Fraunhofer
SIT

FRAUNHOFER INSTITUTE FOR SECURE INFORMATIONTECHNOLOGY

IT FORENSICS

FRAUD DETECTION & FORENSIC ANALYSIS

ANALYSIS OF MASS DATA, ANOMALY DETECTION, PRESERVATION OF EVIDENCE

MOTIVATION

Information technology offers many opportunities for abuse. Computer crime causes an annual damage of more than €10 billion in the German economy alone. IT-supported industrial espionage also results in a damage of approximately €50 billion each year. However, even in the world of IT, perpetrators generally leave behind traces. The aim of IT forensics is to locate and analyse these digital traces to reconstruct the circumstances of the crime.

The opportunities for IT abuse vary widely. Users often abuse their IT system authorisations. In such cases, it can be difficult to distinguish between authorised and criminal activities but with the help of mass data analyses, patterns can be detected and abnormalities identified. However, this bears the question of the effectiveness and legality of today's methods. The IT landscape is changing rapidly, and today data can be transmitted illegally with multifunctional printers or smart phones. This development makes it necessary to develop more modern tools for trace detection and existing tools will have to be improved or adapted to the changed circumstances.

CHALLENGES

IT forensic analyses are often similar to the search for that famous needle in a haystack. The quantity of saved data is constantly increasing, in other words, the haystack is inevitably becoming larger. IT forensic scientists therefore require effective and efficient tools. That being said, many tools used today are not efficient enough and make analyses both complex and expensive.

Fraunhofer SIT is testing existing tools and identifying individual deficits. In this respect, established procedures such as the Benford analysis demonstrate weaknesses under certain conditions. The development of new technologies like smart phones also presents a new challenge for IT forensic tools. Furthermore, the IT security technology such as hard drive encryption can render former IT forensic methods useless. Worse still, traces can be overlooked or even destroyed as a result of incorrect handling of IT forensic tools. If the analysis is not executed legally, the evidence cannot be utilised or only utilised to a limited extent. IT forensics in businesses require extensive and up-to-date expertise in order to meet legal, financial and technical requirements.

OUR OFFERINGS

- **Development and testing of IT forensic tools:** Fraunhofer SIT supports its customers with special test procedures (3LSPG tests) [YFWS10, YFWS11] and comparative studies on existing products.
- **IT forensic analyses:** Fraunhofer SIT has numerous modern analysis tools at its disposal and offers forensic services based on these.
- **Analysis of multifunctional devices:** Should industrial espionage be suspected (for example, confidential document copying), Fraunhofer SIT analyses IT-based devices for data traces for its customers.
- **Software to improve the Benford Analysis (Modified mass data analysis):** The Modified Benford Analysis developed by Fraunhofer SIT leads to a significant reduction in error rates in comparison to the Standard Benford Analysis and reduces the investigation costs [WiScYa11].
- **Consulting and technical support for legally sound analyses:** There is often a very fine line between IT forensic analysis and adhering to compliance requirements. Fraunhofer SIT helps companies operate safely on this fine line [HYFWS10].

[The information in brackets refers to the publication list on the next page]

CUSTOMER BENEFIT

- **Those affected by computer crime:** Such businesses benefit from our know-how. Fraunhofer SIT takes on projects dealing with the confidential search for and analysis of digital traces. This avoids involving prosecution authorities, which is in the interests of many businesses.
- **Users of IT forensic tools:** The IT forensic analysis procedures developed by Fraunhofer SIT make forensic work even more efficient, which, in turn, reduces work and costs.
- **Manufacturers of IT forensic tools:** Manufacturers can improve their products by means of the cooperation with Fraunhofer SIT. The Institute develops tools as well as methods to test and compare tools and helps to improve and adapt products.

These said customers also benefit from the extensive knowledge and experience of the SIT security test laboratory. The hacking specialists of Fraunhofer SIT know many ways of reaching the data traces, which are valuable for the IT forensic work, on supposedly secured IT systems, as is shown in [HeBo11, WoSc07].

REFERENCES

[HeBo11] Jens Heider, Matthias Boll: **Lost iPhone? Lost Passwords!** – Practical Considerations of iOS Device Encryption Security. Fraunhofer SIT, Feb. 2011, http://www.sit.fraunhofer.de/Images/sc_iPhone%20Passwords_tcm501-80443.pdf

[HYFWS10] Dennis Heinson, York Yannikos, Frederik Franke, Christian Winter, Markus Schneider: **Rechtliche Fragen zur Praxis IT-forensischer Analysen in Organisationen.** Datenschutz und Datensicherheit (DuD), Vol. 34, Nr. 2 Februar 2010

[KPMG10] KPMG: **e-Crime-Studie 2010** – Computerkriminalität in der deutschen Wirtschaft. http://www.kpmg.de/docs/20100810_kpmg_e-crime.pdf,2010

[WiScYa11] Christian Winter, Markus Schneider, YorkYannikos: **Modification of Benford Analysis improves Fraud Detection** – Resolving Conflicts between Access Control and IT Forensics. 7th International Conference on Digital Forensics, Orlando, Florida, Jan. – Feb. 2011, in Advances in Digital Forensics VII, Springer-Verlag, 2011

[YFWS10] York Yannikos, Frederik Franke, Christian Winter, Markus Schneider: **Erzeugung synthetischer Daten zum Test IT-forensischer Werkzeuge.** Datenschutz und Datensicherheit (DuD), Vol. 34, Nr. 2, Februar 2010

[YFWS11] York Yannikos, FrederikFranke, Christian Winter, Markus Schneider:3LSPG: **Forensic Tool evaluation by Three Layer Stochastic Process-Based Generation of Data.** In Computational Forensics (IWCF 2010), Springer Verlag, LNCS 6540, Feb. 2011

THE INSTITUTE

Information technology has already permeated large parts of our everyday life: whether it be a car, telephone or heating. Without the use of IT, the majority of devices and systems are almost inconceivable. Businesses in particular use IT systems to effectively design their working processes. The Fraunhofer Institute for Secure Information Technology focuses on protecting these systems against failures, attacks and manipulations.

The Institute works for companies in various industries. Many successful projects with international partners are impressive evidence of the faithful and reliable cooperation. Our customers include HP, Software AG, SAP, Lufthansa and the Federal Office for Information Security.

CONTACT

Dr. Martin Steinebach
Phone +49 6151 869-349
Fax +49 6151 869-224
martin.steinebach@sit.fraunhofer.de

Fraunhofer Institute for Secure Information Technology
Rheinstrasse 75
64295 Darmstadt, Germany
www.sit.fraunhofer.de