FIDIS

Future of Identity in the Information Society

Title:	"D6.7b : Workshop on Forensic Profiling "
Author:	WP6
Editors:	Zeno Geradts
Reviewers:	Mireille Hildebrandt
Identifier:	D6.7b
Type:	Deliverable
Version:	1.0
Date:	Monday, 07 January 2008
Status:	Final
Class:	Deliverable
File:	fidis-wp6-del6.7b.workshop_on_forensic_profiling.doc

Summary

In the workshop on Forensic Profiling in The Hague at 30 September 2007, a multi-disciplinary approach was given to forensic profiling. The limitations and risks are discussed and should be the start for a deliverable on forensic profiling which should be ready at April 1st 2008.

The FIDIS NoE receives research funding from the Community's Sixth Framework Program

Copyright Notice:

Members of the FIDIS consortium

1. Goethe University Frankfurt	Germany
2. Joint Research Centre (JRC)	Spain
3. Vrije Universiteit Brussel	Belgium
4. Unabhängiges Landeszentrum für Datenschutz (ICPP)	Germany
5. Institut Europeen D'Administration Des Affaires (INSEAD)	France
6. University of Reading	United Kingdom
7. Katholieke Universiteit Leuven	Belgium
8. Tilburg University[1]	Netherlands
9. Karlstads University	Sweden
10. Technische Universität Berlin	Germany
11. Technische Universität Dresden	Germany
12. Albert-Ludwig-University Freiburg	Germany
13. Masarykova universita v Brne (MU)	Czech Republic
14. VaF Bratislava	Slovakia
15. London School of Economics and Political Science (LSE)	United Kingdom
16. Budapest University of Technology and Economics (ISTRI)	Hungary
17. IBM Research GmbH	Switzerland
18. Centre Technique de la Gendarmerie Nationale (CTGN)	France
19. Netherlands Forensic Institute (NFI)[2]	Netherlands
20. Virtual Identity and Privacy Research Center (VIP)[3]	Switzerland
21. Europäisches Microsoft Innovations Center GmbH (EMIC)	Germany
22. Institute of Communication and Computer Systems (ICCS)	Greece
23. AXSionics AG	Switzerland
24. SIRRIX AG Security Technologies	Germany

[1] Legal name: Stichting Katholieke Universiteit Brabant
[2] Legal name: Ministerie Van Justitie
[3] Legal name: Berner Fachhochschule

Foreword

FIDIS partners from various disciplines have contributed as authors to this document. The following list names the main contributors for the chapters of this document:

Chapter	*Contributor(s)*
	Zeno Geradts
	…

Table of Contents

1 Executive Summary 6
2 Introduction 7
Annex 1 9

1 Executive Summary

This deliverable describes a workshop which has been held in The Hague at 30 September 2007 in The Hague. D6.7 was continued after the University of Lausanne could contribute on forensic profiling. This meeting was in preparation for the deliverable of Forensic Profiling.

2 Introduction

For the deliverable on forensic profiling a workshop was organized in The Hague at the Netherlands Forensic Institute with several FIDIS participants:

- Peter Sommer (LSE) p.m.sommer@lse.ac.uk
- Jozef Vyskoc (VAF) jozef@vaf.sk
- Denis Royer (GUF) denis.royer@m-lehrstuhl.de,
- Mathias Kirchner, Thomas Gloe (TUD) Thomas.Gloe@inf.tu-dresden.de
- Fanny Coendert (KU Leuven), fanny.coudert@law.kuleuven.be
- Olivier Ribaux (University of Lausanne) Olivier.Ribaux@unil.ch
- Andre Hoogstrate (NFI) andre@holmes.nl
- Gert Jacobusse (NFI) gert@holmes.nl
- Zeno Geradts (NFI) zeno@holmes.nl
- Gerda Edelman (NFI) Gerda@holmes.nl
- Katja de Vries (VUB), edevries@vub.ac.be
- Mireille Hildebrandt (VUB) hildebrandt@frg.eur.nl
- Simone van der Hof (UVT) hof@uvt.nl

According to the agenda as as enclosed in annex 1. The presentations are included in Annex 2. It appeared that there is no real definition of forensic profiling. After a discussion, we came to the next proposal for the deliverable :

PROPOSED DELIVERABLE CONTENTS

Editors : Geradts / Sommer

1. Definitions of Forensic Profiling / Risk Profiling - University of

Lausanne

2. Methods of Forensic Profiling

- data aggregation
- data mining
- software tools
- 3D visualisation (NFI?)

- Image Processing (University Dresden)

3. Examples, Cases Studies

All

4. Legal Implications (Vrije Universiteit Brussel)

- Due Process
- Due Processing

5. Applications of Data Protection / human rights legislation Leuven

- Possible legal remedies
- Possible technical remedies
- Ambient Law

(Link to other FIDIS deliverables where possible).

The contributions could be one or several pages, depending on the subject.

The deliverable should be finished in draft in January 2008. After internal review, it should be available for the review of the European Commission at April 2008.

Annex 1

Draft AGENDA Forensic Profiling meeting at Netherlands Forensic Institute on 1st October 2007

09.30 arrival with tea/coffee

10.00 Opening (Zeno Geradts / what is forensic profiling)

10.15 Digital Investigation (Peter Sommer, London School of Economics)

11.00 Forensic profiling, crime control and due process (Katja de Vries, VUB)

12.00 lunch

13.00 Profiling from forensic perspective (Olivier Ribaux, University of Lausanne)

13.45 Inventory of social network analysis (Gert Jacobusse, NFI)

analysis of a database of traffic offenders and setting up a center of expertise on intelligent data analysis (Gert Jacobusse , Andre Hoogstrate, NFI)

14.45 Data Protection Issues (Fanny Coudert KU Leuven)

15.30 Image Forensics (Mathias Kirchner, Thomas Glue TU Dresden)

16.00 tour through digital evidence department

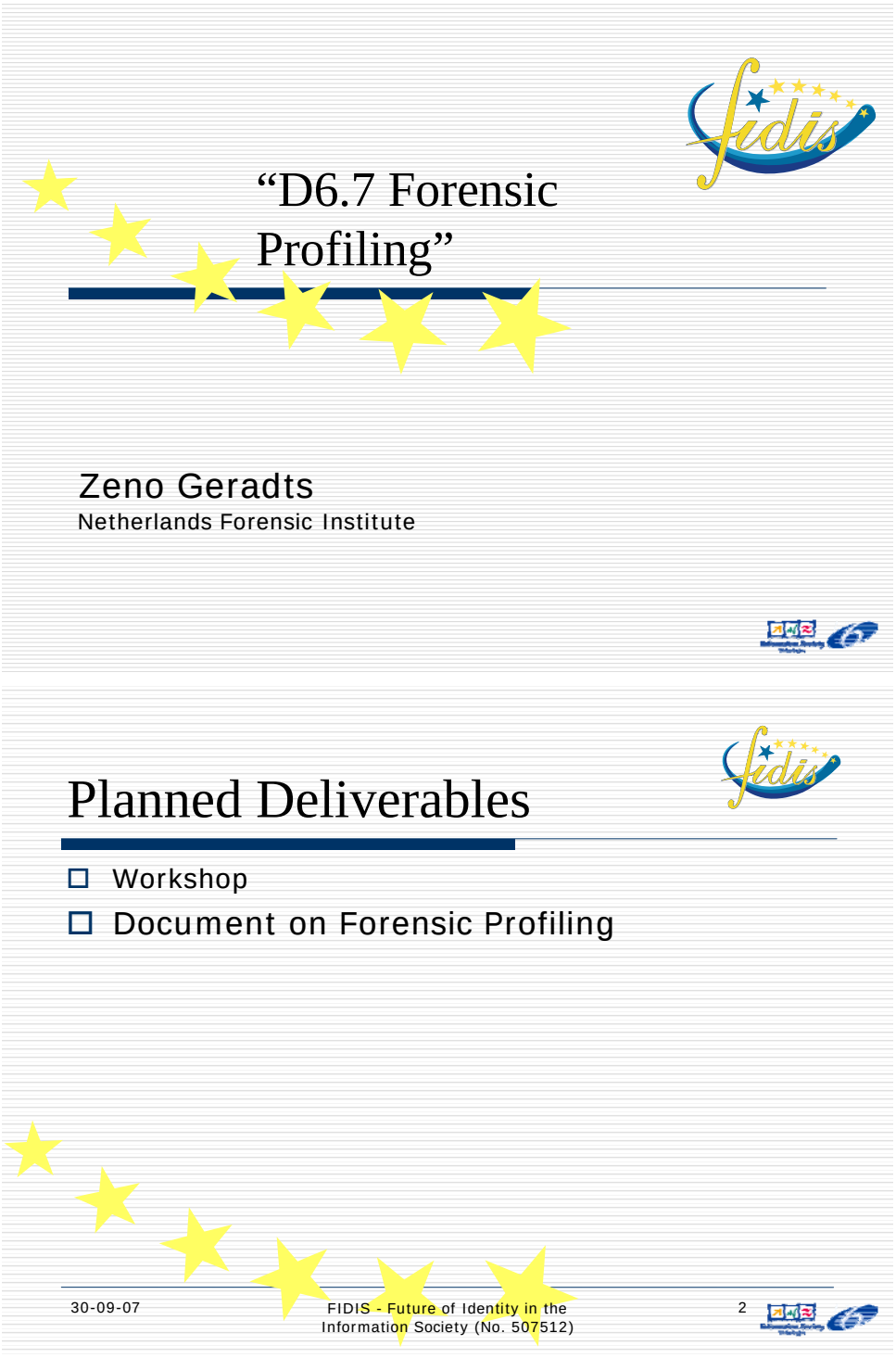
16.30 discussion and suggestion for deliverable (chapters)

17.00 closing

18.00 dinner at De Haagsche Kluisch Plein 20 the Hague (social event)

20.00 end of meeting

Annex 2


"D6.7 Forensic Profiling"
Zeno Geradts
Netherlands Forensic Institute
Planned Deliverables
Workshop
Document on Forensic Profiling
30-09-07
FIDIS - Future of Identity in the Information Society (No. 507512)
2

Program

- =
- 09.30 arrival with tea/coffee
- 10.00 Opening (Zeno Geradts NFI)
- 10.15 identity management systems: the forensic dimension(Peter Sommer, London School of Economics)
- 11.00 Inventory of social network analysis analysis of a database of traffic offenders and setting up a center of expertise on intelligent data analysis (Gert Jacobusse , Andre Hoogstrate, NFI)
- 12.00 Lunch
- 13.00 Profiling from forensic perspective (Olivier Ribaux, University of Lausanne

30-09-07 FIDIS - Future of Identity in the Information Society (No. 507512) 3

Program (2)

- 14.25 FES Project 3D tracking persons and vehicles(Gerda Edelman, NFI)
- 14.00 Profiling upon crime control (Mireille Hildebrandt VUB)
- 14.45 Data Protection Issues (Fanny Coudert KU Leuven)
- 15.30 Image Forensics (Mathias Kirchner, Thomas Glue TU Dresden)
- 16.00 tour through digital evidence department
- 16.30 discussion and suggestion for deliverable (chapters)
- 17.00 closing
- 18.00 dinner at De Haagsche Kluisch Plein 20 the Hague (social event)

30-09-07 FIDIS - Future of Identity in the Information Society (No. 507512) 4

Forensic Profiling, Crime Control & Due Process

Mixing elements from different semantic fields

Not very effective!

I. Due Process
II. Forensic Profiling

I. Due Process: Classical Legal Notion focused on the individual.

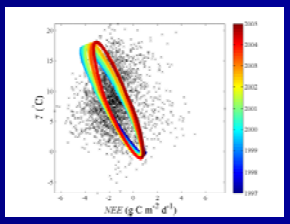
- In Europe: 6 ECHR
  Human Right to a Fair Trial (e.g. equality of arms, adversarial process, presumption of innocence)

- In the USA: 4th Amendment to the US Constitution (Bill of Rights)
  The right of the people to be secure against unreasonable searches and seizures

II. Forensic Profiling Techniques

A crucial difference between classical and some recent profiling techniques

- *Classical* forensic profiling: data matching which is (a) on an *individual* level, and (b) *ex ante* categorisation
- *Modern* forensic profiling: data mining which is (a) on a *group* level, and (b) *ex post* categorisation ("clustering")



Modern forensic profiling: first one looks for patterns, *not* individuals!

Within the modern forensic profiling techniques there is a moment when the umbilical cord between the *data subject* and the *data* which were derived from him is cut.

Modern forensic profiling: only in the 2nd place the individual re-enters the stage

Checking whether new data fit the pattern

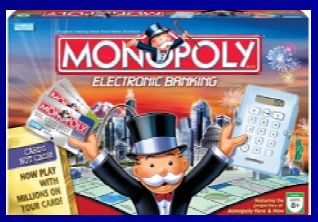
(e.g. passenger screening: identify higher risk airline passengers)

Data mining semantics (1)

- Data *mining*
- Data *harvesting*

Data mining semantics (2)

- Crunch *raw* data into a meaningful *product*: knowledge
- Data *processing*
- DNA *banking*



Two major issues

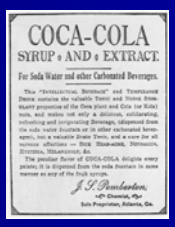
- Black Box
- Probabilistic Knowledge

(1) The Black Box of Data Processing

- So, in the stage of *data processing* the data subject is not in the picture
  a. Data subject is often *unaware* of the data being processed
  b. Data processing is a highly *technical* and *algorithmic* process (taking place literally in a 'black box', namely the computer)
  c. Profiling techniques are frequently applied for investigation and prevention (e.g. surveillance, investigative stops and frisks, searches) which can (or even must) be done without informing the profiled person.
- However, the algorithm in the black box might affect the data subject very profoundly. When a data mining system designates an individual as suspect, the reasons for these suspicions might turn out to be opaque to him. So how can there be a *fair* process?

Opening up? But....

- Algorithm derived from data mining is intrinsically secret, like a 'secret recipe'
- Is not only derived from *one particular* data subject, but from a whole group of people.
- 'Correction' by conscious data subject may be distortion in disguise



(2) The fruits of the harvest: probabilistic knowledge

What is *significant*?

Determining the line between what is significant and what not is in the end a *policy* decision.

e.g. "Which level of false positives?",
"Which level of correct matches?"

Is this "*part of the social burden of living under a government*"?

(a) Being profiled without having access to the profiling-algorithm (how to defend one self?).

(b) Relatively high risk of 'positive' result (in atmosphere wherein crime control is stressed governments will try to reduce false negatives at high cost).

Scientific 'fairness' <-> a 'fair' process in the classical legal sense

Is a judge more biased than a profiling algorithm?

Protected by the New data Framework decision?

Art 4:

1. Member States shall provide that personal data must be:
   (a) processed fairly and lawfully;
   (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards; [...].

Due *Processing* or Due *Process*? (1)

Article 19(2) *Right of information in cases of collection of data from the data subject with his knowledge*

The provision of the information laid down in paragraph 1 shall be refused or restricted only if necessary

(a) to enable the controller to fulfil its lawful duties properly,

(b) to avoid prejudicing of ongoing investigations, inquiries or proceedings or the fulfilment of the lawful duties of the competent authorities,

(c) to protect public security and public order in a Member State,

(d) to protect the rights and freedoms of third parties,

except where such considerations are overridden by the need to protect the interests or fundamental rights of the data subject.

Naïve approach? Some problems (1)

What use of knowing that your data were processed if you do not know *how*?

Who determines if the grounds enumerated in art 19(2) are present?

Due *Processing* or Due *Process*? (2)

Article 20(2) *Right of information where the data have not been obtained from the data subject or have been obtained from him without his knowledge*

The information laid down in paragraph 1 shall not be provided if necessary

(a) to enable the controller to fulfil its lawful duties properly,

(b) to avoid prejudicing of ongoing investigations, inquiries or proceedings or the fulfilment of the lawful duties of the competent authorities,

(c) to protect public security and public order in a Member State,

(d) to protect the rights and freedoms of third parties,

except where such considerations are overridden by the need to protect the interests or fundamental rights of the data subject.

Naïve approach? Some problems (2)

How can a data subject *without knowing that data were obtained from him (!!)* know if its rights were infringed?

Classical, individualistic remedies against techniques involving group level ex post analysis?

Not very effective!

Some alternatives.

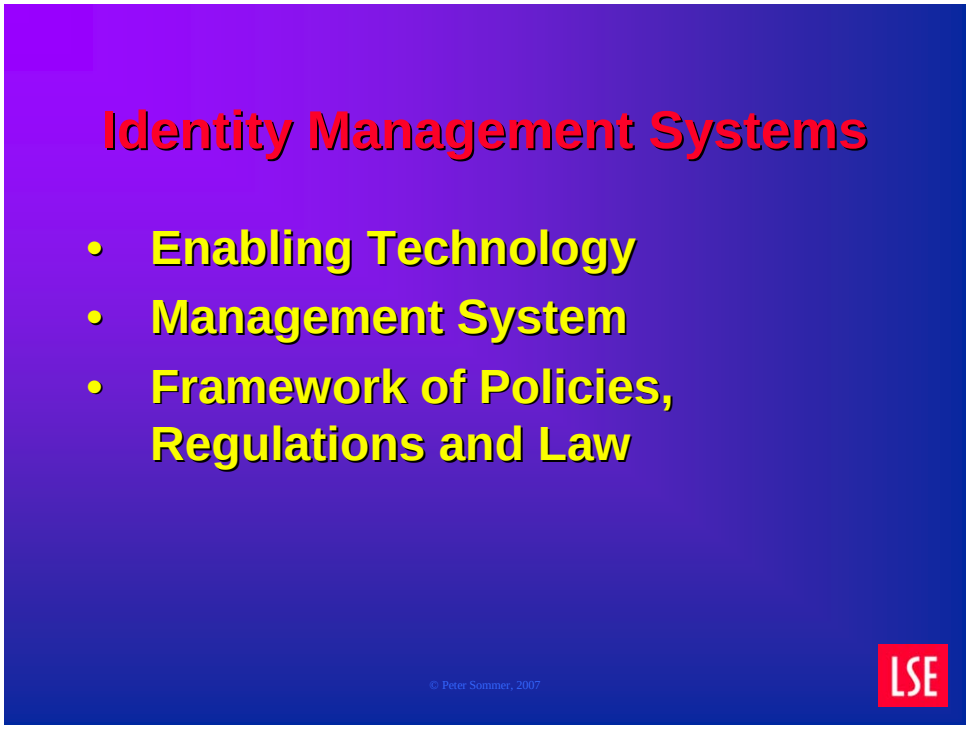
- summary hearings
- independent oversight of the validity of forensic profiling techniques
- post-deprivation correction rights
- compensatory damages

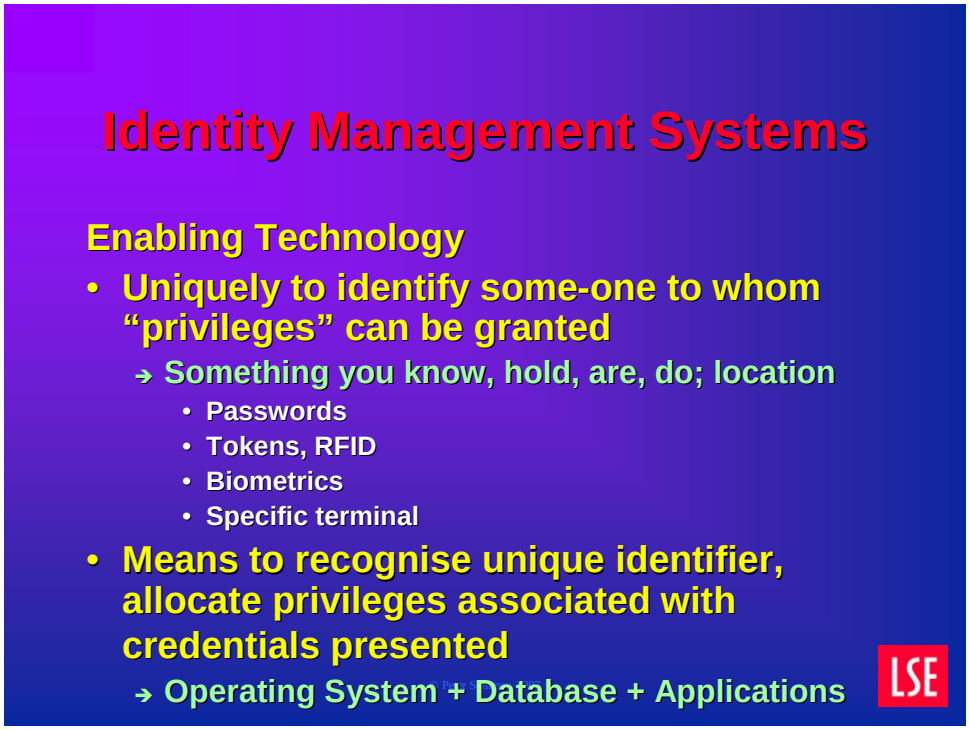
[Daniel Steinbock, Data Matching, Data Mining, and Due Process, 40 *Georgia Law Review* 1 (2005), pp. 1-84]

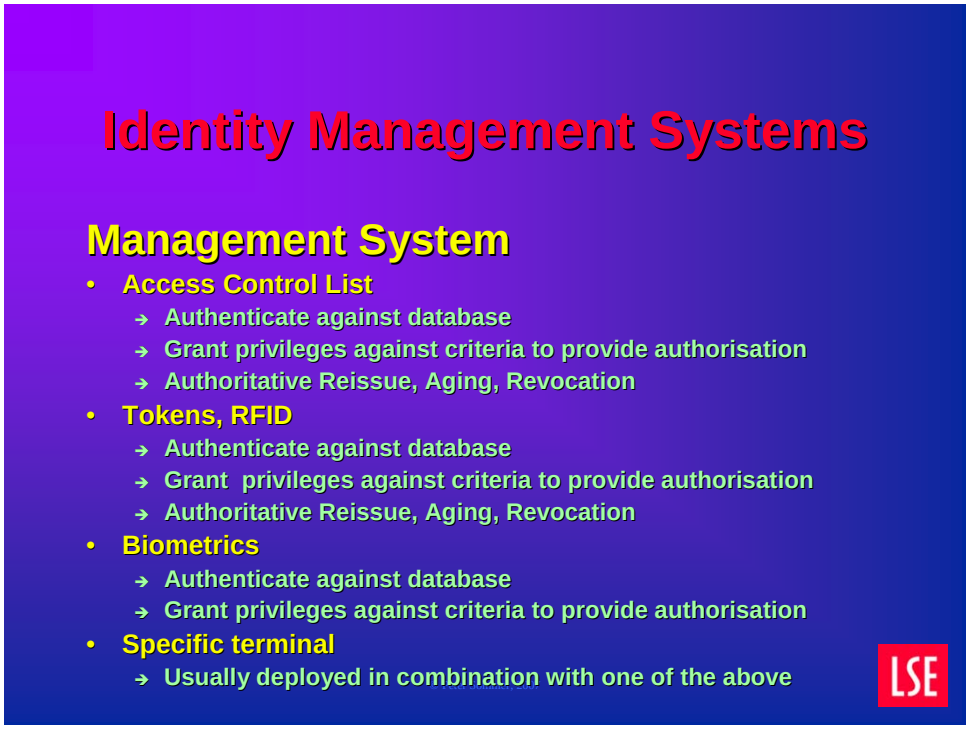

FIDIS
Profiling Meeting
1 October 2007
NFI
Identity Management Systems:
the forensic dimension
Peter Sommer
London School of Economics
© Peter Sommer, 2007
LSE


Let's explore a Paradox…
• Identity Management Systems have to be robust enough to have evidential value in legal proceedings
• Identity Management Systems have a close relative – called Surveillance Methodologies
• The everyday activities of Digital Forensics may expose activities – and hence potentially invade privacy – in ways never intended by designers of IMSs and law policy makers
© Peter Sommer, 2007
LSE

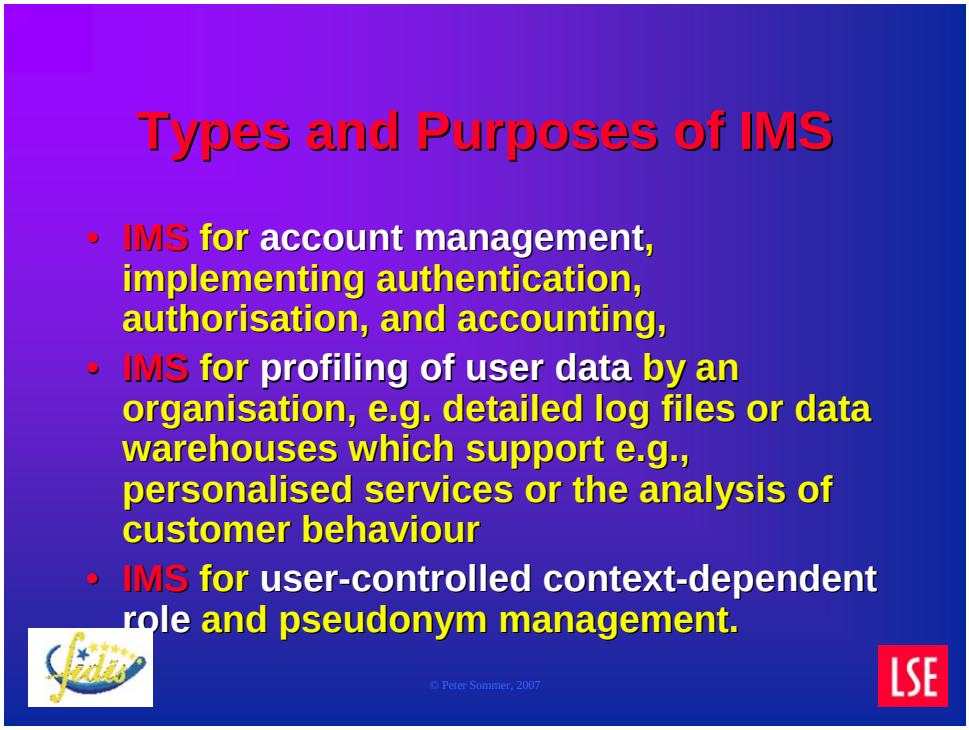

Where we need to get to
• Nature of IMSs
➔ and their weaknesses
• Nature of Digital Forensics
➔ and digital forensics research
• Applicable Law and regulation
• Understanding the Paradox
© Peter Sommer, 2007
LSE


Identity Management Systems
• Enabling Technology
• Management System
• Framework of Policies, Regulations and Law
© Peter Sommer, 2007
LSE

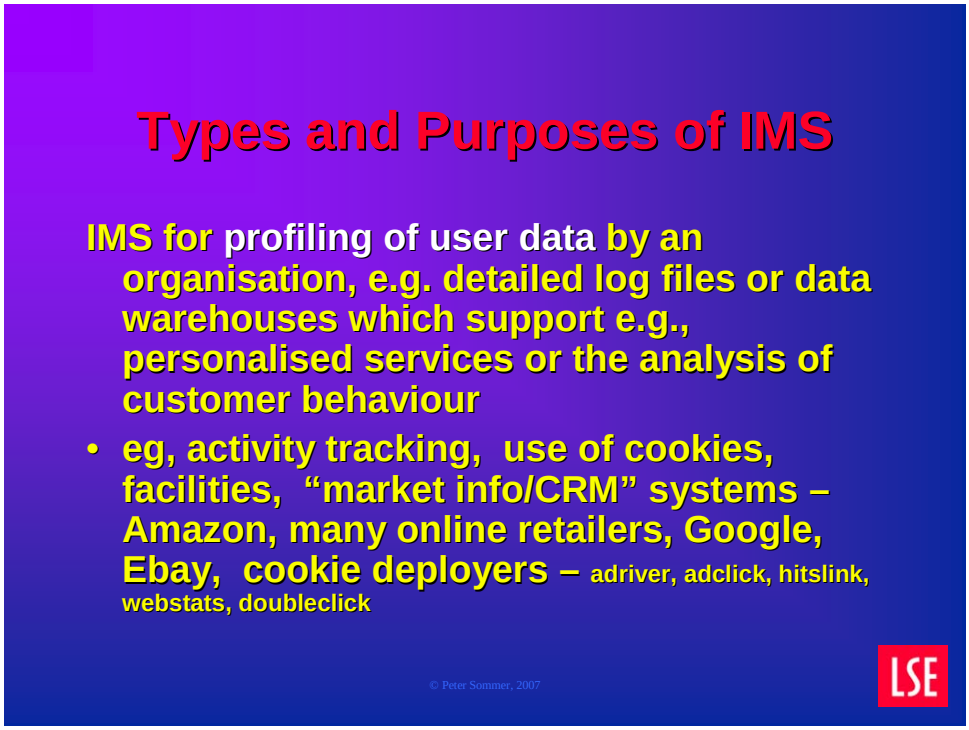

Identity Management Systems
Enabling Technology
• Uniquely to identify some-one to whom "privileges" can be granted
→ Something you know, hold, are, do; location
• Passwords
• Tokens, RFID
• Biometrics
• Specific terminal
• Means to recognise unique identifier, allocate privileges associated with credentials presented
→ Operating System + Database + Applications
LSE

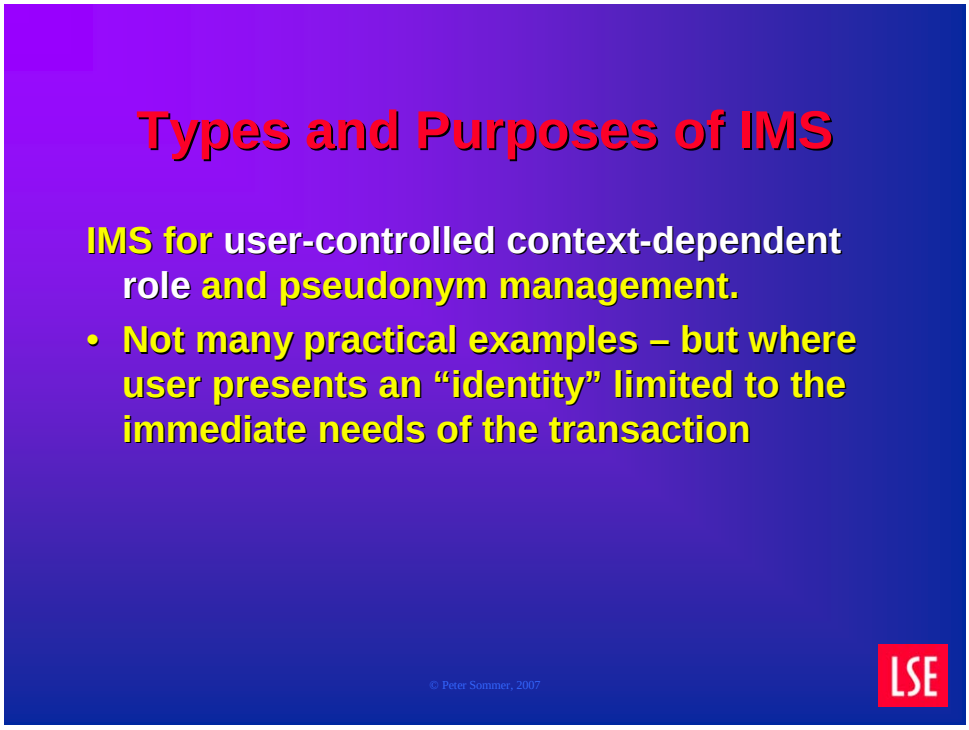

Identity Management Systems
Management System
• Access Control List
→ Authenticate against database
→ Grant privileges against criteria to provide authorisation
→ Authoritative Reissue, Aging, Revocation
• Tokens, RFID
→ Authenticate against database
→ Grant privileges against criteria to provide authorisation
→ Authoritative Reissue, Aging, Revocation
• Biometrics
→ Authenticate against database
→ Grant privileges against criteria to provide authorisation
• Specific terminal
→ Usually deployed in combination with one of the above
LSE

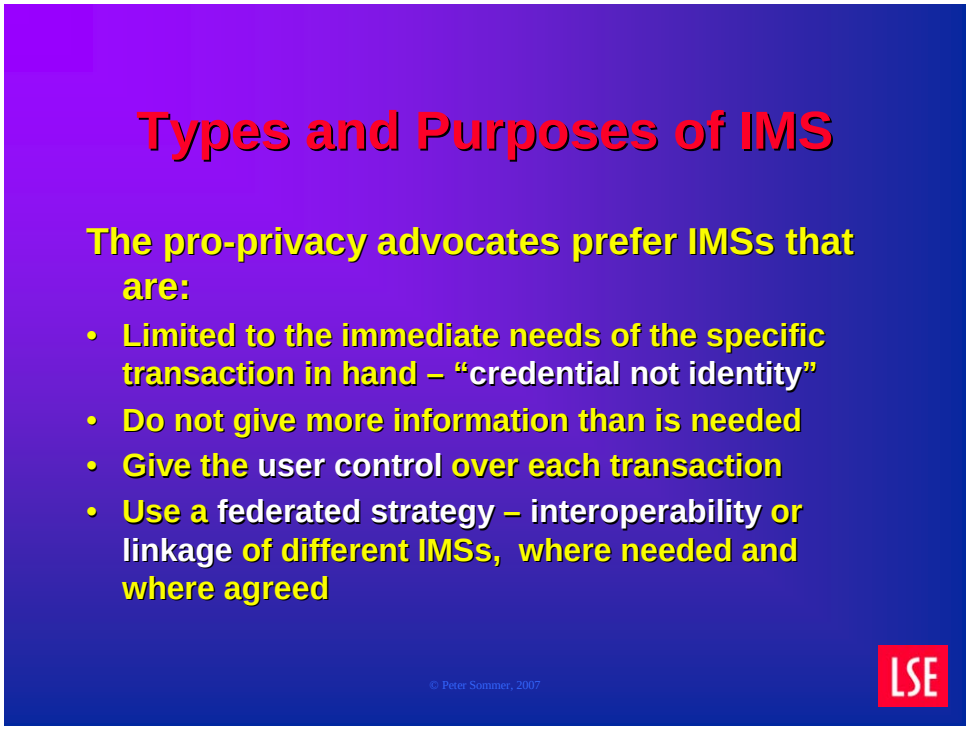

Identity Management Systems
Framework of Policies, Regulations and Law
• Policies:
➔ what are the overall needs, purposes and requirements of IMS?
➔ what unwanted side-effects need to be avoided?
• Regulations, Law:
➔ eg compliance with Data Protection, Human Rights, Employment, Surveillance, Business Records, laws, audit and desirable standards, compliance
© Peter Sommer, 2007
LSE

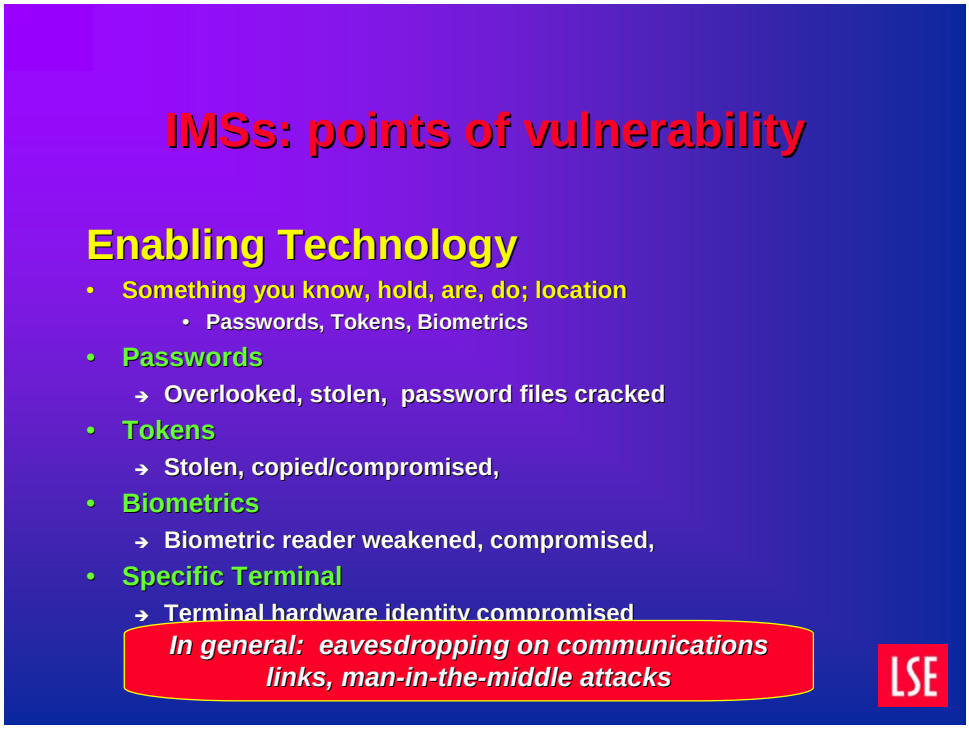

Types and Purposes of IMS
• IMS for account management, implementing authentication, authorisation, and accounting,
• IMS for profiling of user data by an organisation, e.g. detailed log files or data warehouses which support e.g., personalised services or the analysis of customer behaviour
• IMS for user-controlled context-dependent role and pseudonym management.
© Peter Sommer, 2007
LSE

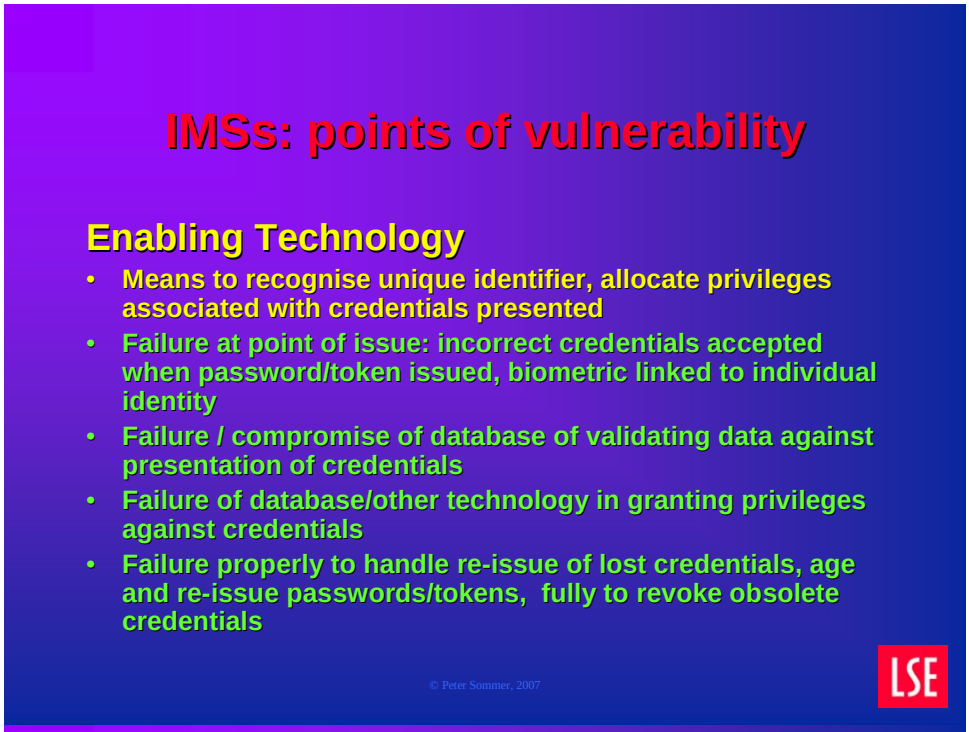

Types and Purposes of IMS
IMS for account management, implementing authentication, authorisation, and accounting
• Used by large organisations for access control to computer systems and networks, etc
→ Inter-company, purchasing systems, ISPs, banks
• eg conventional user-name/password access-control systems, single-sign-on systems, some forms of public key infrastructures
© Peter Sommer, 2007
LSE

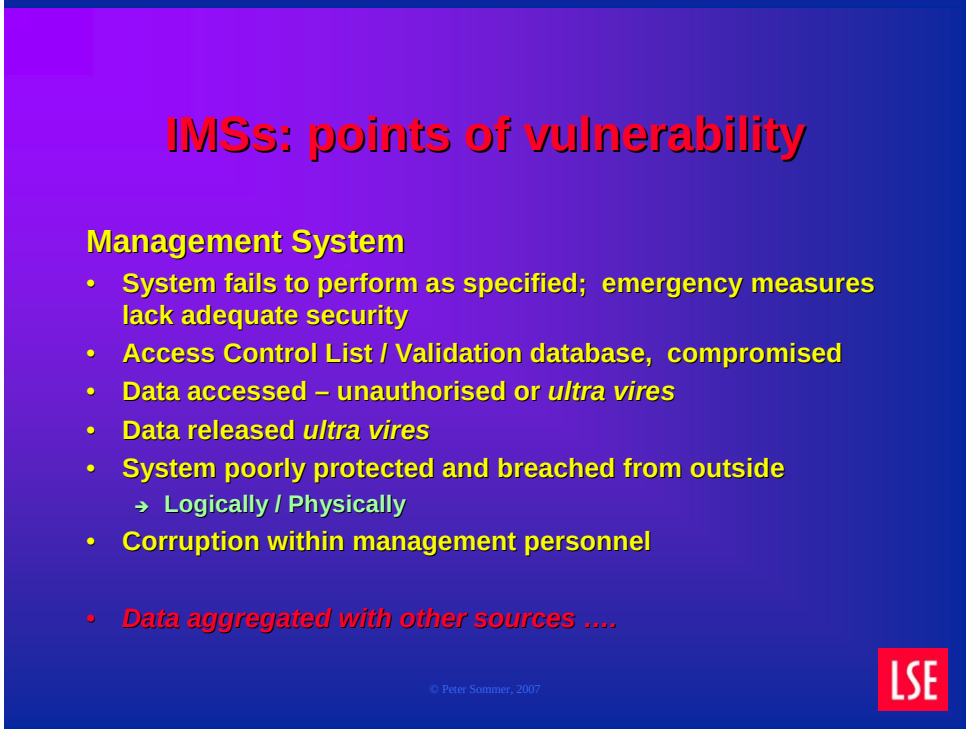

Types and Purposes of IMS
IMS for profiling of user data by an organisation, e.g. detailed log files or data warehouses which support e.g., personalised services or the analysis of customer behaviour
• eg, activity tracking, use of cookies, facilities, "market info/CRM" systems – Amazon, many online retailers, Google, Ebay, cookie deployers – adriver, adclick, hitslink, webstats, doubleclick
© Peter Sommer, 2007
LSE


Types and Purposes of IMS
IMS for user-controlled context-dependent role and pseudonym management.
• Not many practical examples – but where user presents an "identity" limited to the immediate needs of the transaction
© Peter Sommer, 2007
LSE


Types and Purposes of IMS
The pro-privacy advocates prefer IMSs that are:
• Limited to the immediate needs of the specific transaction in hand – "credential not identity"
• Do not give more information than is needed
• Give the user control over each transaction
• Use a federated strategy – interoperability or linkage of different IMSs, where needed and where agreed
© Peter Sommer, 2007
LSE


IMSs: points of vulnerability
Enabling Technology
• Something you know, hold, are, do; location
• Passwords, Tokens, Biometrics
• Passwords
→ Overlooked, stolen, password files cracked
• Tokens
→ Stolen, copied/compromised,
• Biometrics
→ Biometric reader weakened, compromised,
• Specific Terminal
→ Terminal hardware identity compromised
In general: eavesdropping on communications links, man-in-the-middle attacks
LSE


IMSs: points of vulnerability
Enabling Technology
• Means to recognise unique identifier, allocate privileges associated with credentials presented
• Failure at point of issue: incorrect credentials accepted when password/token issued, biometric linked to individual identity
• Failure / compromise of database of validating data against presentation of credentials
• Failure of database/other technology in granting privileges against credentials
• Failure properly to handle re-issue of lost credentials, age and re-issue passwords/tokens, fully to revoke obsolete credentials
© Peter Sommer, 2007
LSE


IMSs: points of vulnerability
Management System
• System fails to perform as specified; emergency measures lack adequate security
• Access Control List / Validation database, compromised
• Data accessed – unauthorised or *ultra vires*
• Data released *ultra vires*
• System poorly protected and breached from outside
→ Logically / Physically
• Corruption within management personnel
• *Data aggregated with other sources ….*
© Peter Sommer, 2007
LSE

IMSs: points of vulnerability

In general: anything based on ICT will be subject over time to *erosion*

- **What once worked well becomes weakened by:**
  - **Prolonged Technical Examination**
  - **Spread of information about vulnerabilities fast and easy over the Internet**
  - **Increasing computer power makes brute force attack more feasible – Moore's Law variant**
  - **Falling computer costs makes brute force attack more feasible**
  - **"Esoteric" hardware/software/technology becomes widely available**

LSE

Forensic Computing

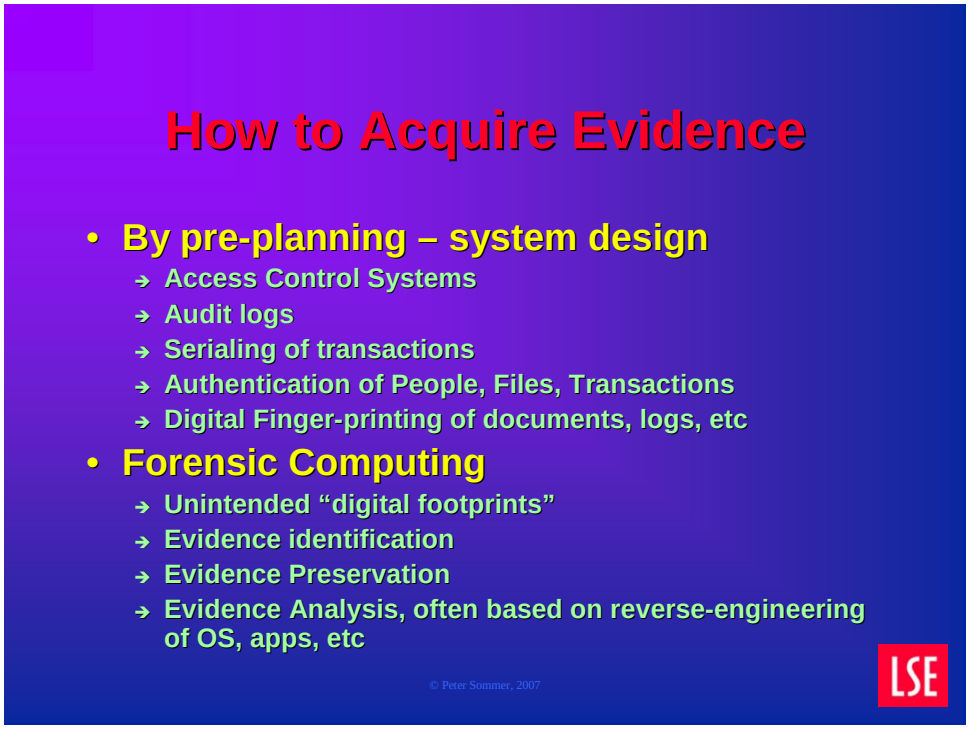
Most presentations are along the lines of:

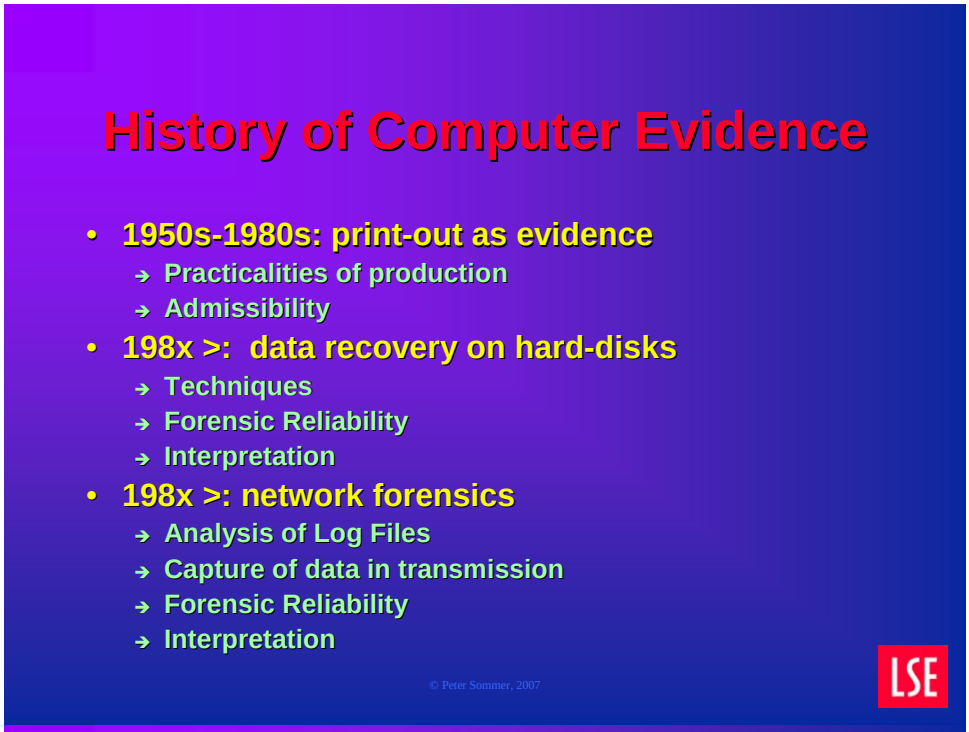
- **What computer forensics can deliver**
  - **Hard disk analysis**
  - **Network data capture and analysis**
- **How to do computer forensics**
- **Protocols and Procedures**

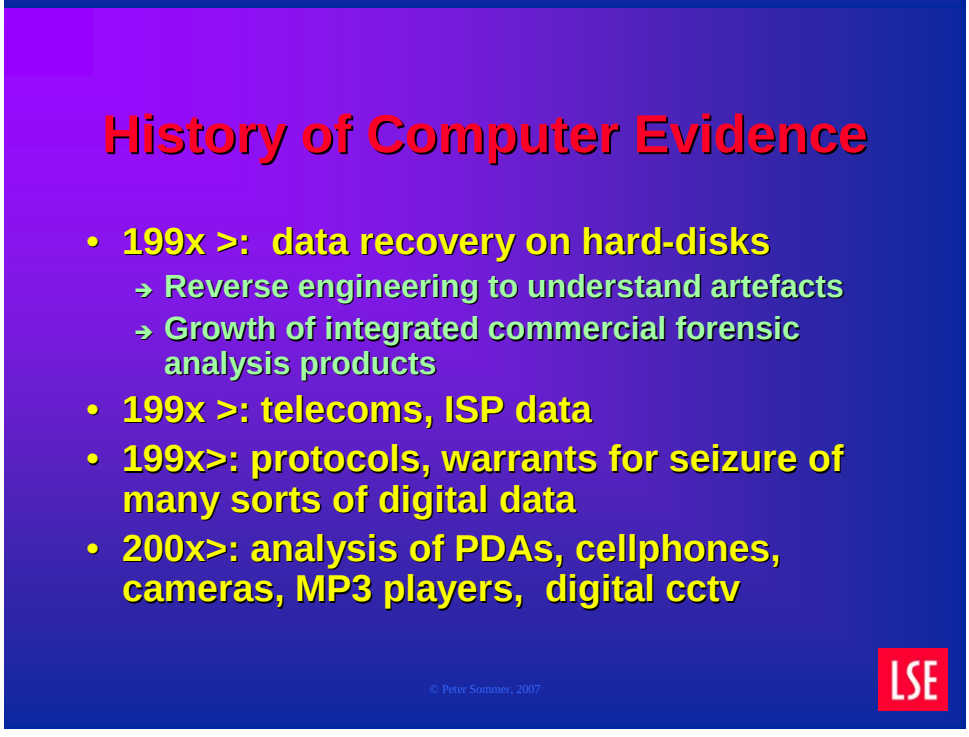
For our purpose I want to look at the nature of Research in Forensic Computing

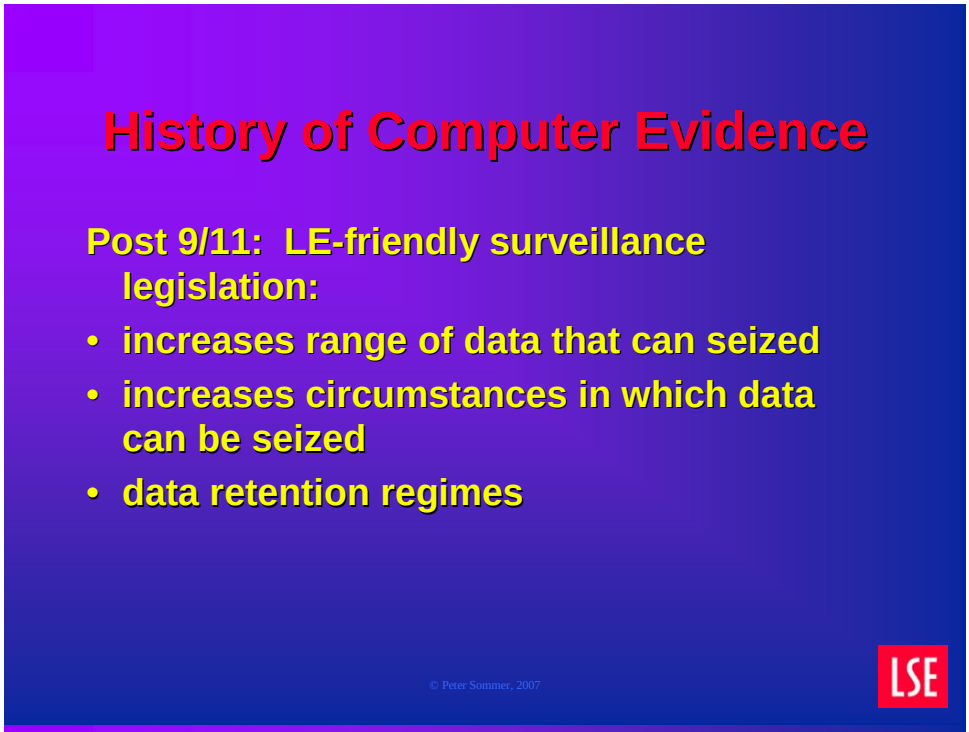
LSE

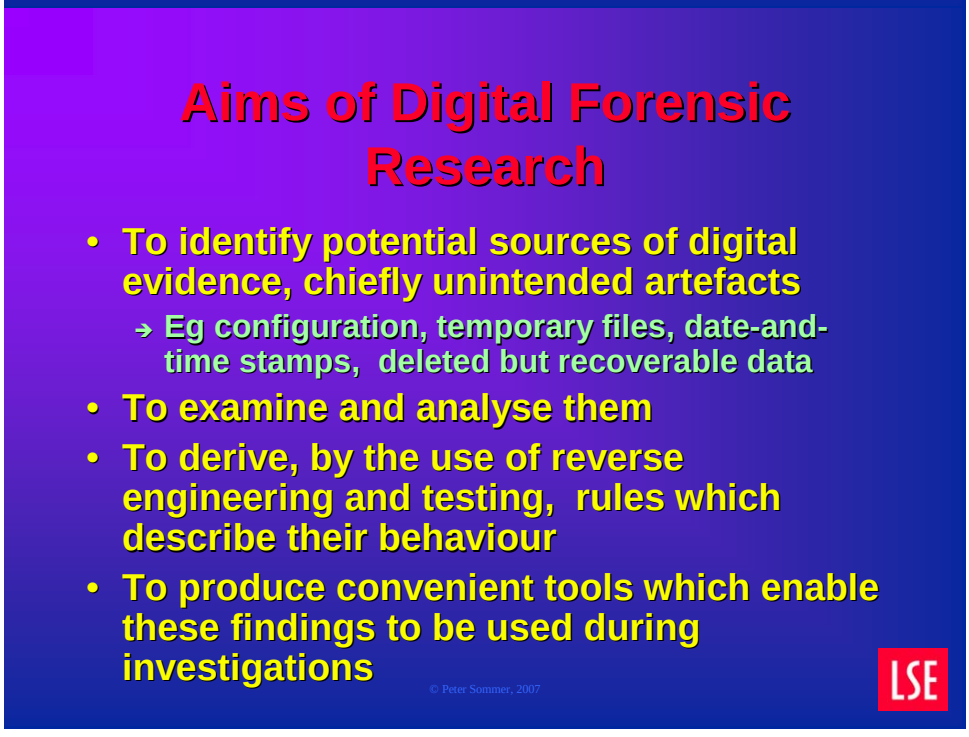

Aims of Digital Forensics
• To identify sources of evidence
• To acquire evidence
• To preserve evidence
• To analyse evidence
• To identify non-obvious sources of evidence
© Peter Sommer, 2007
LSE


How to Acquire Evidence
• By pre-planning – system design
→ Access Control Systems
→ Audit logs
→ Serialing of transactions
→ Authentication of People, Files, Transactions
→ Digital Finger-printing of documents, logs, etc
• Forensic Computing
→ Unintended "digital footprints"
→ Evidence identification
→ Evidence Preservation
→ Evidence Analysis, often based on reverse-engineering of OS, apps, etc
© Peter Sommer, 2007
LSE


History of Computer Evidence
• 1950s-1980s: print-out as evidence
→ Practicalities of production
→ Admissibility
• 198x >: data recovery on hard-disks
→ Techniques
→ Forensic Reliability
→ Interpretation
• 198x >: network forensics
→ Analysis of Log Files
→ Capture of data in transmission
→ Forensic Reliability
→ Interpretation
© Peter Sommer, 2007
LSE

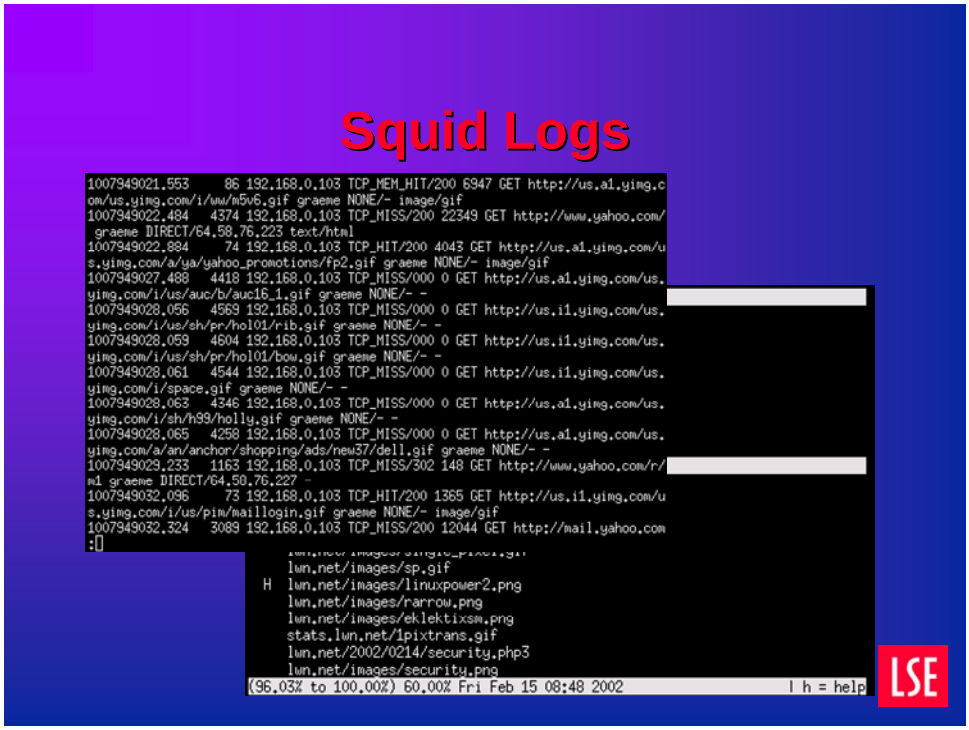

History of Computer Evidence
• 199x >: data recovery on hard-disks
→ Reverse engineering to understand artefacts
→ Growth of integrated commercial forensic analysis products
• 199x >: telecoms, ISP data
• 199x>: protocols, warrants for seizure of many sorts of digital data
• 200x>: analysis of PDAs, cellphones, cameras, MP3 players, digital cctv
© Peter Sommer, 2007
LSE

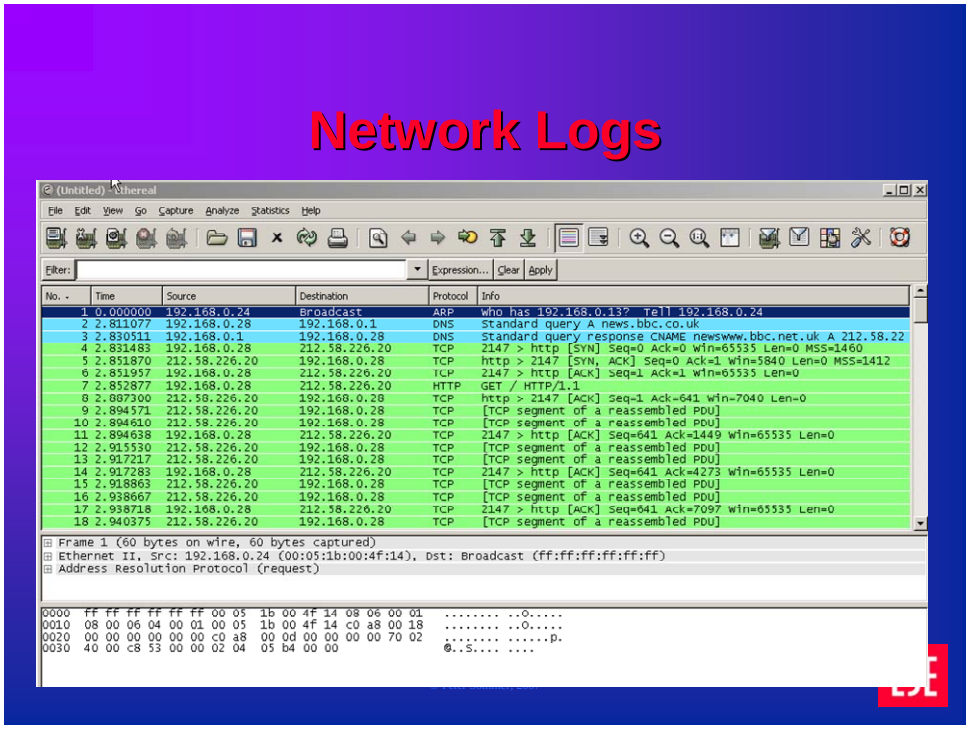

History of Computer Evidence
Post 9/11: LE-friendly surveillance legislation:
• increases range of data that can seized
• increases circumstances in which data can be seized
• data retention regimes
© Peter Sommer, 2007
LSE


Aims of Digital Forensic Research
• To identify potential sources of digital evidence, chiefly unintended artefacts
➔ Eg configuration, temporary files, date-and-time stamps, deleted but recoverable data
• To examine and analyse them
• To derive, by the use of reverse engineering and testing, rules which describe their behaviour
• To produce convenient tools which enable these findings to be used during investigations
© Peter Sommer, 2007
LSE


Aims of Digital Forensic Research
Motivations:
• To solve a problem within a particular investigation
• Geek Fun
• To develop a commercial product
• To improve one's academic standing
• To give Law Enforcement an advantage?
© Peter Sommer, 2007
LSE
Digital Forensic Research
Hard-disk based:
• Recovered Files
→ Deleted, modified files – goes to intent
• MSOffice "properties" / metadata
→ May show authorship, revisions
• Internet cache
→ Shows patterns and history of Internet usage – goes to intent, state of mind
→ Search engine requests
• OS set-up
→ Accounts, passwords, may show authorship
• System Registry (Windows)
© Peter Sommer, 2007
LSE


Digital Forensic Research
• System Restore Points
• P2P software artefacts, database and logging files
• Chat software artefacts, database and logging files
• Exif Data
• LNK files
• Thumbnails – thumbs.db etc
• Email headers
• Desktop indexing artefacts
© Peter Sommer, 2007
LSE
Digital Forensic Research
3rd party logs:
• Web logs
• IDS logs
• Remote service anti-virus logs
• Telco logs, landline, cell, ISP
• ISP RADIUS logs
Aim is to audit activity, seek corroboration and hence identify specific individuals
© Peter Sommer, 2007
LSE


Squid Logs
1007949021.553 86 192.168.0.103 TCP_MEM_HIT/200 6947 GET http://us.a1.yimg.com/us.yimg.com/i/ww/m5v6.gif graeme NONE/- image/gif
1007949022.484 4374 192.168.0.103 TCP_MISS/200 22349 GET http://www.yahoo.com/ graeme DIRECT/64.58.76.223 text/html
1007949022.884 74 192.168.0.103 TCP_HIT/200 4043 GET http://us.a1.yimg.com/us.yimg.com/a/ya/yahoo_promotions/fp2.gif graeme NONE/- image/gif
1007949027.488 4418 192.168.0.103 TCP_MISS/000 0 GET http://us.a1.yimg.com/us.yimg.com/i/us/auc/b/auc16_1.gif graeme NONE/- -
1007949028.056 4569 192.168.0.103 TCP_MISS/000 0 GET http://us.i1.yimg.com/us.yimg.com/i/us/sh/pr/hol01/rib.gif graeme NONE/- -
1007949028.059 4604 192.168.0.103 TCP_MISS/000 0 GET http://us.i1.yimg.com/us.yimg.com/i/us/sh/pr/hol01/bow.gif graeme NONE/- -
1007949028.061 4544 192.168.0.103 TCP_MISS/000 0 GET http://us.i1.yimg.com/us.yimg.com/i/space.gif graeme NONE/- -
1007949028.063 4346 192.168.0.103 TCP_MISS/000 0 GET http://us.a1.yimg.com/us.yimg.com/i/sh/h99/holly.gif graeme NONE/- -
1007949028.065 4258 192.168.0.103 TCP_MISS/000 0 GET http://us.a1.yimg.com/us.yimg.com/a/an/anchor/shopping/ads/new37/dell.gif graeme NONE/- -
1007949029.233 1163 192.168.0.103 TCP_MISS/302 148 GET http://www.yahoo.com/r/ md graeme DIRECT/64.58.76.227 -
1007949032.096 73 192.168.0.103 TCP_HIT/200 1365 GET http://us.i1.yimg.com/us.yimg.com/i/us/pim/maillogin.gif graeme NONE/- image/gif
1007949032.324 3089 192.168.0.103 TCP_MISS/200 12044 GET http://mail.yahoo.com
lwn.net/images/sp.gif
H lwn.net/images/linuxpower2.png
lwn.net/images/rarrow.png
lwn.net/images/eklektixsm.png
stats.lwn.net/1pixtrans.gif
lwn.net/2002/0214/security.php3
lwn.net/images/security.png
(96.03% to 100.00%) 60.00% Fri Feb 15 08:48 2002
h = help
LSE


Network Logs
(Untitled) - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
1 0.000000 192.168.0.24 Broadcast ARP who has 192.168.0.13? Tell 192.168.0.24
2 2.811077 192.168.0.28 192.168.0.1 DNS Standard query A news.bbc.co.uk
3 2.830511 192.168.0.1 192.168.0.28 DNS Standard query response CNAME newswww.bbc.net.uk A 212.58.22
4 2.831483 192.168.0.28 212.58.226.20 TCP 2147 > http [SYN] Seq=0 Ack=0 Win=65535 Len=0 MSS=1460
5 2.851870 212.58.226.20 192.168.0.28 TCP http > 2147 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1412
6 2.851957 192.168.0.28 212.58.226.20 TCP 2147 > http [ACK] Seq=1 Ack=1 Win=65535 Len=0
7 2.852877 192.168.0.28 212.58.226.20 HTTP GET / HTTP/1.1
8 2.887300 212.58.226.20 192.168.0.28 TCP http > 2147 [ACK] Seq=1 Ack=641 Win=7040 Len=0
9 2.894571 212.58.226.20 192.168.0.28 TCP [TCP segment of a reassembled PDU]
10 2.894610 212.58.226.20 192.168.0.28 TCP [TCP segment of a reassembled PDU]
11 2.894638 192.168.0.28 212.58.226.20 TCP 2147 > http [ACK] Seq=641 Ack=1449 Win=65535 Len=0
12 2.915530 212.58.226.20 192.168.0.28 TCP [TCP segment of a reassembled PDU]
13 2.917217 212.58.226.20 192.168.0.28 TCP [TCP segment of a reassembled PDU]
14 2.917283 192.168.0.28 212.58.226.20 TCP 2147 > http [ACK] Seq=641 Ack=4273 Win=65535 Len=0
15 2.918863 212.58.226.20 192.168.0.28 TCP [TCP segment of a reassembled PDU]
16 2.938667 212.58.226.20 192.168.0.28 TCP [TCP segment of a reassembled PDU]
17 2.938718 192.168.0.28 212.58.226.20 TCP 2147 > http [ACK] Seq=641 Ack=7097 Win=65535 Len=0
18 2.940375 212.58.226.20 192.168.0.28 TCP [TCP segment of a reassembled PDU]
Frame 1 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: 192.168.0.24 (00:05:1b:00:4f:14), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)
0000 ff ff ff ff ff ff 00 05 1b 00 4f 14 08 06 00 01 ....O.....
0010 08 00 06 04 00 01 00 05 1b 00 4f 14 c0 a8 00 18 ....O.....
0020 00 00 00 00 00 00 c0 a8 00 0d 00 00 00 00 70 02 ....p.
0030 40 00 c8 53 00 00 02 04 05 b4 00 00 @..S.... ....
LSE


Digital Forensic Research
Interception
• Who contacted whom, when, for how long – and what was said.
• Forensics: how do you do this practically and with integrity-checking?
• Law: how do you do this legally?
➔ Most jurisdictions distinguish between content and traffic data – in terms of warrants required / level of intrusion
© Peter Sommer, 2007
LSE


Practical Investigations
• Multiple streams of evidence to build a detailed picture
• Corroboration from several weak streams
© Peter Sommer, 2007
LSE

Data Protection Principles

7. Appropriate measures against unauthorised and unlawful use
8. Non-transference outside EU

Exemptions:

National Security, crime, taxation, health, education, social work, regulatory activity, journalism, research, history, statistics, legal proceedings

LSE

FIDIS type 2 IMSs:

- Cell-site analysis
- Automatic Number Plate Recognition / Traffic Congestion Charging
- Radio-based traffic charging
- Oyster Cards
- Swipe cards for physical access control
- CCTV + facial recognition

LSE


FIDIS type 2 IMSs:
• Credit cards – general and specialised: purchases plus locations
• Store Loyalty cards
• Library books taken out
• Medical databases
• Education databases
• Google logs
© Peter Sommer, 2007
LSE
Broad-based ID cards:
• Leave a trail each time they are presented:
• Locations, movements
• Use of social and medical services
© Peter Sommer, 2007
LSE

Understanding the Problem

- Data obtained by LE without warrant remains unusable in court proceedings
- Data held by 3rd parties and then ceded to LE under warrant: provided original warrant is valid, 3rd parties may not be able to restrain subsequent use
- Data obtained by LE with a warrant but used *ultra vires* through technical ingenuity – courts may lack the understanding to forbid its use.
- Position of data aggregation by LE unclear but appears unprotected by courts

LSE

Remedies?

- First step is to describe the problem
- Can we frame precise laws?
- Do we grant judges discretion to exclude for "unfairness" or "abuse of process"?
- ????

LSE


FIDIS
Profiling Meeting
1 October 2007
NFI
Identity Management Systems:
the forensic dimension
Peter Sommer
London School of Economics
© Peter Sommer, 2007
LSE

Outline

1. Mission, motivation and activities of KECIDA
2. Example activity: exploration of Social Network Analysis

KECIDA: Motivation

- The scale of individual agencies is too small to efficiently organize the required capacity, knowledge and facilities
- Many efforts like building knowledge are carried out multiple times.
- Natural mechanisms for synergy between applications are lacking if they are organized individually.

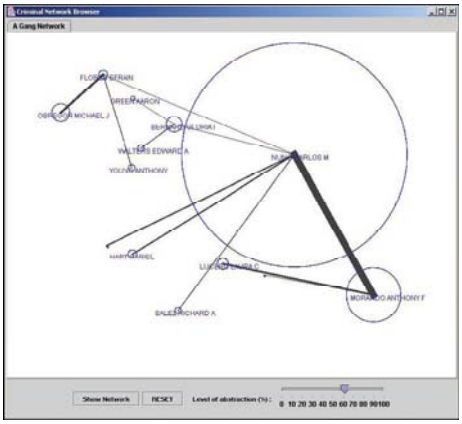
KECIDA: Activities (2)

- To supply a safe environment where other security agencies (OOV) can work together and try out state-of-the-art analysis techniques without interrupting their operational processes.
- To mediate between scientific institutes and security agencies and between suppliers of products and security agencies.
- To organize training to use relevant methods and techniques.

SNA - criminal network analysis

- What subgroups exist in the network?
- How do these subgroups interact with each other?
- What is the overall structure of the network?
- What are the roles network members play?

SNA – Coplink Example (2)



- Several subgroups with their leaders detected
- Strength of relationships between subgroups calculated

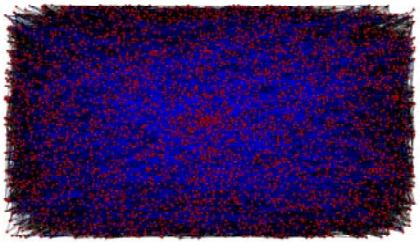
SNA - Activities

- Collect literature
- Establish contacts with universities
- 'Quickscan' SNA software
- Pilot project

SNA - issues (2)

Large datasets

- Computer memory limitations
- Comprehensible visualization



>>> first identify components or clusters and select partitions

SNA - issues (1)

- Data transformation - extracting links
- Merging data sources - record matching
- Multiple types of relations - modality
- User friendliness of software
  - (Open source) freeware from the scientific community - for developing?
  - Commercial software for end users - for implementing?

SNA - issues (3)

How to use the result?

- in an investigation
  - network detection
  - network visualization
  - network parameters: centrality, betweenness, closeness, density
  - equivalence of networks
- in court
  - reliability, viability, evidence?

Pilot project

Challenges

Coordinate working with different agencies

- Define a realistic scope
- Select data to use
- Choose software
- Security measures
- Privacy regulations
- Merge data from different agencies
- Share project results

SNA - share knowledge (2)

Expectation management

- You can't just "load a database", look at the pictures and start arresting new suspects.
- Most of the work will be preparation of the data.
- Human intelligence is necessary to get usable results.

FORENSIC PROFILING

FIDIS - WP 6.7

R. A. Reiss

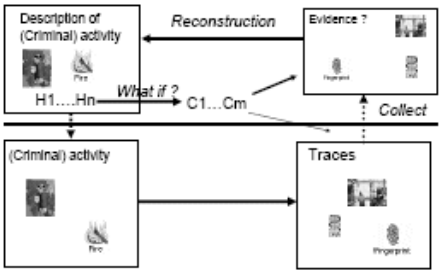
Olivier RIBAUX, NFI, October 1st, 2007

// FORENSIC PROFILING

Forensic profiling:

What are we talking about ?

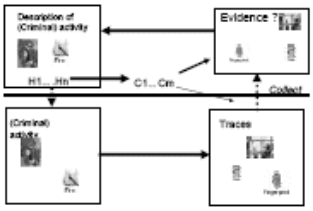
// FORENSIC PROFILING



// MANY ACTORS

What ?
Who ?
Why ?
Where
When ?
How ?

•Judges
•Jury
•Investigator
•Intelligence officer
•Experts
•Victim, witness
•…
•Forensic scientist



// FORENSIC PROFILING

« The term forensic, as used in this report, refers to information that is used in court as evidence »

FIDIS, WP 6.1., final version p. 10

// HIERARCHY OF PROPOSITIONS

THREE LEVEL FRAMEWORK:

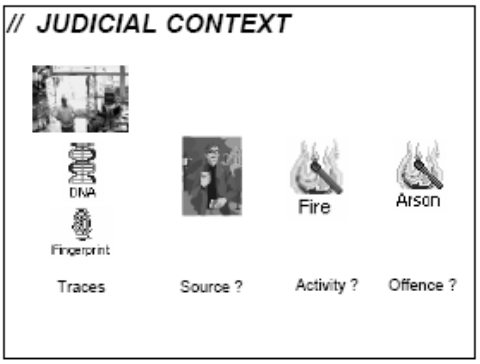
•SOURCE

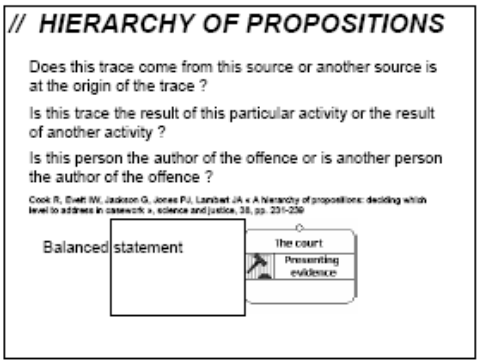
•ACTIVITY

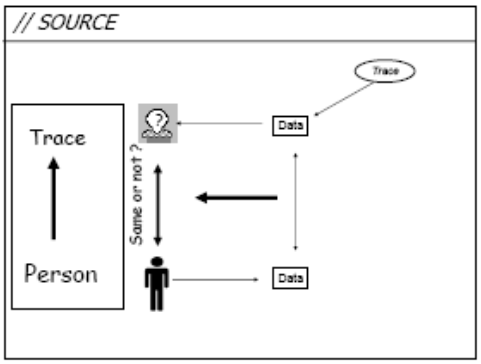
•OFFENCE

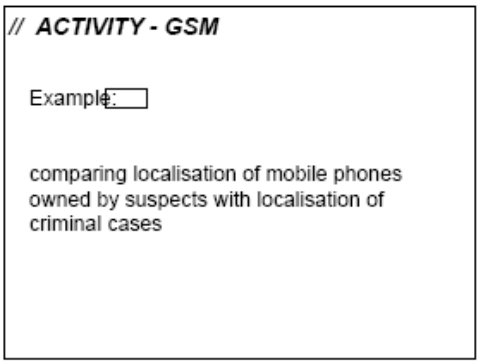
Cook R, Evett IW, Jackson G, Jones PJ, Lambert JA « A hierarchy of propositions: deciding which level to address in casework », science and justice, 38, pp. 231-239

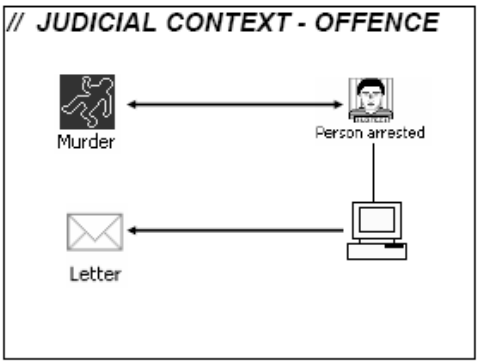
1

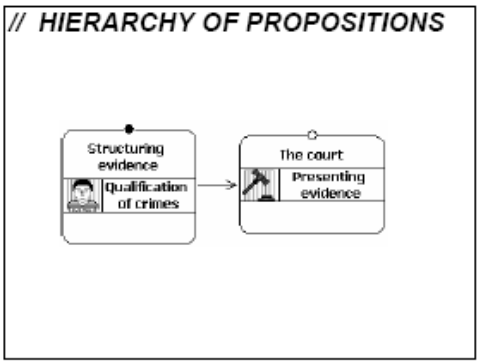

// JUDICIAL CONTEXT
DNA
Fingerprint
Fire
Arson
Traces
Source ?
Activity ?
Offence ?


// HIERARCHY OF PROPOSITIONS
Does this trace come from this source or another source is at the origin of the trace ?
Is this trace the result of this particular activity or the result of another activity ?
Is this person the author of the offence or is another person the author of the offence ?
Balanced statement
The court
Presenting evidence


// SOURCE
Trace
Person
Same or not ?
Data
Data

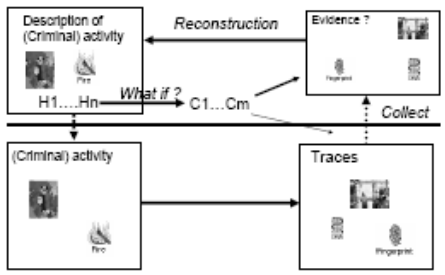

// ACTIVITY - GSM
Example:
comparing localisation of mobile phones owned by suspects with localisation of criminal cases


// JUDICIAL CONTEXT - OFFENCE
Murder
Person arrested
Letter


// HIERARCHY OF PROPOSITIONS
Structuring evidence
Qualification of crimes
The court
Presenting evidence

2

// FORENSIC PROFILING



// JUDICIAL CONTEXT - EXCLUSION

Does the arrested person and his assumed activity are consistent with the collated data?

Refutation of hypotheses

Collection of new data

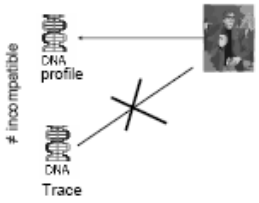
// CONNECTIONS

Example:

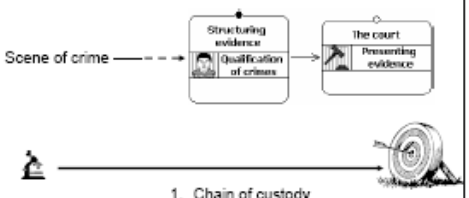
Who has been in connection with who ?
(analysis of relations)

// JUDICIAL CONTEXT - EXCLUSION

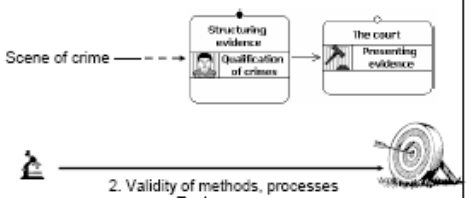
This person is not the source of this data (DNA for instance)



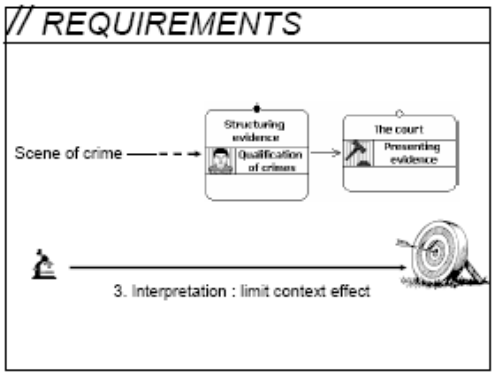
// REQUIREMENTS

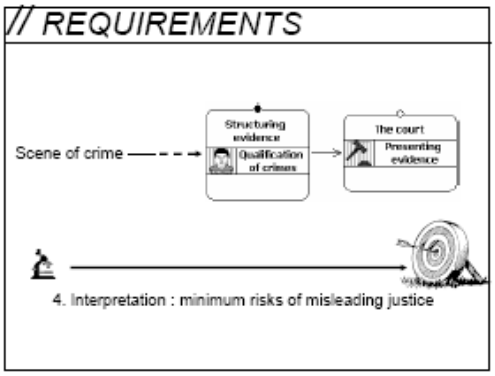


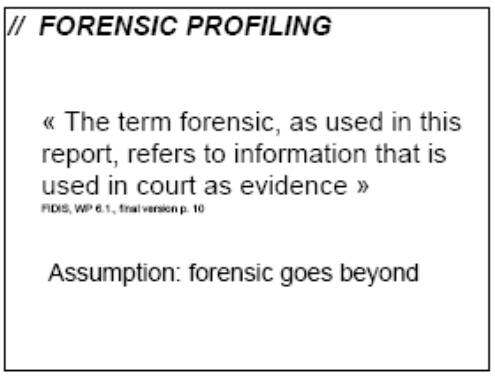
// REQUIREMENTS

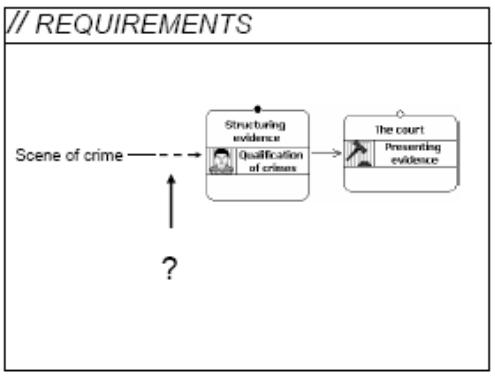


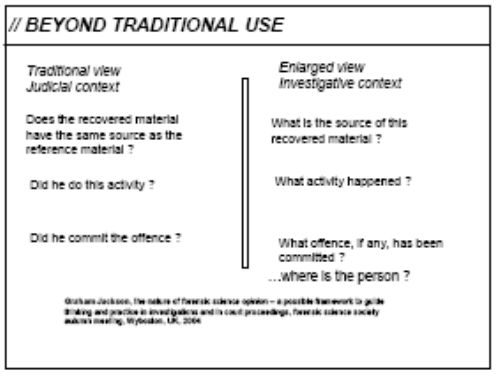
3

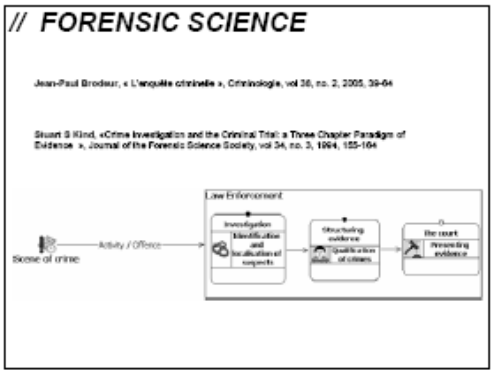

// REQUIREMENTS
Scene of crime
Structuring evidence
Qualification of crimes
The court
Presenting evidence
3. Interpretation : limit context effect


// REQUIREMENTS
Scene of crime
Structuring evidence
Qualification of crimes
The court
Presenting evidence
4. Interpretation : minimum risks of misleading justice


// FORENSIC PROFILING
« The term forensic, as used in this report, refers to information that is used in court as evidence »
FIDIS, WP 6.1., final version p. 10
Assumption: forensic goes beyond


// REQUIREMENTS
Scene of crime
Structuring evidence
Qualification of crimes
The court
Presenting evidence
?


// BEYOND TRADITIONAL USE
Traditional view
Judicial context
Does the recovered material have the same source as the reference material ?
Did he do this activity ?
Did he commit the offence ?
Enlarged view
Investigative context
What is the source of this recovered material ?
What activity happened ?
What offence, if any, has been committed ?
...where is the person ?

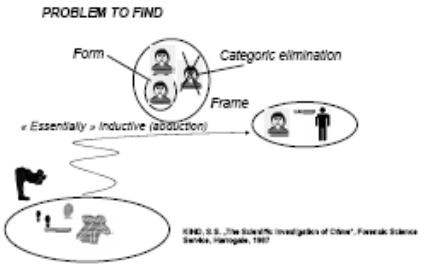

// FORENSIC SCIENCE
Jean-Paul Brodeur, « L'enquête criminelle », Criminologie, vol 38, no. 2, 2005, 39-64
Stuart S Kind, «Crime Investigation and the Criminal Trial: a Three Chapter Paradigm of Evidence », Journal of the Forensic Science Society, vol 34, no. 3, 1994, 155-164
Law Enforcement
Scene of crime
Activity / Offence
Investigation
Identification and localisation of suspects
Structuring evidence
Qualification of crimes
The court
Presenting evidence

// BEYOND TRADITIONAL USE

Traditional view Judicial context	Enlarged view Investigative context
Interpreting and presenting evidence	Identify, localise
Well defined questions	Questions are manifold, complex inference patterns, goes often through reconstruction
De-contextualisation	Integrated into the investigative process
Minimum risk	Draw hypotheses

Graham Jackson, the nature of forensic science opinion – a possible framework to guide thinking and practice in investigations and in court proceedings, Forensic science society autumn meeting, Wyboston, UK, 2004

// GENERALISATION: FRAME ET FORM



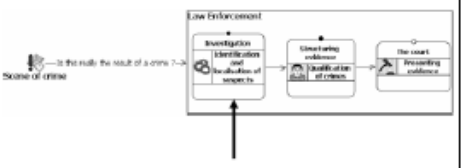
KIND, S.S. „The Scientific Investigation of Crime", Forensic Science Service, Harrogate, 1987

// CATEGORIC ELIMINATION

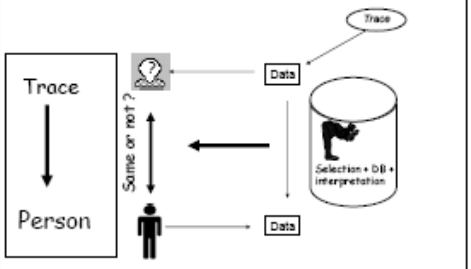
Example: DNA screening (systematic elimination on the basis of a determined frame)

KIND, S.S. „The Scientific Investigation of Crime", Forensic Science Service, Harrogate, 1987

// FORENSIC PROFILING



// SOURCE



// SOURCE

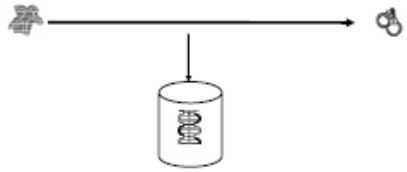
Example:

DNA databases across Europ:

- differences in proportion of the population profiled, proportion of traces/profiles

5

// **PARTIAL DNA**



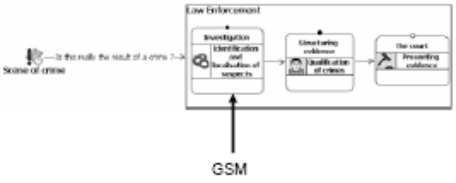
Partial DNA, mixtures (~16 % of traces with a profile)

Taroni F, Castella V, Ribaux O, Hicks-Champod T « *Statistical foundations and ethical considerations on partial DNA profiles and familial searching using the Swiss National DNA Database* », Fonds National Suisse de la Recherche Scientifique, no. 100011-113881)

// *FAMILIAL SEARCH*

Familial search ?

// **FORENSIC PROFILING**



GSM

// **GSM**

Example: localisation through GSM

- geographic « profiles », mobility
- where suspects live
- where criminals operate

// **FORENSIC PROFILING**

Credit card theft and withdrawal

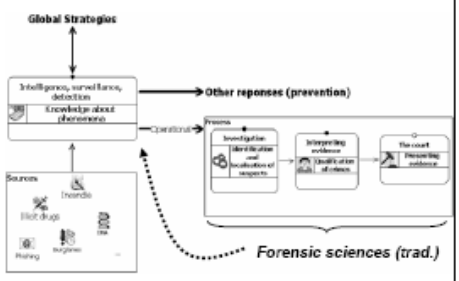
// **FORENSIC PROFILING**

Is this forensic profiling ?

Assumption: we can go further

6

// INTELLIGENCE – DETECTION - SURVEILLANCE



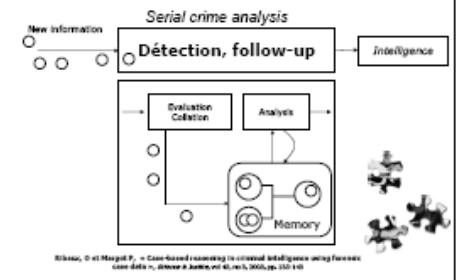
// IDENTITY CONTROLS

Example of changes:

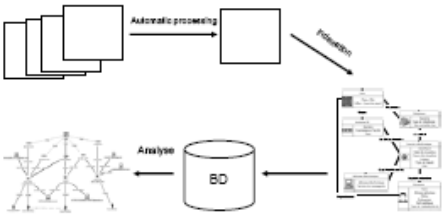
Systematic use of IdentiScan remote terminals, via AFIS databases:

Nature of the controls change dramatically

// INTELLIGENCE, SURVEILLANCE, DETECTION

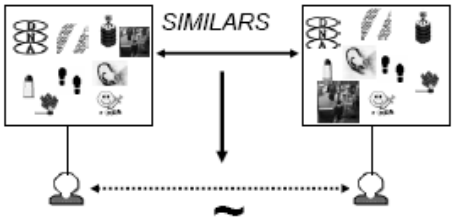


// FORMALISATION BY THEMES



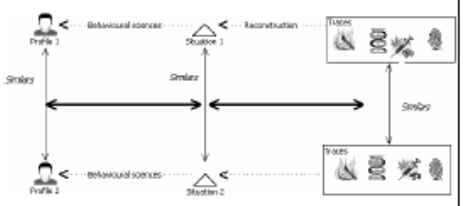
Source – activity – offence ? Where is the offence ?

// BASIC CONTRIBUTION



Sources, activities, offences ?

// SERIAL CRIME ANALYSIS



Linking crimes through physical traces

7

// SERIAL CRIME ANALYSIS

Linking crimes through physical traces:

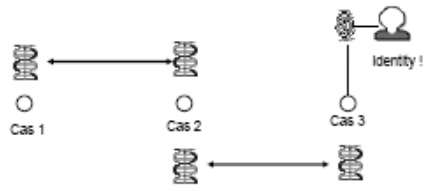
Useful :

- Detecting series of crimes
- Understanding some aspects of criminal phenonema without working on nominal data: mobility, criminal career, specialisation of criminals, size and structure of the phenomena (organisation ?)

Easy ?

In reality not, because of separation of domains, specialties and restricted view on forensic science

// SERIAL CRIME ANALYSIS



// CARD THEFTS

// CONNECTING THE DOTS

Main failure in intelligence:

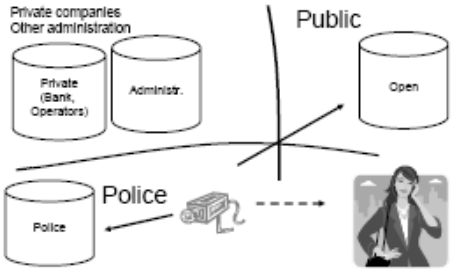
- *legal framework*
- *organisations*
- *separations of disciplines*
- *communication*
- *methods (lack of formalisation)*
- *knowledge*
- *techniques*

// INTERNET MONITORING

Real time monitoring, examples:

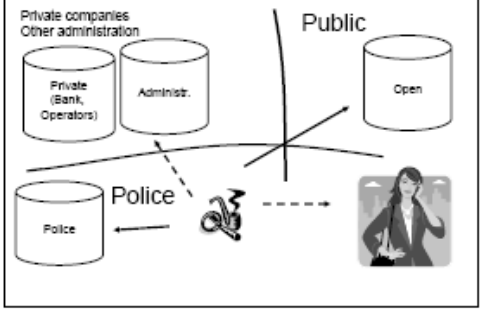
- Internet videos downloading
- Newsgroups surveillance
- Nigerian scammers
- Couternfeits diploma
- Counterfeits watches
- GSM call pattern analysis
- Credit cards thefts and uses
- …

// DIFFERENCES - SOURCES

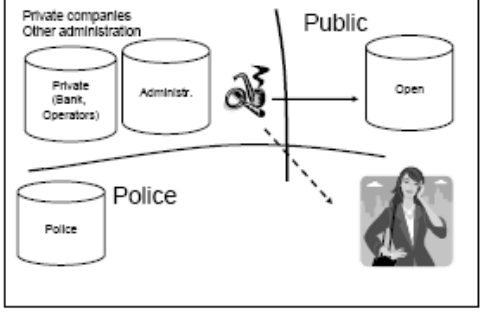


8

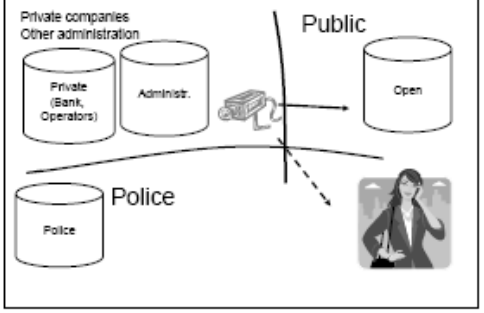
// DIFFERENCES - SOURCES



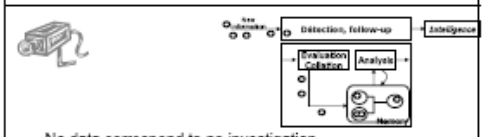
// FORENSIC APPROACH ?



// FORENSIC ?



// CONCLUSION



- No data correspond to no investigation
- No exchange of data lead inevitably to linkage blindness
- Too much data, but not enough analysis
- Ill-defined processes lead to linkage blindness, too many false positives – think small, tractable
- Assessment (what works and what do not work) ?

Fundamental research

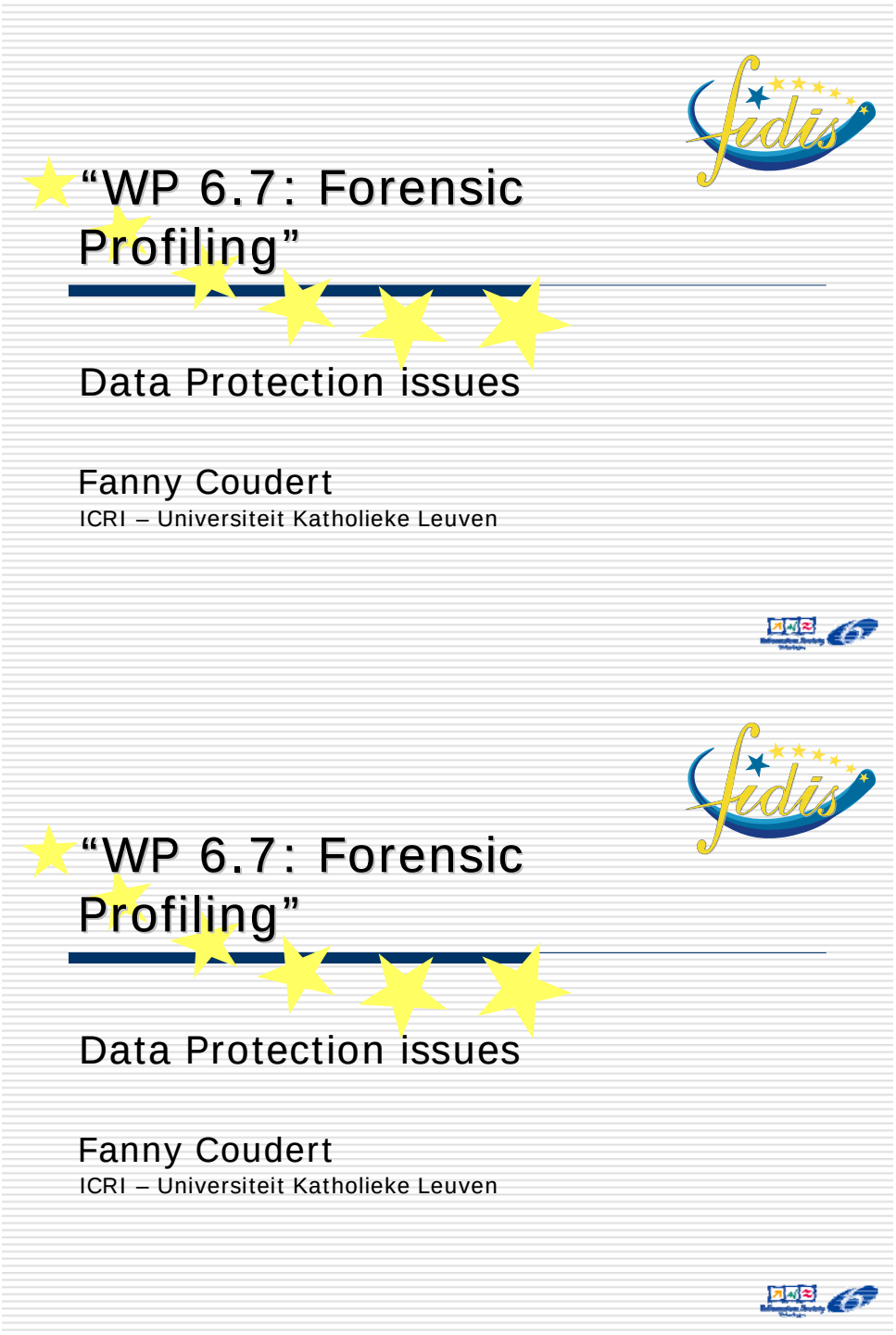
// CONCLUSION ? - provoking statement

Pour **Brodeur** (Le renseignement, distinctions préliminaires, Revue Canadienne de Criminologie et de Justice Pénale (47) 1, p. 40): « Nous estimons en effet qu'au regard de la puissance d'intrusion des moyens de recueillir des données sur les personnes et de l'érosion sérieuse des garanties juridiques protégeant les renseignements personnels, la vie privée est une notion maintenant obsolète. La menace qui pèse n'est pas tant que l'Etat soit informé sur nous mais que les renseignements qu'il a accumulé soient incorrects et conduisent à des décisions clandestines de grande conséquence pour nos vies (…). Or, la validation des renseignements que possèdent les services de renseignement de toute nature ou, autrement dit, le contrôle de qualité, appartient de façon plus étroite à l'obligation de résultat (…) qu'à l'obligation de moyens(…). C'est pourquoi le maintien de l'obligation de résultat, entendue comme contrôle de qualité, peut se révéler un instrument puissant de protection des libertés civiles ».

// THANK YOU

- Anne-Laure TERRETAZ-ZUFFEREY
- Quentin ROSSY
- Damien DESSIMOZ

9


"WP 6.7: Forensic Profiling"
Data Protection issues
Fanny Coudert
ICRI – Universiteit Katholieke Leuven
"WP 6.7: Forensic Profiling"
Data Protection issues
Fanny Coudert
ICRI – Universiteit Katholieke Leuven


Agenda
Applicability of data protection legislation
Data protection implications of Profiling
Questions and Answers
27.12.2007
FIDIS - Future of Identity in the Information Society (No. 507512)
2
Concept of Personal data
"Information related to identified or identifiable individual"
- Direct/Indirect relation between the data and the individual
- Possible link to be established
- Intention of the controller: e.g. damages caused by graffiti
27.12.2007
FIDIS - Future of Identity in the Information Society (No. 507512)
4

Limited scope of application of the Data Protection Directive

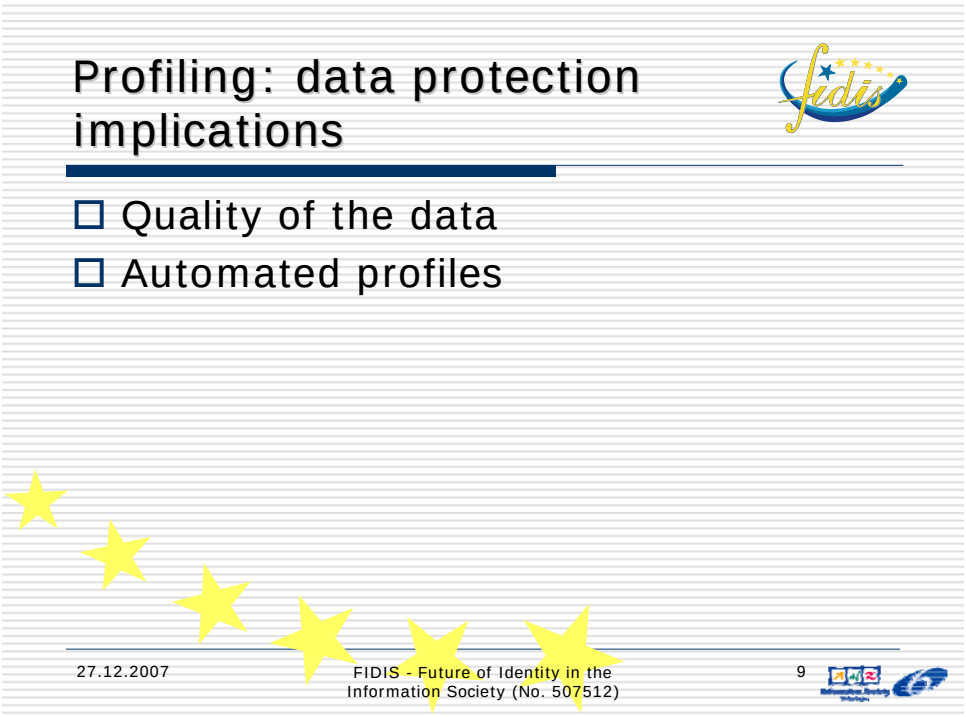
- Data Protection Directive only applies to First Pillar activities
- Forensic Profiling usually pertains to IIIrd Pillars activities
- Personal data obtained from the Ist Pillar activities: the PNR Judgement

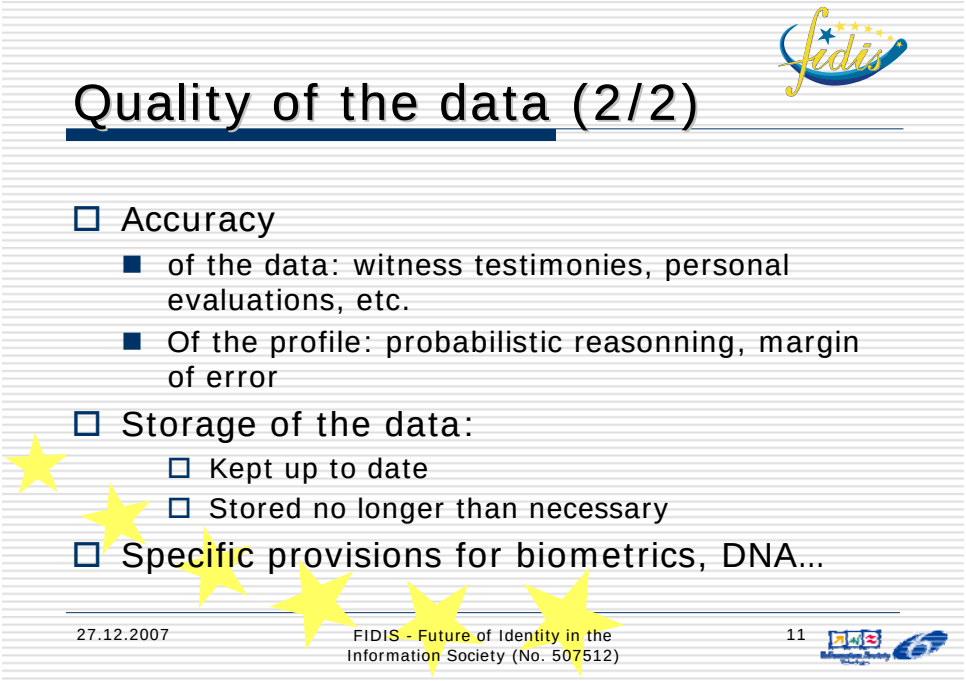
27.12.2007 FIDIS - Future of Identity in the Information Society (No. 507512) 6

Agenda

- Applicability of data protection legislation
- Data protection implications of Profiling
- Questions and Answers

27.12.2007 FIDIS - Future of Identity in the Information Society (No. 507512) 8


Profiling: data protection implications
Quality of the data
Automated profiles
27.12.2007
FIDIS - Future of Identity in the Information Society (No. 507512)
9

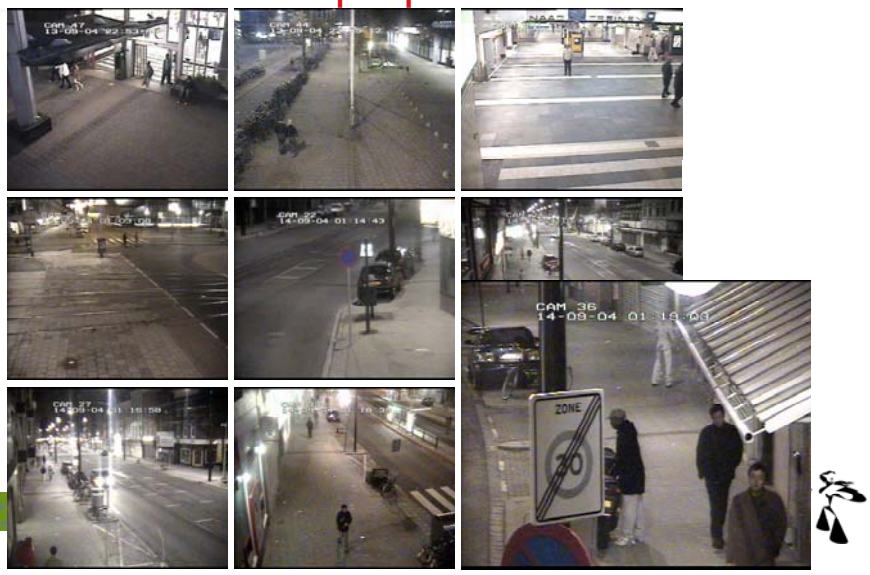

Quality of the data (2/2)
Accuracy
of the data: witness testimonies, personal evaluations, etc.
Of the profile: probabilistic reasonning, margin of error
Storage of the data:
Kept up to date
Stored no longer than necessary
Specific provisions for biometrics, DNA...
27.12.2007
FIDIS - Future of Identity in the Information Society (No. 507512)
11


Questions and Answers
Thank you for your attention!
Any questions?
fanny.coudert@law.kuleuven.be
27.12.2007
FIDIS - Future of Identity in the Information Society (No. 507512)
13

Outline

- Introduction
- Keileweg experiment
- Casework – further developments
- Software

Where did the perpetrators come from?



Problems current procedure

- Lack of context (analyst needs to know the scene)
- No connection between different video streams
- Playing and replaying important parts is a lot of work
- Combining data to other evidence is difficult (phone cams, GSM-data etc)

Aim of the project

The aim of the project is to get an organization for:

- Finding and downloading CCTV.
- Converting CCTV data into synchronized movie files.
- Analyzing CCTV, and movies from other sources, in context of space and time.
- Updating technology and 3d-models.
- Research on better methods for tracking people and cars, and detection of patterns in movements that require police attention.

Aim of the project

The aim of the project is to get an organization for:

- Finding and downloading CCTV.
- Converting CCTV data into synchronized movie files.
- Analyzing CCTV, and movies from other sources, in context of space and time.
- Updating technology and 3d-models.
- Research on better methods for tracking people and cars, and detection of patterns in movements that require police attention.

CCTV data

- NFI got permission to use public CCTV data for experiments.
- Footage of 12 different security cameras in Rotterdam was obtained.

‘Perpetrators’

- 4 people
- 1 car
- 1,5 hours

New procedure

- Synchronisation of video streams
- Building of a 3D model
- Placing of virtual cameras
- 3D reconstruction of movements

Synchronisation

Complications:

- Multiplexed video streams
- Dynamic frame rates

Future:

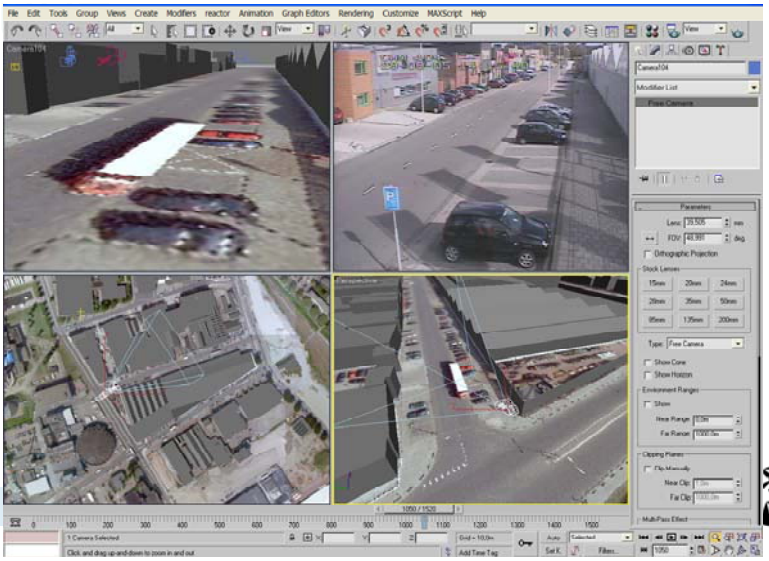
Optical Character Recognition

3D model by aerial stereo photography

- Large area
- Not very much detail
- Accuracy: +/- 50 cm

Future:
Experiments with other 3D models (by laser scan, from helicopters etc)

Virtual cameras

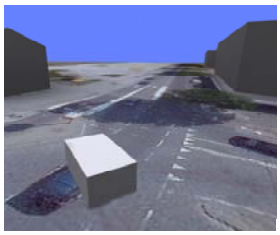


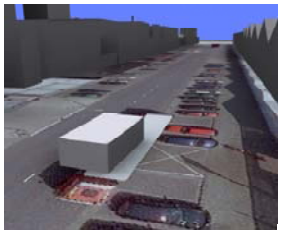
Reconstruction of movements




Suspect car seen on 4 different cameras

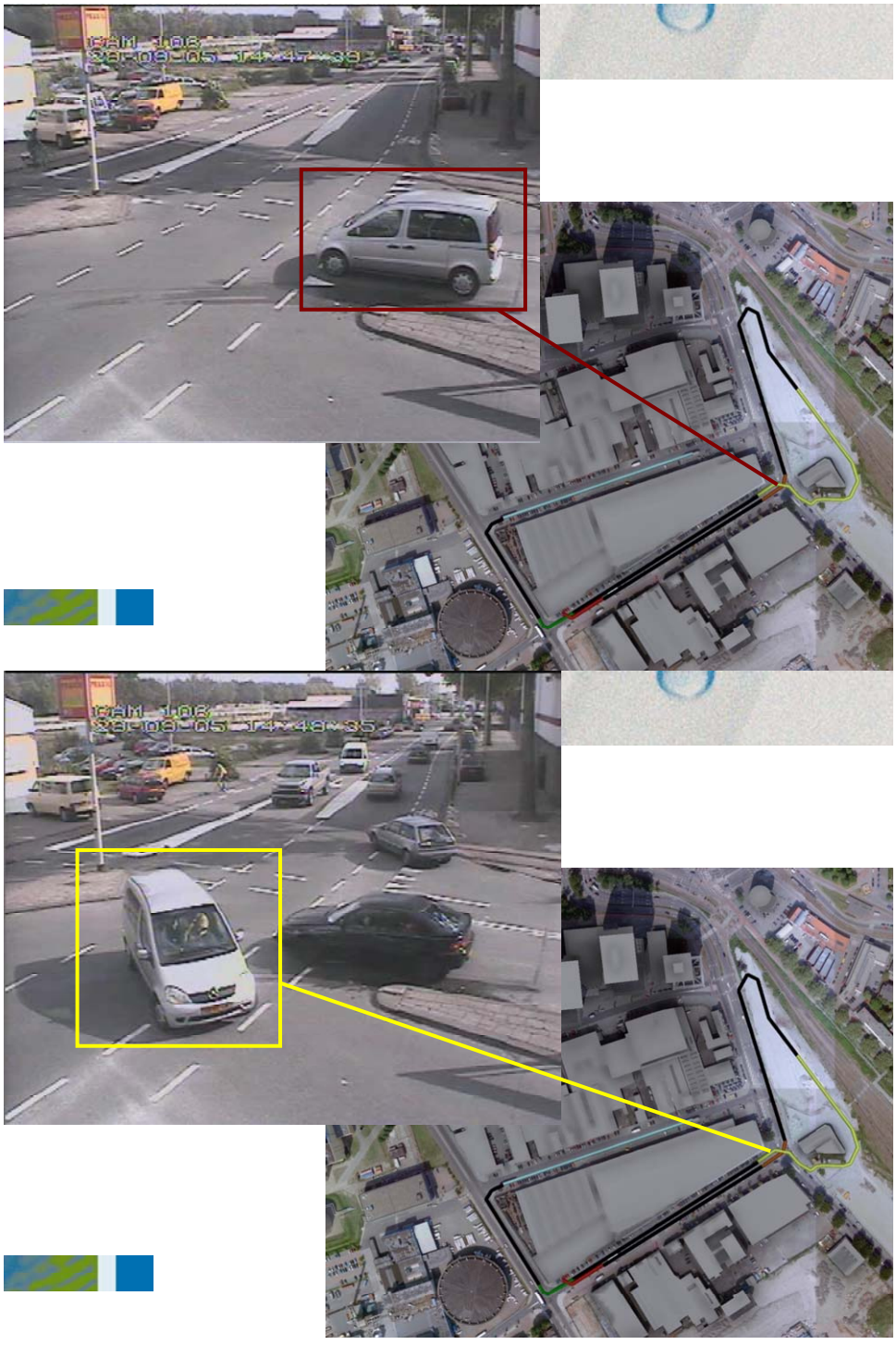
Reconstruction of movements

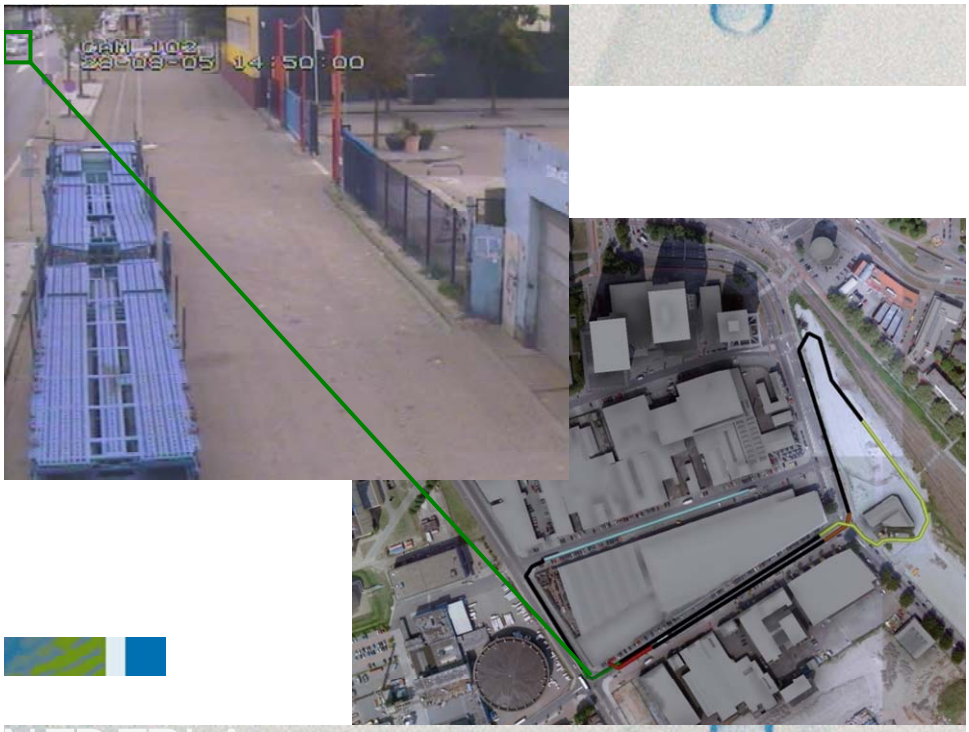





Camera image of the car

3D model of the car





Do the results from tracking in CCTV match with the GPS data ?

Distance: 1350 m

Distance: 1290 m

NEDERLA
NDSFORE
NSISCHIN
STITUUT

Advantages of a 3D model

- Overview (not necessary to know the scene)
- Visualization of movements
- Ability to look at the scene from different perspectives
- Ability to test testimony's

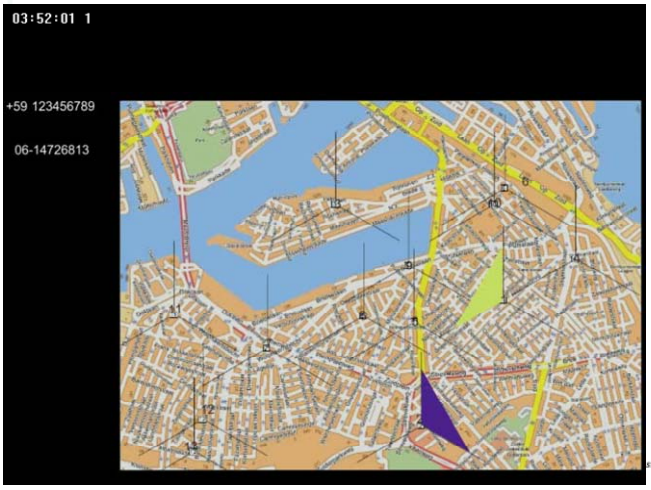
Casework

Further developments

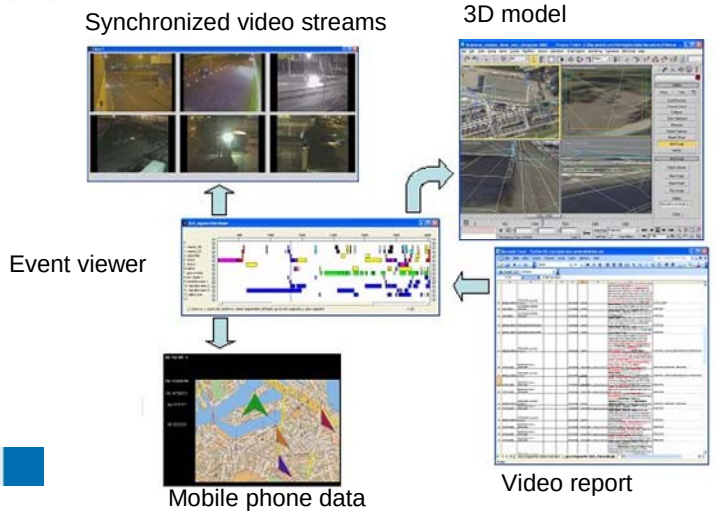
Synchronized video streams

Cell sites

Animation



Event viewer

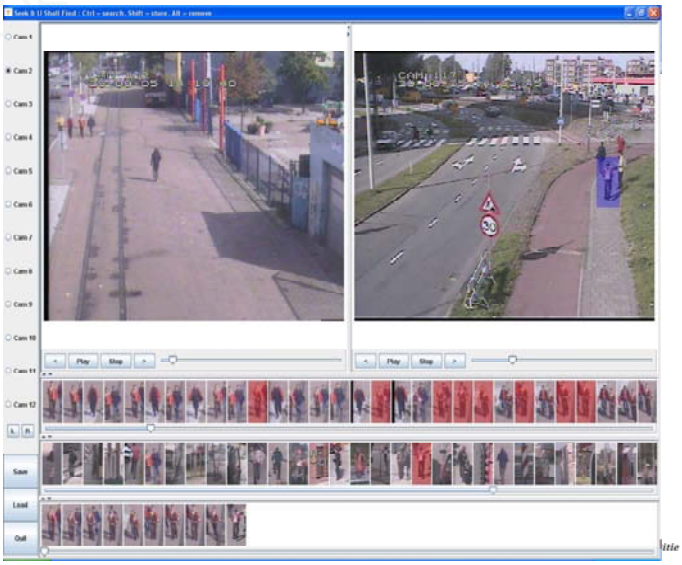


NEDERLA
NDSFORE
NSISCH
STITUUT

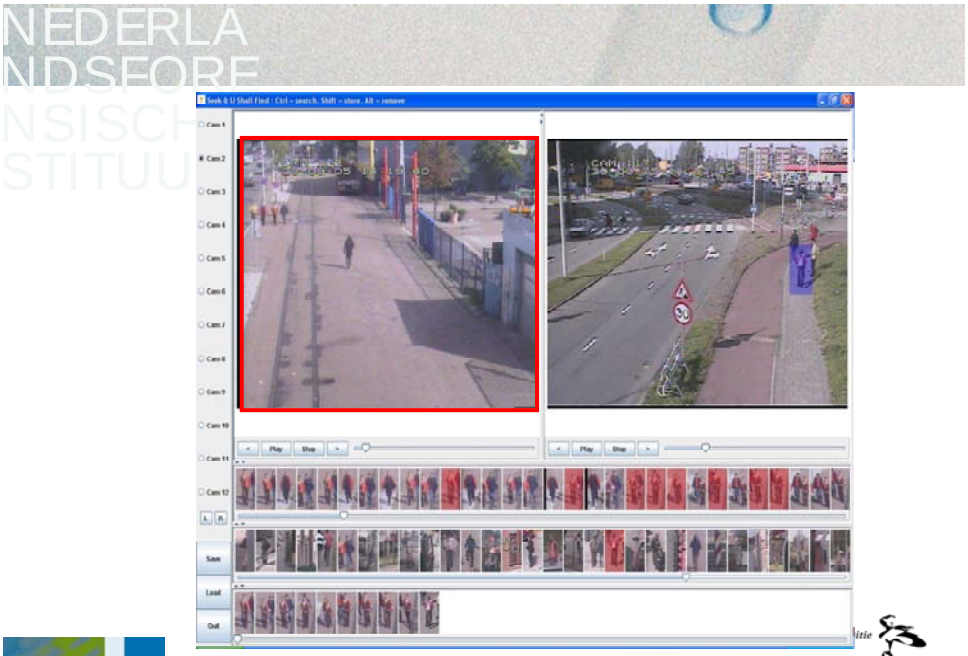
Software for detecting people

Justitie

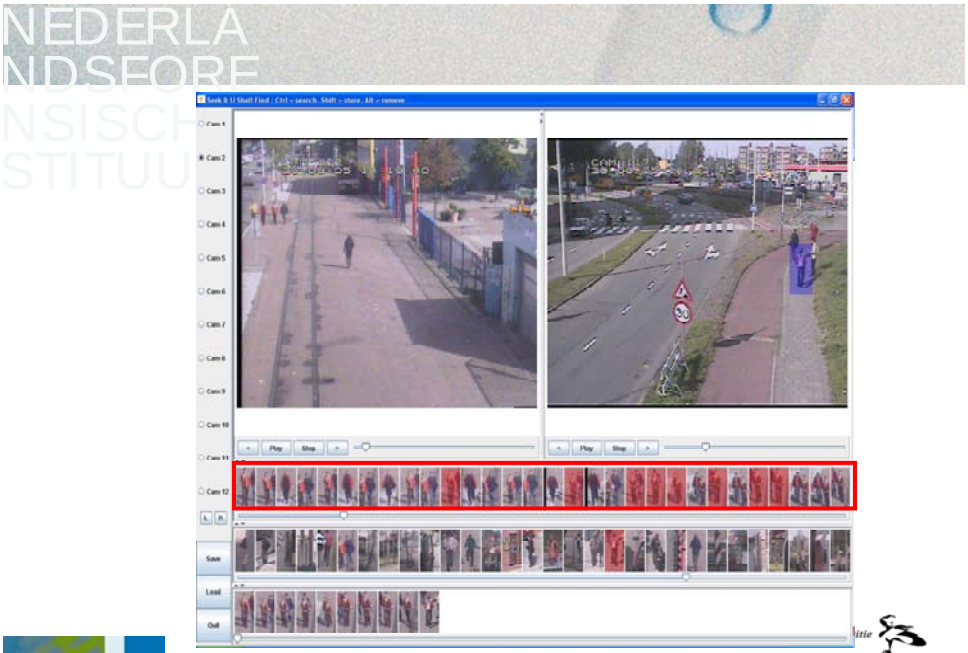
NEDERLA
NDSFORE
NSISCH
STITUUT



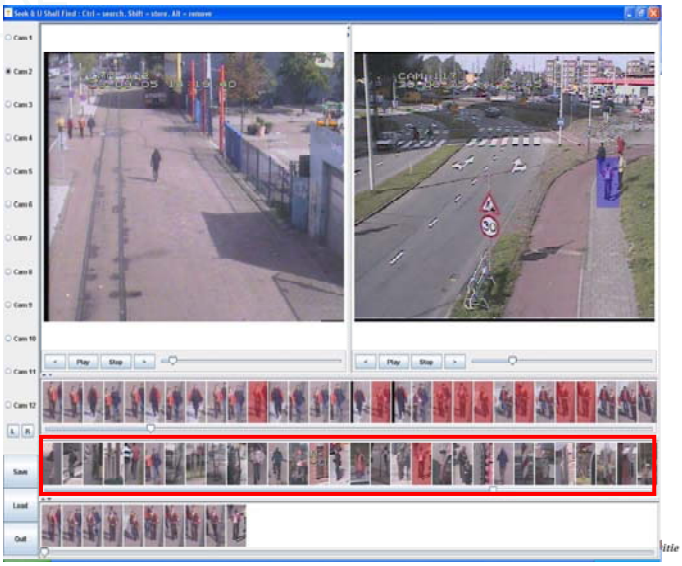
Justitie



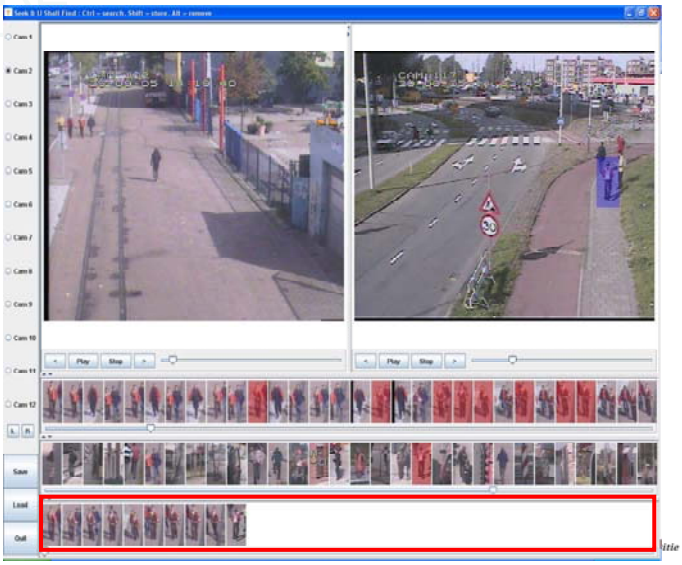
Selected camera



Detections of all persons in the selected camera

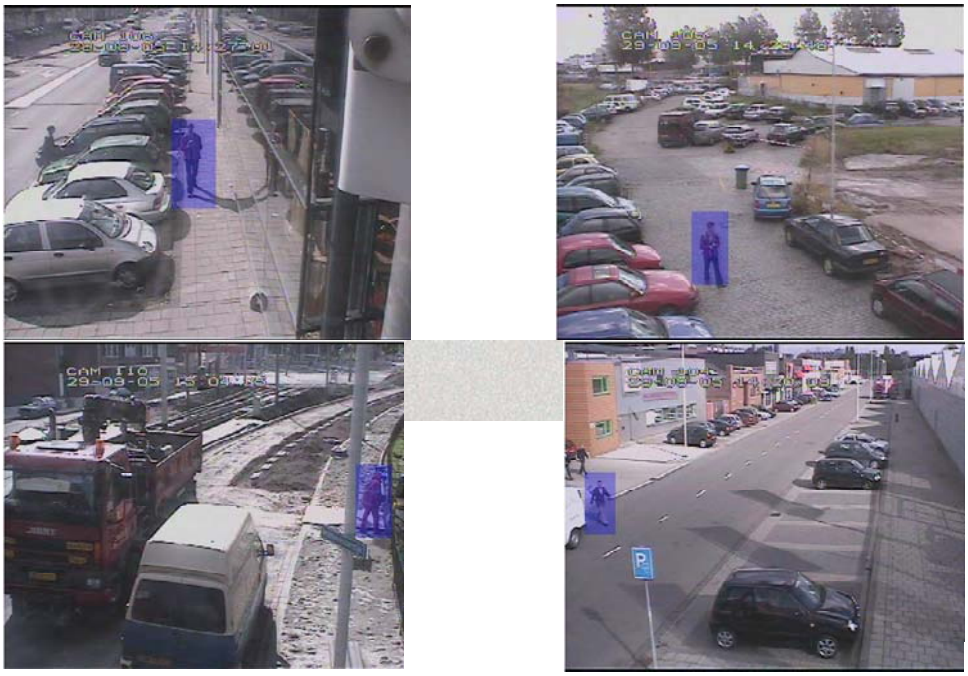


Detections of 1 selected person in all cameras



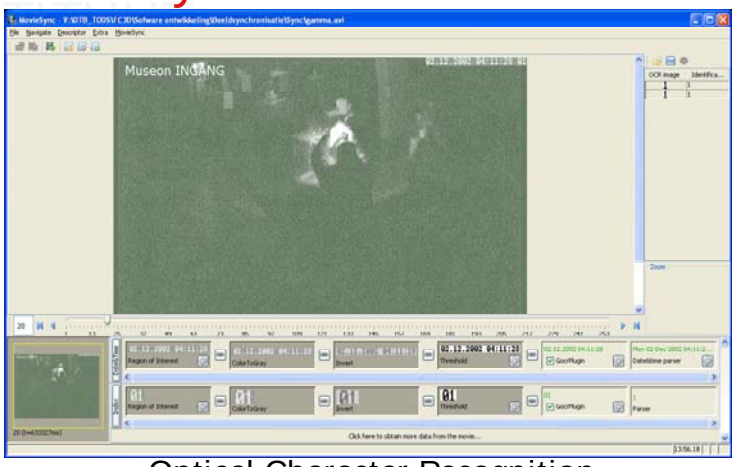
Saved detections

Right detections



Wrong detections

Synchronisation tool



- Optical Character Recognition
- Automatic synchronisation of video streams

Acknowledgements

- Jurrien Bijhold
- Ton ten Kate
- Jan de Moet
- Derk Vrijdag
- Bart Hoogeboom

And many others!

Can We Trust Digital Image Forensics?

Thomas Gloe Matthias Kirchner
{thomas.gloe,matthias.kirchner}@inf.tu-dresden.de

Technische Universität Dresden
Institute for System Architecture
01062 Dresden, Germany

FIDIS Forensic Profiling Meeting 2007
Netherlands Forensic Insitute · Den Haag · 1 October 2007

Structure of the Talk

1. Digital image forensics
2. Attacks against digital image forensics
   - Resampling detection
   - Digital camera identification
3. Concluding remarks

Digital Image Forensics

What it is and what it is good for

- Today's image processing toolboxes make it easy to manipulate digital images
  - Nevertheless authentic images are important in our media society (courtroom, science, public opinion, . . .)
- How to assure the authenticity of digital images?

(c) 2002, unknown author, Klaus Kleinfeld
www.spiegel.de

One solution: Digital Image Forensics

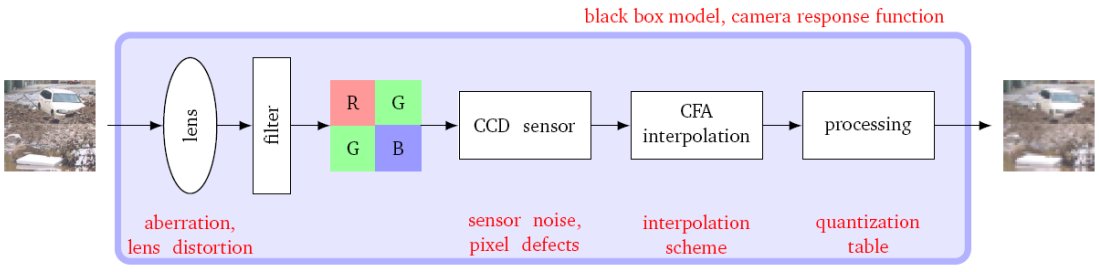
- Detection of manipulations
- Source identification

Approaches for Digital Image Forensics

Detectable traces of prior image manipulation, e.g.

resampling · copy & paste · inconsistencies in lighting · inconsistent specular highlights · double JPEG compression

Camera characteristics for acquisition-based image forensics, e.g.



Introducing Attacks

✓ Existing forensic schemes work well in laboratory test

✘ What happens in case of a farsighted counterfeiter?

Attack = Approach to systematically mislead a forensic detection scheme

Possible goals of an attacker

- Camouflage of malicious post-processing or tampering
- Suppression of correct image origin identification
- Forgery of image origin

. . . in the Following

- Recall two state-of-the-art forensic techniques
  - Resampling detection [Popescu & Farid, 2004]
  - Digital camera identification by sensor noise [Lukáš, Fridrich & Goljan, 2005]
- Present approaches for targeted attacks against these schemes

Detection of Resampling

Resampling

- Image manipulations often rely on geometric transformations
  - resampling to a new image lattice

$$\begin{bmatrix} i_x \\ j_x \end{bmatrix} \longrightarrow \begin{bmatrix} i_y \\ j_y \end{bmatrix}$$

- Typically involves an interpolation step

General Scheme

- Model each pixel as a linear combination of neighboring pixels (window of size $N \times N$, $N = 2K + 1$) and an independent residual

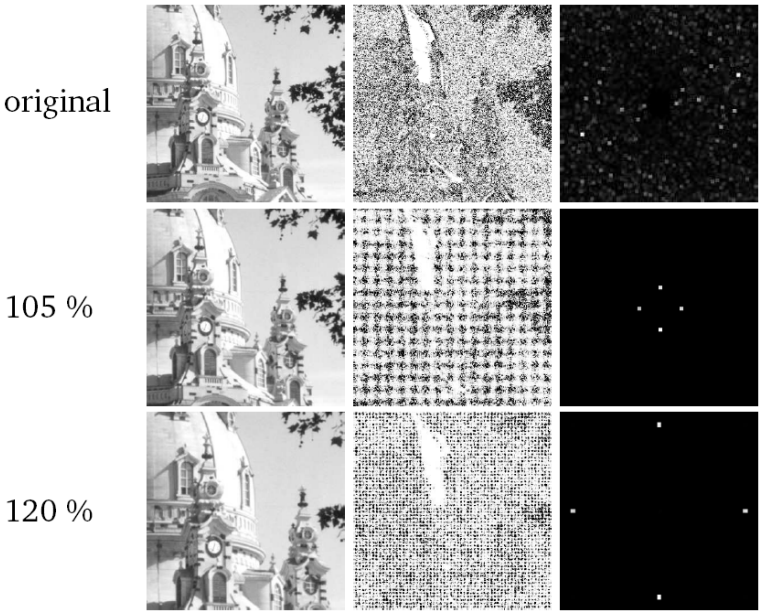
$$y_{i,j} = \sum_{(k,l) \in \{-K,\dots,K\}^2} \alpha_{k,l} \cdot y_{i+k,j+l} + \epsilon_{i,j} \qquad \alpha_{0,0} = 0$$

- Estimate scalar weights α and each pixel's probability of being correlated with its neighbors using the EM algorithm ▸▸ p-Map
- For a transformed image, correlation appears in a periodic pattern as interpolation is applied to an equidistant sampling lattice

Attacks against Digital Image Forensics | Detection of Resampling

Characteristic Peaks in the p-Map's Spectrum

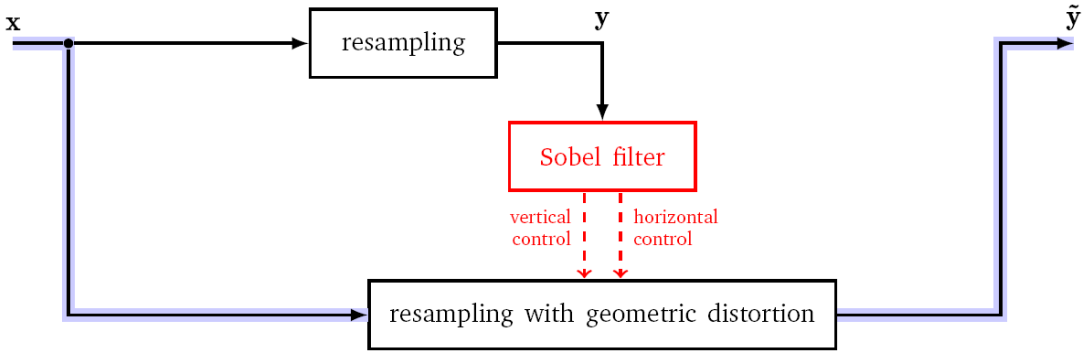
A p-map's periodic pattern shows up as distinct peaks in the frequency domain (2D FFT)



Can We Trust Digital Image Forensics? 9

Attacks against Digital Image Forensics | Detection of Resampling

Approach to Undetectable Resampling



- Detection scheme relies on an equidistant image lattice

  Attack approach: local geometric distortions

$$\begin{bmatrix} i_{\tilde{y}} \\ j_{\tilde{y}} \end{bmatrix} = \begin{bmatrix} i_y \\ j_y \end{bmatrix} + \begin{bmatrix} e_{1,i,j}\,(1 - 1/255\,\mathrm{sobelH}(y, i_y, j_y)) \\ e_{2,i,j}\,(1 - 1/255\,\mathrm{sobelV}(y, i_y, j_y)) \end{bmatrix}$$

Can We Trust Digital Image Forensics? 10

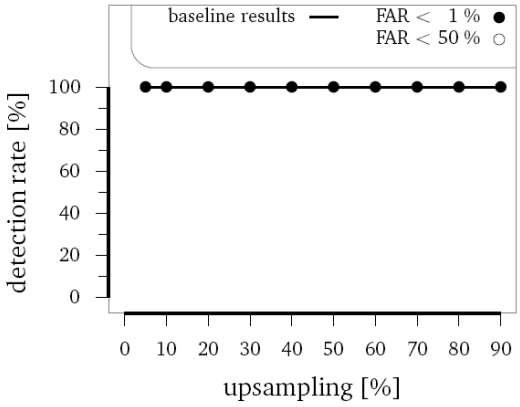
Detection (dual path approach, 7×7 median, $\sigma = 0.3$)

5 % upsampling

- Suppression of characteristic peaks
- No visible artifacts ▸ comparison

Resampling Detection Results

Upsampling of 100 gray scale images



- Perfect detection in case of no attack

Digital Camera Identification by Sensor Noise

Image acquisition process introduces noise

Main components:

- *Temporal Noise* differs for each image
- *Spatial Noise* is relatively stable between different images of the same camera

Identification Scheme (Lukáš, Fridrich & Goljan)

- Uses spatial noise as camera-specific fingerprint
- Well-documented and promising results for bitmap and JPEG images

General Scheme

- Generate a reference noise pattern $\mathbf{r}_c$ for each digital camera c under suspicion by averaging the estimated noise of images from the same device
- Measure the similarity between the reference noise pattern $\mathbf{r}_c$ and the estimated noise $\hat{\mathbf{n}}$ of the image under investigation

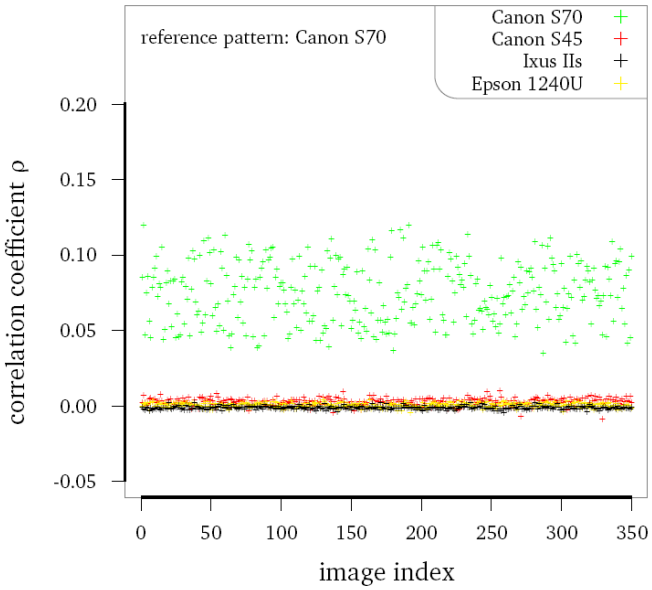
$$\rho(\mathbf{r}_c, \hat{\mathbf{n}}) = \frac{\sum \left((\hat{\mathbf{n}} - \mathsf{E}[\hat{\mathbf{n}}]) \cdot (\mathbf{r}_c - \mathsf{E}[\mathbf{r}_c]) \right)}{\| \hat{\mathbf{n}} - \mathsf{E}[\hat{\mathbf{n}}] \| \| \mathbf{r}_c - \mathsf{E}[\mathbf{r}_c] \|}$$

- Assign an image to its source c

$$c = \arg \max_{c \in \mathcal{C}} \rho(\mathbf{r}_c, \hat{\mathbf{n}})$$

Identification Results

Identification scheme enables clear separation between images made with the Canon S70 and images of other devices



Approach to Manipulate the Image's Source

Main components of spatial noise

- *Fixed Pattern Noise* - additive signal independent
- *Photo Response Non-Uniformity* - multiplicative and signal dependent

. . . can be described by a tuple $(\mathbf{d}, \mathbf{f})$

- use darkframe as estimate for Fixed Pattern Noise

$$\mathbf{d} = \frac{1}{K} \sum_{K} \mathbf{x}_{\text{dark}}$$

- use flatfieldframe as estimate for Photo Response Non-Uniformity

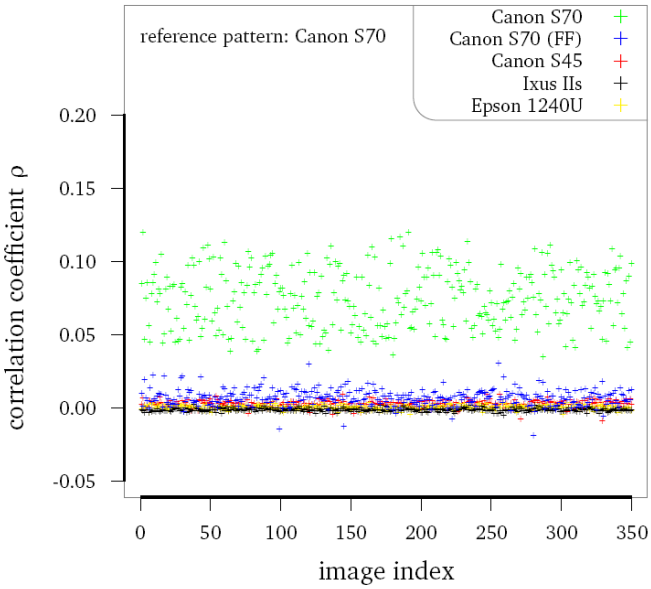
$$\mathbf{f} = \frac{1}{L} \sum_{L} (\mathbf{x}_{\text{light}} - \mathbf{d})$$

Impeding Correct Identification of Image Origin

- Flatfielding to impede the image origin

$$\tilde{\mathbf{x}} = \frac{\mathbf{x} - \mathbf{d}}{\mathbf{f}}$$

  - ▷ Correlation coefficients decreased considerably for flatfielded Canon S70 images

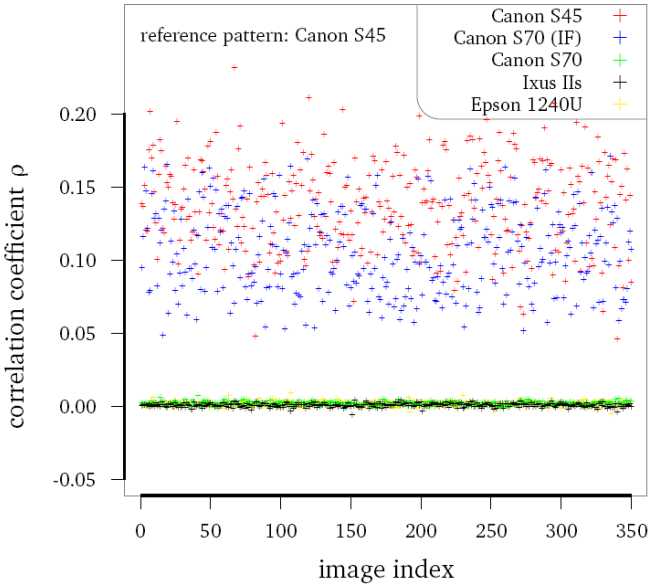


Forging Digital Image Origin

- Inverse flatfielding to forge the image origin

$$\tilde{\mathbf{y}} = \tilde{\mathbf{x}} \cdot \mathbf{f}_{\text{forge}} + \mathbf{d}_{\text{forge}}$$

- Example: let S70 images appear as S45 images
  - ▷ Results of the forged images are comparable to S45 images



Concluding Remarks

Results in a nutshell

- Presented methods to deceive digital image forensics:
  - Geometric distortion as an approach to undetectable resampling
  - Flatfielding as a tool to manipulate correct camera identification
- Good visual quality of resulting images

Can we trust digital image forensics?

- No — at least to the extent that currently known techniques are concerned

Limitations

- Proposed attacks are likely to introduce new (detectable?) artifacts
- May result in improved forensic methods

Q & A

Parts of this work were supported by the German Research Foundation (DFG).

Thomas Gloe Matthias Kirchner
{thomas.gloe,matthias.kirchner}@inf.tu-dresden.de

TECHNISCHE UNIVERSITÄT DRESDEN

Technische Universität Dresden
Institute for System Architecture
01062 Dresden, Germany