FIDIS

Future of Identity in the Information Society

Title:	D6.5/D6.6: Second thematic Workshop forensic implications combined with the workshop on forensic profiling: Crime control and due process
Author(s):	Zeno Geradts (NFI)
Reviewer(s):	Denis Royer (JWG) Nicolas Duvinage (ICGRN)
Identifier:	D6.5 & D.6.6.
Type:	Workshop report
Version:	1.2
Date:	Thursday, 04 May 2006
Status:	[Final]
Class:	[Public]

File: fidis-wp6-del6 5_del6 6 workshop_on_forensic_implications.doc

Summary

This is the report of the workshops on forensic implications (D.6.5) and profiling (D6.6) that have been held in Amsterdam at 14th of September 2005. The workshops were part of the ENFSI (European Network of Forensic Instititutes) Forensic IT working group meeting, integrating members of the FIDIS consortium and of the ENFSI organisation.

Within this document, an overview is given of deliverable D6.1 on forensic implications and comments for the revision where also taken here. Furthermore presentations where given on profiling issues and the due process, building the starting point for deliverable D 6.7 on forensic profiling.

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

Copyright Notice:

PLEASE NOTE: This document may change without notice – Updated versions of this document can be found at the FIDIS NoE website at www.fidis.net.

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	Germany
5. Institut Europeen D'Administration Des Affaires (INSEAD)	France
6. University of Reading	United Kingdom
7. Katholieke Universiteit Leuven	Belgium
8. Tilburg University	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	Czech Republic
14. VaF Bratislava	Slovakia
15. London School of Economics and Political Science	United Kingdom
16. Budapest University of Technology and Economics (ISTRI)	Hungary
17. IBM Research GmbH	Switzerland
18. Institut de recherche criminelle de la Gendarmerie Nationale	France
19. Netherlands Forensic Institute	Netherlands
20. Virtual Identity and Privacy Research Center	Switzerland
21. Europäisches Microsoft Innovations Center GmbH	Germany
22. Institute of Communication and Computer Systems (ICCS)	Greece
23. AXSionics AG	Switzerland
24. SIRRIX AG Security Technologies	Germany

Versions

Version	*Date*	*Description (Editor)*
0.1	30.09.2004	• Initial release (Denis Royer)
0.2	02.10.2004	• Changed formatting of Headers (Denis Royer)
0.3	06.10.2004	• Added version list (Denis Royer)
0.4	23.02.2005	• Updated list of partners • Minor changes in formatting
0.5	22.03.2005	• Changed naming of partners
0.6	04.07.2005	• Added IST & FP6 Logo • Changed Copyright notice
0.7	25.09.2005	• Revised title page
0.8	01.04.2006	• First version of report
1.0	19.04.2006	• Review by Denis Royer
1.1	04.05.2006	• Review by Nicolas Duvinage
1.2	05.05.2006	• Minor changes by Zeno Geradts

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)*
All	Zeno Geradts (NFI) / Ian Fulton (FSS)
Review	Denis Royer (JWG) Nicolas Duvinage (IRCGN)

Table of Contents

1 Executive Summary 7

2 The workshop 8

2.1 Presentation 1: The use of memory analysis in the recovery of digital data from mobile phone equipment. 8
2.2 Presentation 2: Time stamp interpretation in relation to identity................................ 8
2.3 Presentation 3: Biometric devices methods for spoofing and circumventing............. 9
2.4 Presentation 4: Profiling issues and due process 9
2.5 Discussion Session 10

3 Annex 1: Participants.. 11

1 Executive Summary

This is the report of the workshops on forensic implications (D.6.5) and profiling (D6.6) that have been held in Amsterdam at 14th of September 2005. The workshops were part of the ENFSI Forensic IT working group meeting, integrating members of the FIDIS consortium and of the ENFSI organisation.

Within this document, an overview is given of deliverable D6.1 on forensic implications and comments for the revision where also taken here. Furthermore presentations where given on profiling issues and the due process, building the starting point for deliverable D 6.7 on forensic profiling.

2 The workshop

These are the notes on the combined FIT-WG, FIDIS and IOCE conference proceedings and further information in relation to the contents of each person's presentation are available of the conference and will also be available on the FIDIS website[1].

The first day of this conference was open to FIDIS participants together with FIT-WG and IOCE members and any other registrations.

Richard Koning from the NFI (NL) thanked all participants for their attendance and wished them an enjoyable and enlightening meeting. He was followed by Zeno Geradts NFI (NL) who gave an introduction to the FIDIS NoE, its *"raison d'être"* and the implications for the forensic community.

2.1 Presentation 1: The use of memory analysis in the recovery of digital data from mobile phone equipment.

The first talk was presented by Seyton Bradford, Forensic Telecommunication Services (UK). His presentation was focused on his organisation's research and development work. The goal of this work is to automatically manipulate the hexadecimal encoded (HEX) data obtained from the memory chips of mobile phones. This HEX data can be extracted by a variety of methods, including the removal of integrated circuits (IC) from the circuit board and using IC programmers to do the actual data extraction.

Such methods allow to retrieve far more data than connecting the mobile handset to a PC with a cable: in addition to user-accessible data (including multimedia files), erased data and administration-level data can also be retrieved in many cases (security code, former IMEI, used IMSI, etc.).

A software program (FTS Hex) has been written to search and manipulate the stored data, enabling its user to output it into a standard format, independent of the brand or the model of the mobile phone. Currently, the application covers approximately 70% of the mobile phone market in the UK, and will be expanded to deal with more in the future. The examination of a mobile phone by FTS is charged approximately £100 (145 Euro), and FTS Hex software may be sold to law enforcement agencies in the near future.

2.2 Presentation 2: Time stamp interpretation in relation to identity

The second presentation was by Svein Ingvar Willassen from the Norwegian University of Science and Technology (Norway). This was the first of two presentations from Svein and this presentation was on the interpretation of time stamps. Svein is currently only six months

[1] http://internal.fidis.net/fileadmin/fidis/workpackages/wp6/Workshop_Amsterdam/FIDIS_AMSTERDAM_WP6_2005.zip

into this research topic – This research is being carried out for a three-year duration PhD thesis and will hopefully improve the understanding of time stamps to enable them to be better used in evidence. Purdue University (USA) and private company iBAS also contribute to the project, called "TID – Timestamps In Digital forensics" (TID means time in Norwegian).

Up to date, Svein focused specifically on dates in FAT and NTFS filesystems (file last modified date, file last accessed date, file created date, MFT last modified date).

Time stamps can present many problems, including different computers having different time stamps, which may or may not correlate, miss-adjusted clocks (accidental or deliberate), non-synchronisation of time clocks and the fact that different applications will handle time stamps in different ways.

2.3 Presentation 3: Biometric devices methods for spoofing and circumventing

The third presentation by Arnout Ruifrok from the NFI (NL) was on Biometric Devices, methods for Spoofing, and circumventing. Biometrics is defined as the (automatic) identification of an individual's identity by electronic means. There are a number of identification modalities including, facial, fingerprint, iris, hand scans, vascular pattern, signature writing, speech, and keystroke analysis.

Each of these systems has different false acceptance rates and false rejection rates. Three systems were looked at in detail: Facial, fingerprint and iris recognition systems. Each of these have their own individual problems – i.e. facial recognition systems will have difficulties in operating correctly as a result of different lighting conditions, pose and position of the subject, the background and also the expression on a persons face.

2.4 Presentation 4: Profiling issues and due process

The fourth and last presentation was held by Prof. Paul de Hert, Vrije Universiteit Brussel (Belgium). His presentation was on profiling issues and the due process – an European perspective. According to Paul de Hert, profiling is the use of previous criminal cases database to point out possible correlations with a current criminal case and identify potential suspects. Such methods are widely used in the insurance field by private companies (e.g. car and driver insurance).

Privacy of an individual is something, which is supported by the European Convention for the Protection of Human Rights. This privacy becomes a blocking power and prevents the 'State' from doing what it wishes in relation to investigation of an individual.

However since 9/11, governments throughout Europe and the rest of the world have a need to protect the general public from those that would do it harm. This requires the governments to access information and it is this access which has to be controlled. One of the forms of control is the use of data protection legislation. The issue of an individual's right for privacy and anonymity is something, which still needs to be addressed with the greater use of biometric systems being introduced.

2.5 Discussion Session

A discussion session was chaired by Zeno Geradts NFI (NL) discussing the issues raised during the day. The session also dealt with issues surrounding future research fields in forensics. One of the issues is that most forensic labs do not often search in data, and that most often this is handled by the police. For Paul de Hert some case examples were extracted which were of interest to him.

3 Annex 1: Participants

Name	Organisation	Country
Adrian Shaw	Warwickshire police HTCU	UK
Andy Wild	NHTCU	UK
Barrie Mellars	LGC	UK
Bue Hjort	National High Tech Crime Centre	Denmark
Carrie Whitcomb	National Center for Forensic Science	USA
Chrisian Förster	Landeskriminalamt Niedersachsen	Germany
Dimitris Agelopoulus	Hellenic police	Athens
Duncan Monkhouse	Bureau de la concurrence	Canada
Elena Karpukhina	Russian Federal Centre	Russia
Els Soenens	*VU Brussel*	*Belgium*
Heinz Guenther	Bundeskriminalamt	Germany
Holger Hochgraef	Bundeskriminalamt	Germany
Ian Fulton	Forensic Science	Northern Ireland
Jacek Hebenstreit	Institute of Forensic Research	Poland
Ján Čapo	Kriminalistický a expertízny Ústav PZ	Slovakia
Jim Lyle	NIST	USA
John Proudlock	The Forensic Science Service	UK
Joseph Maria Arques Soldevila	Unitat de Delictes en Technologies de la Informacio	Spain
Jürgen Frinken	BKA KT52	Germany
Leif Johansen	Danish Security Intelligence	Denmark
Lena Sjöblom	Swedish National Laboratory of FS	Sweden
Louis Maatman	Europol	The Netherlands
Manon den Dunnen	Politie Amsterdam/Amstelland	Netherlands
Marcin Flinta	Institute of Forensic Reseach	Poland
Marco Mattiucci	Ra.C.I.S. - HTC Section	Italy
Mark Gasson	*Reading Univerisity*	*UK*
Nicky Waterreus	Ministerie van Justitie	The Netherlands
Nicolas Duvinage	*Institut de recherche criminelle de la gendarmerie nationale (Gendarmerie Nationale Forensic Research Institute)*	*France*

Olivier Delhomme	Police Technique et Scientifique	France
Paul de Hert	*VU Brussels and University of Leiden*	*Belgium*
Peter Geersten	Danish Security Intelligence	Denmark
Peter Rosenbak Hansen	National High Tech Crime Centre	Denmark
Peter Sommer	*London School of Economics*	*UK*
Sébastien Bachet	DNRED	France
Seyton Bradford	Forensic Telecommunications Services	UK
Stefan Rhodin	Swedish National Laboratory of FS	Sweden
Stephan Viehl	Bundeskriminalamt	Germany
Svatopluk Machalka	Institute of Criminalistics Prague	Czech Republic
Tak-kwong, Collins Leung	Hong Kong Police Force	China
Terri Lang	Centre of Forensic Sciences	Canada
Terry London	Estonian Forensic Service Centre	Estonia
Thomas Dahl	National Criminal Investigation Service	Norway
Vilnis Vevers	State Forensic Science Bureau	Latvia
Vytautas Jonas Kligys	Forensic Science Center of	Lithuania
Wesley Krause	RCMP	Canada
Yan-leung Lewis Tse	Hong Kong Police Force	China
Yoichi Kumota	National Police Agency	Japan
Zeno Geradts	*NFI*	*Netherlands*

Persons in cursive are member of FIDIS.