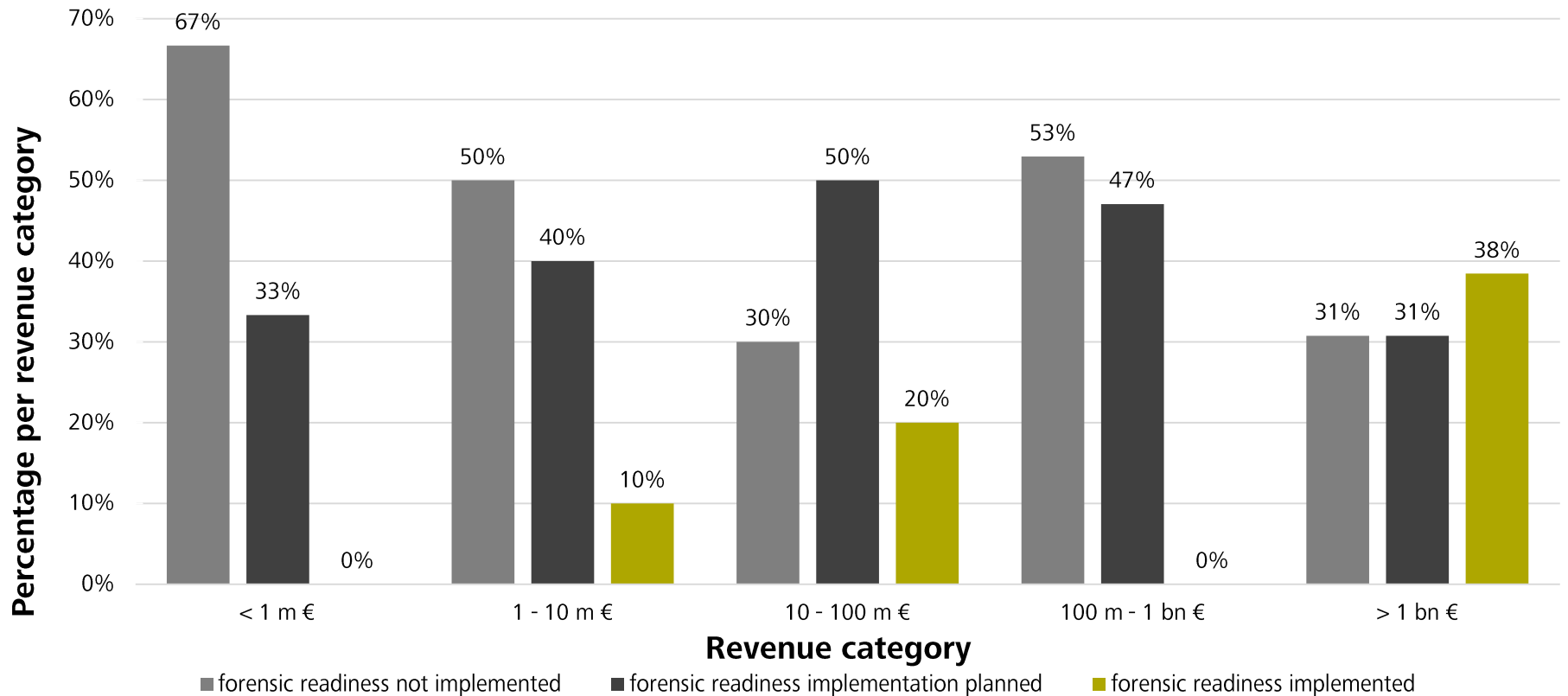
Digital Forensic Readiness Goals

1. Maximize an environment's ability to collect credible digital evidence.
2. Minimize the cost of forensics in an incident response.

(Tan 2001)



Forensic Readiness in Organizations



n = 59

Agenda

1. Introduction to Digital Forensics
2. Digital Forensics in Enterprises
3. Need for Digital Forensic Readiness
4. **Capability Maturity Model for Digital Forensic Readiness**

How to implement Digital Forensic Readiness – Capability Levels

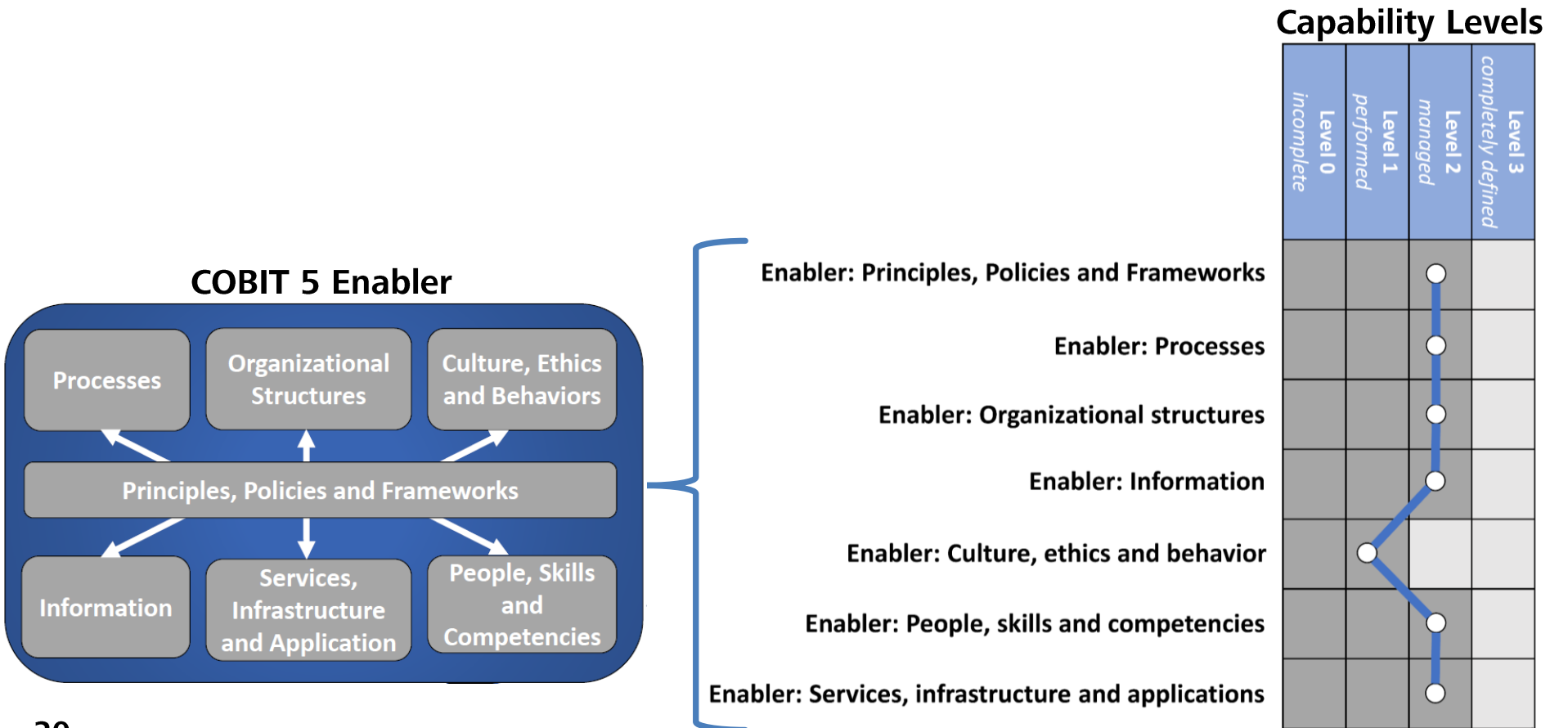
Step 1: Defining capability levels

Description of the defined capability levels

Level	Description
0 - Incomplete	The DF related objectives are <u>not</u> reached.
1 - Performed	The intended goals in DF are reached.
2 - Managed	DF initiatives and activities are managed and not ad-hoc performed.
3 - Completely defined	A standardized process for DF activities is in place. The procedures underlie a continuous improvement.

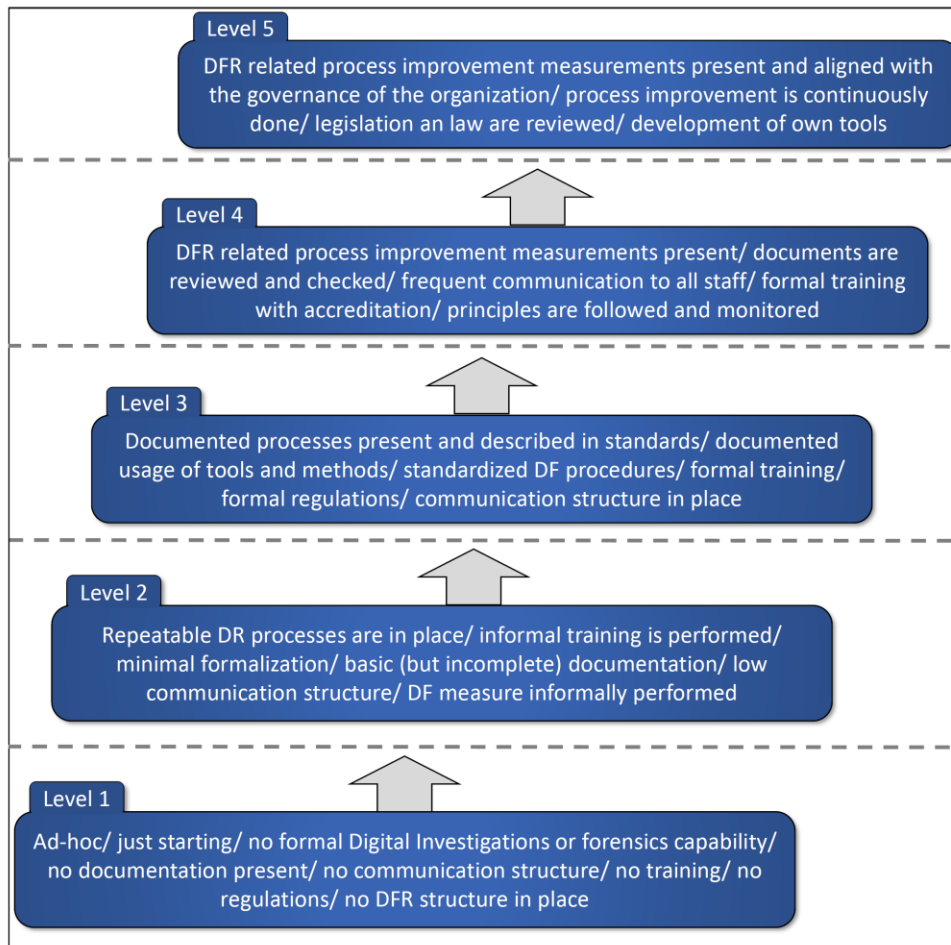
How to implement Digital Forensic Readiness – IT-Governance

Step 2: For each COBIT 5 enabler a certain level of capability can be determined



How to implement Digital Forensic Readiness – Maturity Levels

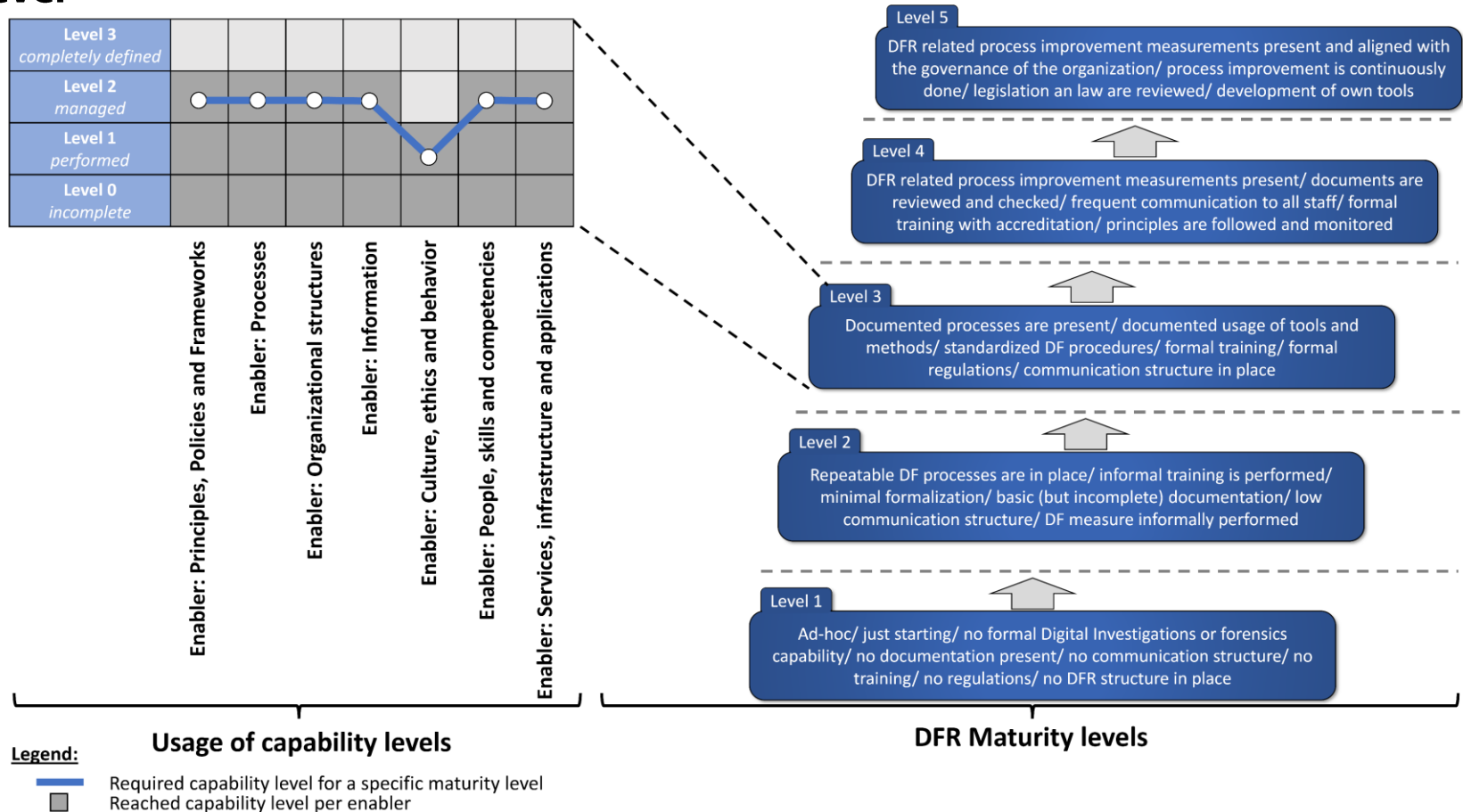
Step 3: Defining maturity levels



- *„Optimized“*
- *„Quantitatively Managed“*
- *„Defined“*
- *„Managed“*
- *„Initial“*

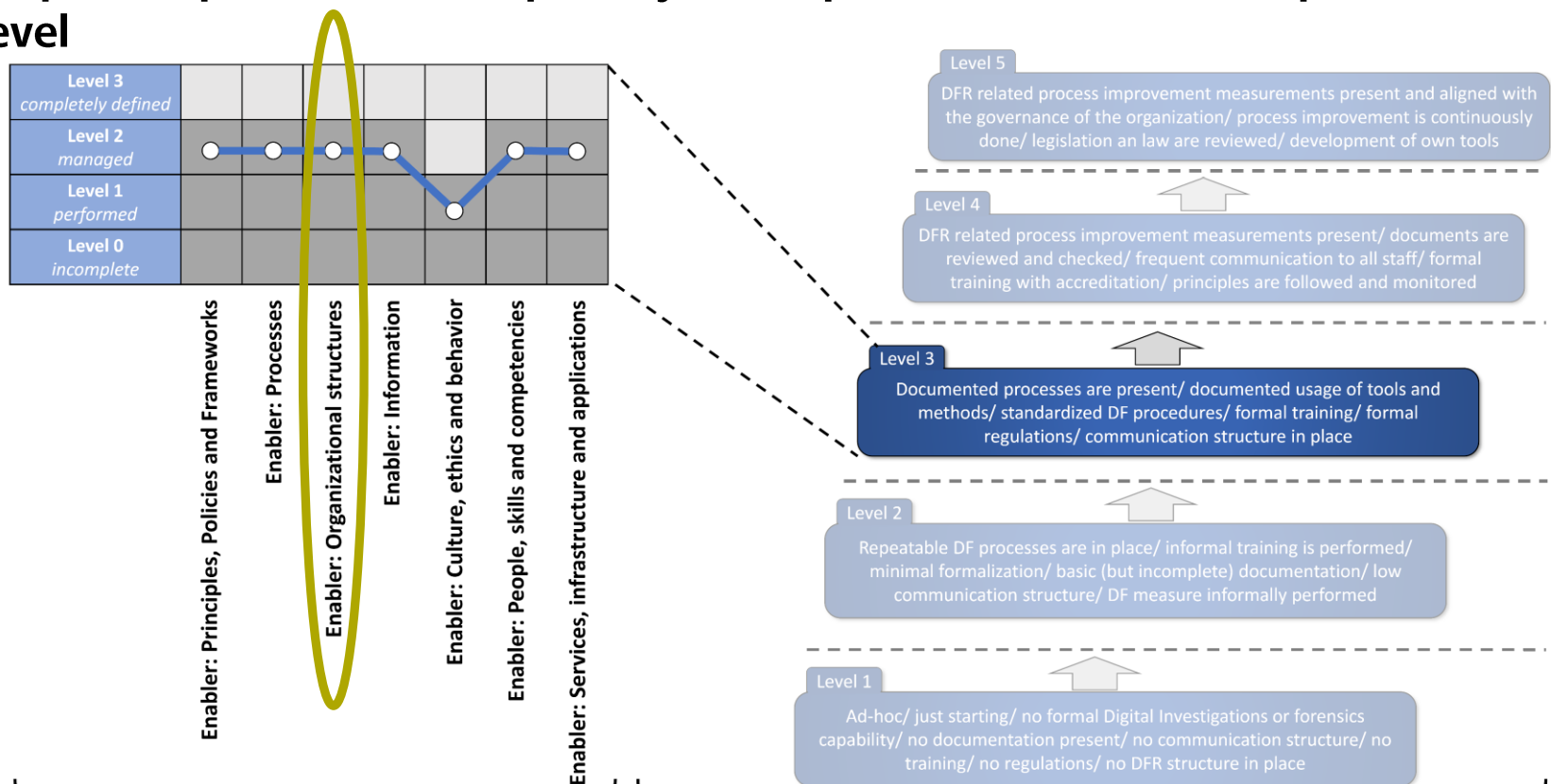
How to implement Digital Forensic Readiness – Overview

Step 4: A specific set of capability levels per Enabler defines a specific maturity level



How to implement Digital Forensic Readiness – Example

Step 4: A specific set of capability levels per Enabler defines a specific maturity level



Legend:

- Required capability level for a specific maturity level
- Reached capability level per enabler

How to implement Digital Forensic Readiness – Example

Indicators to determine the capability level of the Enabler “Organizational structures”

Indicator	aligned to <i>enabler</i>	max. contribution (<i>cap. level</i>)	type <i>m = mandatory</i> <i>o = optional</i>
Responsibilities for the case of a DF investigation are known	Organizational structures	1	
Responsibilities for the case of a DF investigation are defined	Organizational structures	2	m
DF related decision making guidelines are included in job-descriptions or roles	Organizational structures	3	m
Rights within Information Systems are defined	Organizational structures	1	m
Rights within Information Systems are defined and adjusted to prevent potential destroying or tampering of evidences	Organizational structures	2	m
Identity management system is in place	Organizational structures	3	o
Escalation rules are defined	Organizational structures	2	m
Escalation rules are defined, reviewed and monitored	Organizational structures	3	m

Presence of this indicator is mandatory to reach level 1

How to implement Digital Forensic Readiness – Example

Level 3

Documented processes are present/ documented usage of tools and methods/
standardized DF procedures/ formal training/ formal regulations/ communication
structure in place

- The minimal necessity to have DFR in place is the maturity level 3
- The higher levels, Level 4 and 5, assist to set up necessary requirements to faster adopt new demands in DFR
- The model can be used for continuous improvements in specific areas and to stay digital forensic ready

Current state of research

- **Further evaluation of the DFR capability maturity model by using a interactive web tool for self-assessment and conducting expert interviews.**
- **Define enterprise forensics as a new academic field of research.**
- **Integration of business process descriptions into enterprise forensics investigations.**
- **Create methods and tools for the investigation of application systems on the application systems abstraction layer.**

Any questions?

Contact Information



Universität Regensburg

Prof. Dr. Günther Pernul
Lehrstuhl für Wirtschaftsinformatik I
Universität Regensburg
Universitätsstr. 31
D-93053 Regensburg

Tel: +49 (0) 941 943 2743
Fax: +49 (0) 941 943 2744
eMail: guenther.pernul@wiwi.uni-regensburg.de
Web: www-ifs.uni-regensburg.de

Literature

Beckett J, Slay J (2011) Scientific underpinnings and background to standards and accreditation in digital forensics. Digital Investigation 8(2):114–121.

Bundesamt für Sicherheit in der Informationstechnik (2011) Leitfaden IT-Forensik.

Casey E (2011) Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Academic Press.

Dewald A, Freiling F (2011) Forensische Informatik. Books on Demand.

Dewald A, Freiling F (2012) Is Computer Forensics a Forensic Science? Current Issues in IT Security.

Ferstl O, Sinz E (2013) Grundlagen der Wirtschaftsinformatik. 7. aktualisierte Auflage. Oldenbourg.

Garfinkel Simson, Nelson A, Young J (2012) A general strategy for differential forensic analysis. Digital Investigation.

C Hertneck, R Kneuper (2011) Prozesse verbessern mit CMMI® for Services

ISO/IEC 27043:2014(E) (2014) Information technology - Security techniques - Incident investigation principles and processes

Rowlingson R (2004) A Ten Step Process for Forensic Readiness. International Journal of Digital Evidence (IJDE) 2(3).

Slay J, Lin Y, Turnbull B, Beckett J, Lin P (2009) Towards a Formalization of Digital Forensics. In: Peterson G, Sheno S (Hrsg.) Advances in Digital Forensics V. Springer Berlin Heidelberg.

Tan J (2001) Forensic Readiness.