Fraunhofer
SIT

FRAUNHOFER-INSTITUT FÜR SICHERE INFORMATIONSTECHNOLOGIE

IT FORENSICS
DIGITALE SPUREN FINDEN UND AUSWERTEN

ANGRIFFE WIRKSAM UND BEWEISSICHER AUFKLÄREN

TRENDS

In sämtlichen Lebensbereichen – egal ob privat oder im Unternehmen – unterstützen uns digitale Geräte und Systeme. Neue technische Entwicklungen, neue Dienste für Unternehmen und Konsumenten sowie immer komplexere IT-Systeme erleichtern den Arbeitsalltag.

IT-Systeme sind aber nicht nur nützlich, sondern sie können auch das Ziel von Angriffen sein oder als Werkzeug bzw. Hilfsmittel von Tätern ausgenutzt werden. Laut Angaben des Bundeskriminalamts verursacht allein in Deutschland IT-gestützte Kriminalität jährlich Schäden im zweistelligen Milliardenbereich. Oft missbrauchen Anwender dabei ihre Berechtigungen in den IT-Systemen. In vielen Fällen ist es nicht leicht, legitime von kriminellen Vorgängen zu unterscheiden. Erst mithilfe geeigneter Analyseverfahren lassen sich die kriminellen Muster identifizieren: Bei Angriffen hinterlassen die Täter meist Spuren in den IT-Systemen. Das Auffinden und die Analyse dieser digitalen Spuren zur Rekonstruktion von Tathergängen ist Aufgabe der IT-Forensik. Der Einsatz von IT-Forensik in Unternehmen erfordert umfangreiches und aktuelles Know-how, um rechtliche, wirtschaftliche und technische Anforderungen zu erfüllen.

HERAUSFORDERUNGEN

Spiegelbildlich zur Bedeutung der IT steigen die Möglichkeiten des Missbrauchs von Informationstechnologie. Mit dem technischen Fortschritt entwickeln Täter stets neue Wege, kriminelle Handlungen durchzuführen und zu verschleiern. Daneben werden IT-Systeme immer komplexer, so dass die Suche nach Spuren entsprechend aufwendiger wird. IT-Forensiker müssen deshalb stets auf dem aktuellen Stand der Technik sein, um neue Systeme zu analysieren, neue Arten von Spuren zu suchen und neue Fragestellungen zu beantworten. IT-Forensiker müssen dabei viele Datenquellen – offline und online – berücksichtigen und viele unterschiedliche Arten von Daten verarbeiten können. Zusätzlich kann der Einsatz von Sicherheitsvorkehrungen wie z. B. Verschlüsselung von Festplatten oder Betragsgrenzen in Buchungsprozessen etablierte IT-forensische Methoden unbrauchbar machen.

Durch unsachgemäßen Umgang mit IT-forensischen Werkzeugen können Spuren übersehen oder sogar zerstört werden. Wird die Analyse nicht rechtsverträglich durchgeführt, lassen sich die Beweise nicht oder nicht vollständig verwerten. Daneben steigt die Arbeitsbelastung von IT-Forensikern von Jahr zu Jahr sowohl durch Anzahl als auch Umfang der Fälle. Es werden daher Werkzeuge benötigt, die schnell, zuverlässig und gerichtsverwertbar Fälle bearbeiten können, um eine Datenüberlastung der Ermittler zu vermeiden oder abzubauen.

ANGEBOTE

Die am Fraunhofer SIT entwickelten Verfahren können als Software lizenziert werden. Dabei sind auch individuelle Anpassungen möglich.

- **Erkennung von illegalem Bild- und Videomaterial:** Die robusten Hashverfahren des Fraunhofer SIT sind für eine schnelle und zuverlässige Erkennung optimiert.
- **Statistische Finanzdatenanalyse:** Das Fraunhofer SIT kann mit der modellbasierten Ziffernanalyse Unregelmäßigkeiten in Finanztransaktionsdaten identifizieren.
- **Digitale Textforensik:** Ist die Autorschaft eines Textes fraglich, können die Fraunhofer-Verfahren basierend auf dem Sprachstil z. B. Verleumdung aufklären.
- **File Carving:** Das Fraunhofer SIT hat File Carver für verschiedene Multimediaformate entwickelt, um Daten wiederherzustellen, die sonst nicht gefunden werden.
- **Analysen und Gutachten:** Das Fraunhofer SIT führt für Unternehmen und Behörden IT-forensische Analysen durch und fertigt Gutachten an. Dabei werden gängige Werkzeuge sowie Eigenentwicklungen eingesetzt.
- **Test und Vergleich von Werkzeugen:** Das Fraunhofer SIT testet die Qualität und Leistungsfähigkeit von IT-forensischen Werkzeugen. Dies geschieht z. B. mit synthetischen Testdaten aus eigens entwickelten Verfahren.

Anwendertag IT-Forensik
Das Fraunhofer SIT veranstaltet diese Tagung jährlich für Anwender aus Behörden und Wirtschaft.
www.anwendertag-forensik.de

KUNDENNUTZEN

- **Unternehmen:**
  Unternehmen können durch externe oder interne Angriffe geschädigt werden. Das Fraunhofer SIT hilft mit seinem Know-how, diese Vorfälle vertraulich aufzuklären. Die Begrenzung der Schäden vermeidet unnötige Kosten und Verluste. Passende Sicherheitsmaßnahmen erschweren zukünftige Angriffe.
- **IT-forensische Ermittler:**
  Die vom Fraunhofer SIT entwickelten Lösungen zur IT-forensischen Analyse machen die Ermittlungsarbeit effizienter und effektiver. Das reduziert Aufwand und Kosten und führt schneller zu detaillierten und belastbaren Ergebnissen. Ermittler können sowohl die Lösungen lizenzieren als auch das Fraunhofer SIT mit IT-forensischen Untersuchungen beauftragen, um dadurch ihre Arbeitslast weiter zu reduzieren.
- **Hersteller von IT-forensischen Werkzeugen:**
  Durch die Kooperation mit dem Fraunhofer SIT können Hersteller ihre Produkte effektiver, effizienter, zuverlässiger und sicherer machen: Hersteller können Lösungen des Fraunhofer SIT zur Integration in ihre Produkte lizenzieren, ihre Produkte testen lassen oder einen neutralen Vergleich mit Produkten anderer Anbieter durchführen lassen. Dies erhöht den Wert der Produkte.

REFERENZEN

Projekte

- **ForBild und ForSicht:** Projekte zur Entwicklung von robusten Hashverfahren für Bild und Video, gefördert vom Land Hessen, 2010–2014
- **EWV**: Projekt zur Erkennung von Wirtschaftskriminalität und Versicherungsbetrug, gefördert vom Bundesministerium für Bildung und Forschung BMBF, 2015–2017
- **ILLICID**: Projekt zur Erhellung des Dunkelfeldes in Bezug auf illegalen Handel mit antikem Kulturgut in Deutschland, gefördert vom BMBF, 2015–2018

Veröffentlichungen

- M. Steinebach, Y. Yannikos, S. Zmudzinski, C. Winter: **Advanced Multimedia File Carving**. In: Handbook of Digital Forensics of Multimedia Data and Devices, Wiley, 2015
- Y. Yannikos, L. Graner, M. Steinebach, C. Winter: **Data Corpora for Digital Forensics Education and Research**. In: Advances in Digital Forensics X, Springer, 2014
- O. Halvani, M. Steinebach: **An Efficient Intrinsic Authorship Verification Scheme Based on Ensemble Learning**. In: Availability, Reliability and Security (ARES 2014), IEEE Computer Society, 2014
- C. Winter, M. Schneider, Y. Yannikos: **F2S2: Fast Forensic Similarity Search through Indexing Piecewise Hash Signatures**. Digital Investigation, Vol. 10, Nr. 4, Elsevier, 2013

DAS INSTITUT

Das Fraunhofer-Institut für Sichere Informationstechnologie SIT gehört zu den angesehensten Forschungseinrichtungen für IT-Sicherheit weltweit. Mehr als 160 Mitarbeiter unterstützen Unternehmen und Behörden bei der Absicherung von Daten, Diensten, Infrastrukturen und Endgeräten.

Das Fraunhofer SIT ist Teil einer vielseitigen Forschungslandschaft mit Schwerpunkt Cybersicherheit: In Darmstadt forschen mehr als 400 Wissenschaftlerinnen und Wissenschaftler in den Bereichen IT-Sicherheit und Datenschutz. Das Institut ist beteiligt am vom Land Hessen geförderten Center for Advanced Security Research Darmstadt (CASED) sowie am Center for Research in Security and Privacy (CRISP), das von Bund und Land gefördert wird. CRISP-Partner sind neben dem Fraunhofer SIT die TU Darmstadt, die Hochschule Darmstadt sowie das Fraunhofer IGD.

KONTAKT

Dr.-Ing. Martin Steinebach
Telefon 06151 869-349
Fax 06151 869-224
martin.steinebach@sit.fraunhofer.de

Fraunhofer-Institut für Sichere Informationstechnologie
Rheinstraße 75
64295 Darmstadt
www.sit.fraunhofer.de