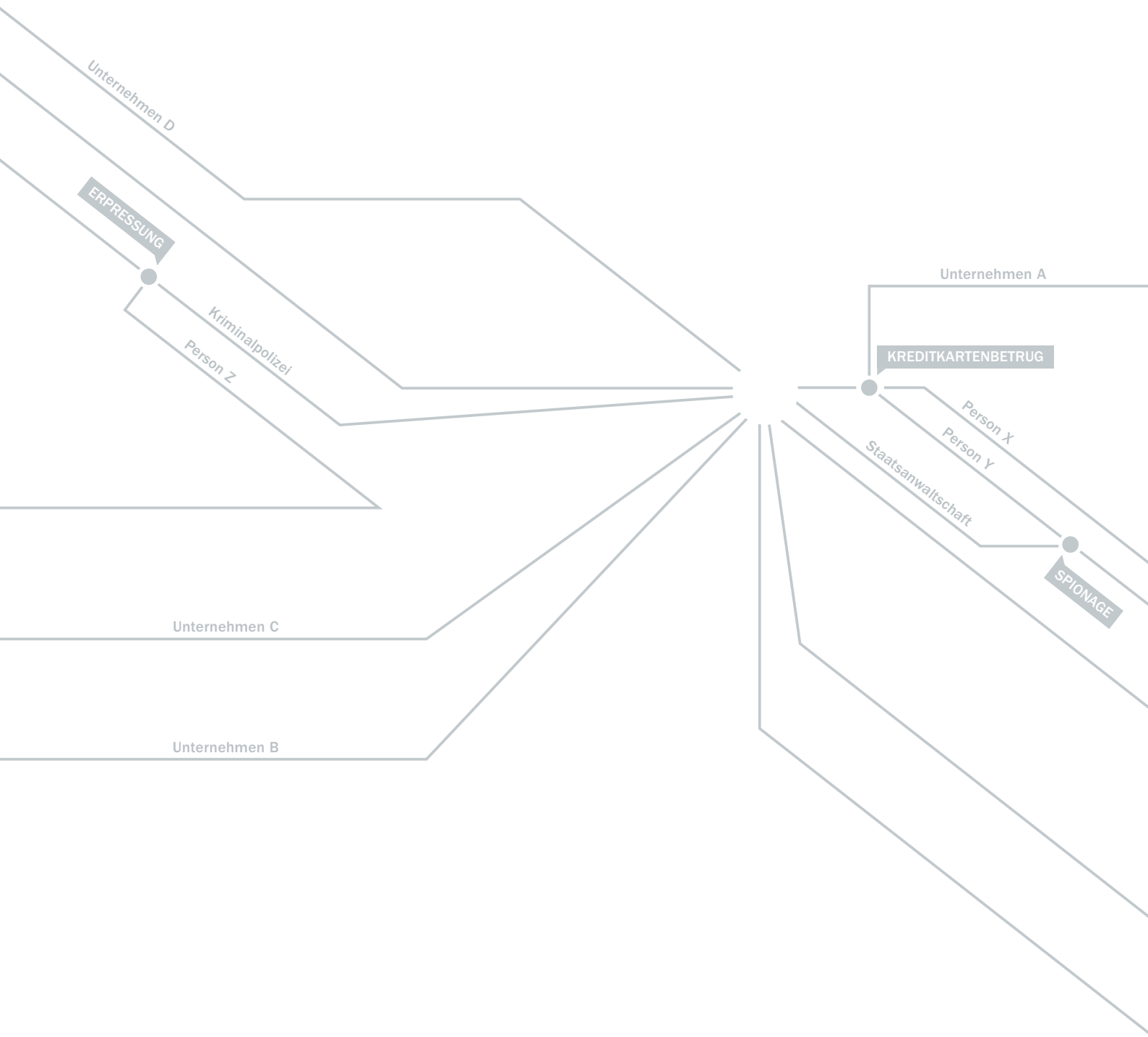
FAST DETECT

SACHVERSTÄNDIGENBÜRO
FÜR IT-FORENSIK



IT-FORENSIK
UNTERSTÜTZUNG DER JUSTIZ

WILLKOMMEN BEI FAST-DETECT

Klassische Computerstraftaten
sowie Straftaten, bei denen ein Computer oder das Internet ein wesentliches Tatmittel darstellen, nehmen rapide zu.

Entsprechend benötigen Gerichte zunehmend die Expertise von Sachverständigen, die sich auf die Aus-wertung digitaler Spuren spezialisiert haben.

Aus diesem Grund wurde 2003 die FAST-DETECT GmbH als erstes deutsches Sachverständigenbüro für IT-Forensik gegründet. Wir sind Pioniere auf diesem spannenden Spezialgebiet der Informatik und gehören zu den Wegbereitern dieser Wissenschaft.

Unsere Entwicklung zum größten Sachverständigenbüro für IT-Forensik basiert unter anderem auf der erfolgreichen Auswahl und Weiterbildung hervorragender Mitarbeiter, der Investition in modernste Technik und Forschung, der Entwicklung eigener Auswertungssoftware und -prozesse, dem Aufbau von Wissensdatenbanken, der Anwendung größtmöglicher Sicherheitsmaßnahmen sowie der Zertifizierung unseres Informationssicherheits- und Qualitätsmanagements.

Die FAST-DETECT Sachverständigen für IT-Forensik erstatten jährlich in enger Zusammenarbeit mit Kriminalermittlungsbehörden und Landeskriminalämtern über 250 Gutachten für mehr als 60 Staatsanwaltschaften und Gerichte. Hinzu kommen zahlreiche Gutachtenaufträge von Rechtsanwälten und aus der Privatwirtschaft im In- und Ausland.

Wir sind stolz darauf, dass unsere Gutachten als besonders verständlich, nachvollziehbar und hilfreich gelten – und laut Aussage vieler Kunden die besten IT-Forensik-Gutachten in Deutschland sind.

Ich lade Sie herzlich ein, die Kompetenzen von FAST-DETECT im Bereich IT-Forensik auf den folgenden Seiten näher kennenzulernen.

Thomas Salzberger
Geschäftsführer FAST-DETECT GmbH

IT-FORENSIK WIRD IMMER WICHTIGER

Mit dem zunehmenden Einzug des Computers in alle Lebensbereiche und der explosionsartig anwachsenden Informationsflut durch das Internet nehmen auch zwangsläufig Straftaten und ungesetzliche Handlungen zu, die in unmittelbarem Zusammenhang mit der Nutzung von Computern, dem Internet und digitaler Informationen stehen.

IT-Forensik ist u.A. in folgenden Bereichen bei der Aufklärung von Straftaten sehr hilfreich:

- Sabotage, Spionage, Hackerangriffe
- Verbreitung von Schadprogrammen
- Computerbetrug, Kreditkartenbetrug, eBay-Betrug
- Urheberrechtsverletzung (z.B. Filme, Musik oder Software)
- Urkundenfälschung und Identitätsdiebstahl
- Wirtschaftskriminalität
- Veränderung, Löschung oder Diebstahl von Geschäftsdaten
- Erpressung, Bedrohung, Verleumdung, Mobbing
- Verbreitung pornografischer, kinderpornografischer oder verfassungsfeindlicher Schriften
- Verabredung zu gemeinschaftlichen kriminellen Handlungen

Die IT-Sachverständigen von FAST-DETECT besitzen Spezialwissen in all diesen Bereichen.

Schwerpunkte unserer Tätigkeit sind die Gutachtenerstellung bezüglich Wirtschaftskriminalität, Cybercrime und Kinderpornografie.

FAST-DETECT AUF EINEN BLICK

- Das größte Sachverständigenbüro für IT-Forensik in Deutschland
- Führend in der IT-Forensik
- Jährlich über 250 erstattete IT-Forensik-Gutachten
- Europaweit tätig
- Spezialisiert, zertifiziert, zuverlässig

WAS IST IT-FORENSIK?

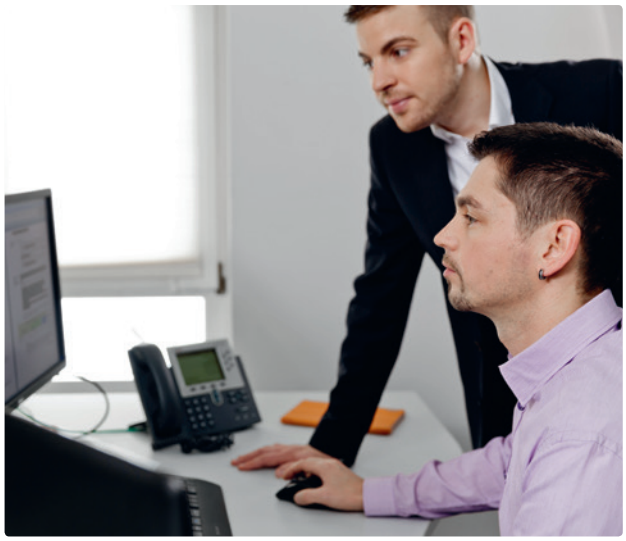
Durch den Einsatz wissenschaftlicher Methoden zur gerichtsfesten Sicherung, Sammlung, Überprüfung, Identifikation, Analyse, Interpretation und Dokumentation von digitalen Spuren kann die IT-Forensik maßgeblich zur Wahrheitsfindung und zur Aufklärung von Straftaten beitragen.

Als digitale Spuren werden jegliche Formen von Daten bezeichnet, die mit Hilfe von Computersystemen gespeichert oder übertragen werden und ein belastendes oder entlastendes Indiz für die Durchführung einer Straftat darstellen. Sie können beispielsweise Informationen zu Besitz oder Weitergabe von Daten, finanziellen Transaktionen, Kommunikationspartnern, Nutzung von E-Mail- oder Chat-Programmen sowie sonstigen Auffälligkeiten liefern.

In der IT-Forensik kann die digitale Spurensuche auf jedem Gerät stattfinden, welches über einen integrierten elektronischen Speicher verfügt. Die Herausforderung für IT-Forensik-Labore besteht darin, mit unzähligen Varianten an mobilen Geräten, Speichermedien und Betriebssystemen umzugehen, die immer größer werdenden Datenmengen zu verarbeiten, darunter potenziell relevante, digitale Spuren zu finden und diese richtig zu interpretieren.

Die Erfassung und Dokumentation festgestellter Spuren findet in den gerichtsfesten Gutachten von FAST-DETECT unter Berücksichtigung geltender Gesetze statt.

Fundierte Systemkenntnisse unserer Mitarbeiter, der Einsatz von Spezialsoftware, moderne technische Ausrüstung sowie langjährig erprobte und optimierte Prozesse machen uns zu den führenden Spezialisten auf dem Gebiet der IT-Forensik.



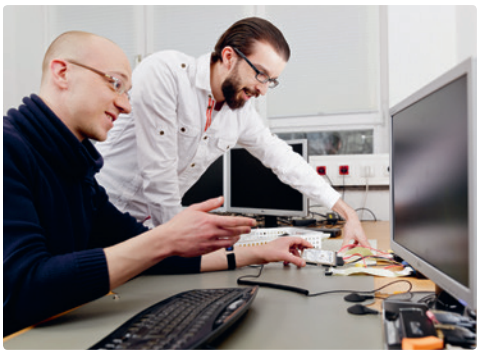
IT-FORENSIK

„IT-Forensik ist die Anwendung wissenschaftlicher Methoden der Informatik auf Fragen des Rechtssystems."

Quelle: Dewald/Freiling 2015

VERSCHLÜSSELTE DATEN UND CONTAINER

Wir dechiffrieren im Rahmen der technischen Möglichkeiten verschlüsselte Daten und Container durch Passwortanalysen, automatisierte Abgleiche mit speziell angefertigten Wörterbuchsammlungen sowie durch den Einsatz komplexer, rechenintensiver und zeitaufwendiger Entschlüsselungsverfahren wie z.B. Brute-Force- oder Rainbowtable-Attacken.



DAS KÖNNEN UNSERE IT-SACHVERSTÄNDIGEN FÜR SIE AUSWERTEN:

Prinzipiell lassen sich alle Arten digitaler Speicher mit den Methoden der IT-Forensik auswerten.
Beispiele sind:

- Der Arbeitsspeicher im laufenden Rechnerbetrieb
- In Rechnern eingebaute, sowie externe Festplatten einschließlich komplexer und proprietärer RAID Verbundsysteme
- Netzwerkkomponenten wie Router und Firewalls
- Mobiltelefone, Smartphones, Tablets und Navigationsgeräte
- Digitale Kameras und Videokameras
- Speicherkarten und USB-Sticks sowie optische Speichermedien wie CDs oder DVDs
- Magnetbänder mit Datensicherungen
- Rechnerbasierte Telefonanlagen

Bei auszuwertenden Daten wird zwischen vom Nutzer verwalteten Daten und Spuren der Rechnernutzung unterschieden.

Vom Nutzer verwaltete Daten können beispielsweise Dokumente, Bild- und Videodateien oder gespeicherte Kommunikationsdaten wie E-Mails, Chat und SMS-Nachrichten sein. Im Unternehmensbereich zählen hierzu auch Datenbanken und Anwendungsdaten von z.B. ERP-Systemen oder Kassen- und Arzt-Abrechnungsanwendungen.

Bei der Auswertung von Rechnernutzungsspuren stehen z.B. die Analyse und Interpretation von Protokoll- bzw. Verlaufsdaten und Dateizeitstempeln sowie die Zuordnung vorhandener Dateien und Spuren zu einzelnen Nutzern im Vordergrund. Dabei werten unsere Experten Daten aller gängigen Betriebs- und Dateisysteme aus und beherrschen die Analyse von Programmen zur Internetkommunikation und den verwendeten Protokollen.

FAST DETECT

VORGEHEN BEI DER AUSWERTUNG

WERKZEUGE UND METHODEN

Wir setzen hardwarebasierte Schreibschutzsysteme für alle Arten von wiederbeschreibbaren Speichermedien ein, um zu verhindern, dass Inhalte auf Beweismitteln verändert werden. Die Auswertung der Daten erfolgt mit weltweit bei Ermittlungsbehörden anerkannten IT-Forensik-Werkzeugen und mit von FAST-DETECT entwickelten Spezialprogrammen.

Unsere Versionsverwaltung und Softwareverteilung garantiert definierte sowie einheitliche Softwarestände und gewährleistet somit auch die Nachprüfbarkeit von Befunden.

Alle relevanten Auswertungsprozesse folgen den Vorgaben der ISO Normen 27001 sowie 9001 und werden systemgestützt protokolliert.

KOSTEN

Wir sind transparent in der Auftragsbearbeitung, wahren die Verhältnismäßigkeit der Mittel und rechnen auf Stundenbasis ab.

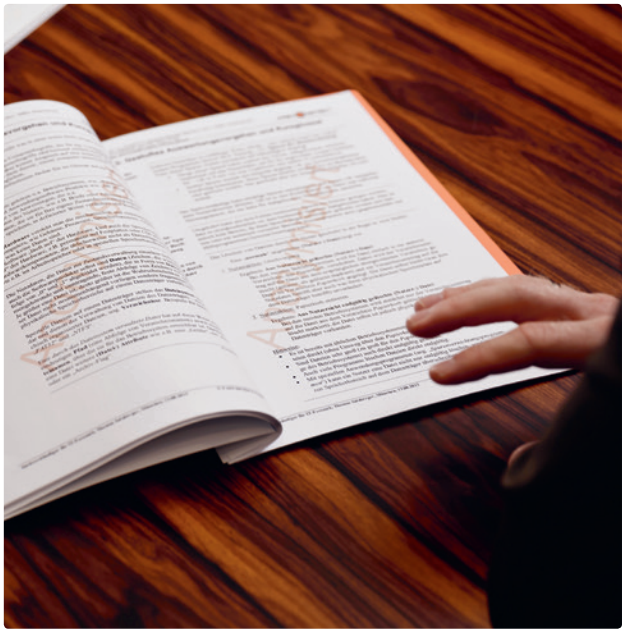
Für Justizbehörden erfolgt die Abrechnung gemäß JVEG. Alle dabei anfallenden Kosten sind Verfahrenskosten.

Wir beantworten ausschließlich die im Beweisbeschluss oder im Auftrag gestellten Fragen.

In folgenden Fällen halten wir umgehend Rücksprache mit unseren Auftraggebern, bevor wir mit der Auswertung fortfahren:

- Wir finden Hinweise auf weitere, nicht im Auftrag genannte Straftaten
- Wir können Informationen für Folgeermittlungen liefern
- Weitere sinnvolle Auswertungsschritte wären mit deutlichen, zusätzlichen Kosten verbunden. Hierbei informieren wir über die Erfolgsaussichten möglicher weiterer Maßnahmen.

Die Auftraggeber können dann auf Grundlage der bisherigen Ergebnisse und unserer Einschätzung die weiteren Auswertungsschritte festlegen und haben somit die größtmögliche Kostenkontrolle.



DIE FAST-DETECT GUTACHTEN

Das Ergebnis unserer Auswertungen ist häufig ein IT-Forensik-Gutachten, das vor Gericht ein Beweismittel darstellt und der Wahrheitsfindung dient.

DIE IHK-EMPFEHLUNGEN

Die IHK-Empfehlungen für Gutachten sind unseres Erachtens wichtige Anforderungen an ein gerichtsfestes Gutachten und werden von uns umfassend berücksichtigt: FAST-DETECT-Gutachten werden durch unsere erfahrenen Sachverständigen objektiv, unparteiisch und weisungsfrei erstellt, sowie inhaltlich korrekt, nachprüfbar, nachvollziehbar und für Laien verständlich verfasst.

WEITERE GÜTEKRITERIEN UNSERER GUTACHTEN

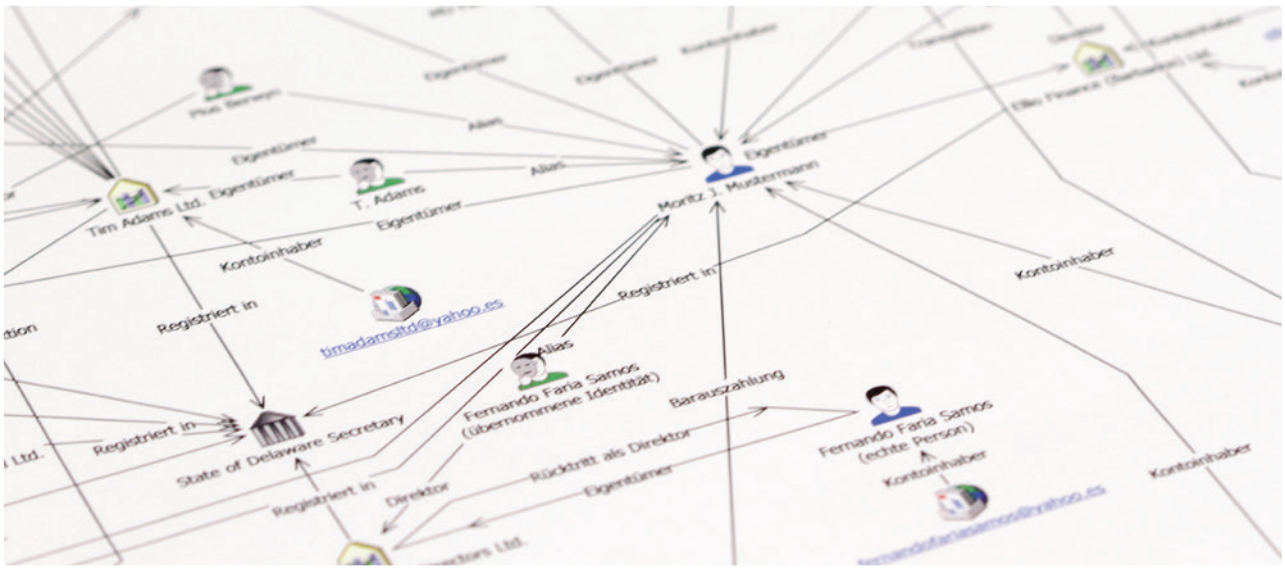
Damit unsere Gutachten wirklich hilfreich sind, befolgen wir zudem unter anderem folgende Punkte:

1. Wir beantworten alle wesentlichen Fragen und orientieren uns bei der Gliederung und Formulierung der Befunde am Leser.
2. Wir trennen klar zwischen dem Auswertungsergebnis und unserem Vorgehen.
3. Wir unterscheiden deutlich erkennbar zwischen dem Befund (Fakten) und unseren Ableitungen.
4. Wir lagern Definitionen, Glossarbegriffe und Bewertungshilfen sowie lange und komplexe Belege in Anhänge aus. Komplizierte Sachverhalte werden durch Tabellen, Grafiken oder Bildschirmfotos übersichtlich und verständlich dargelegt.
5. Wir verwenden ein wissenschaftlich erprobtes Layout, das ein schnelles Lesen und Erfassen unserer Gutachten ermöglicht.
6. Ein zweiter, nicht an der Auswertung beteiligter, Sachverständiger, führt eine Qualitätssicherung durch.

GÜTEKRITERIEN UNSERER KIPO-GUTACHTEN

Für unsere Gutachten im Bereich Kinderpornografie befolgen wir zusätzlich folgende Punkte:

1. Wir gliedern den Befund nach geltenden Gesetzen, berücksichtigen aktuelle Urteile und weisen Tatmehrheiten aus, ohne dabei den Sachverhalt juristisch zu bewerten.
2. Wir nehmen häufige Einlassungen vorweg und gehen mit Wahrscheinlichkeiten hilfreich um.
3. Kinder- und jugendpornografische Schriften drucken wir getrennt vom Gutachten in separaten Anhängen ab.



WIRTSCHAFTSKRIMINALITÄT

So gut wie keine Straftat aus dem Bereich Wirtschaftskriminalität kann ohne die Unterstützung von EDV-Systemen begangen werden. Dies bedeutet, dass bei der Aufklärung von Wirtschaftsstraftaten IT-Systeme fast immer wertvolle Informationen beinhalten.

Relevante Informationsquellen können beispielsweise folgende IT-Systeme sein:

- CRM- und ERP-Systeme
- Buchhaltungsysteme
- Kommunikationssysteme, wie E-Mail, Chat etc.
- Dokumente in analoger oder digitaler Form

Beispiele für Delikte aus dem Bereich Wirtschaftskriminalität sind Abrechnungsbetrug oder Kick-Back-Zahlungen.

ALLGEMEINES VORGEHEN

Zunächst gilt es zu bestimmen, welche IT-Systeme relevante Daten für die Aufklärung von Wirtschaftsstraftaten verarbeiten oder speichern. Diese IT-Systeme müssen anschließend im Unternehmensumfeld IT-forensisch gesichert werden – möglichst so, dass der Geschäftsbetrieb nur wenig gestört wird.

Durch die Verknüpfung einzelner Datenquellen bei der Analyse können einerseits schnell Ergebnisse geliefert und anderseits mehr Informationen extrahiert werden. So kann der Sachverhalt möglichst vollständig aufgeklärt werden.

Hierbei arbeiten die IT-Forensiker bei FAST-DETECT sehr eng und effizient mit dem Auftraggeber zusammen.

BEISPIELE FÜR WIRTSCHAFTSKRIMINALITÄT

ABRECHNUNGSBETRUG

Für die Erkennung und den Nachweis einer Abrechnungsmanipulation im Gesundheitswesen müssen strukturierte Daten aus den Abrechnungssystemen der jeweiligen Praxen analysiert und aufbereitet werden.

KICK-BACK-ZAHLUNGEN

Als Kick-Back-Zahlung oder verdeckte Provision bezeichnet man die unrechtmäßige Rückerstattung von Teilbeträgen eines Geschäfts. Für die Aufdeckung oder den Nachweis von Kick-Back-Zahlungen sind z.B. Kommunikationsdaten wie E-Mails und Chats von zentraler Bedeutung. So kann möglicherweise die Abstimmung zwischen den beteiligten Parteien identifiziert und nachvollzogen werden.

BETRUGSDELIKTE

Betrugsdelikte können in verschiedenen Formen auftreten. Für die effiziente Aufklärung können unterschiedliche Informationsquellen in einem Unternehmen herangezogen werden. So können zum Beispiel Daten aus einem CRM- oder ERP-System mit Kommunikationsdaten verknüpft werden, um in der Gesamtheit mehr sachverhaltsrelevante Informationen festzustellen als bei der Analyse einzelner Datenquellen.

LEISTUNGSSPEKTRUM BEI DOLOSEN HANDLUNGEN

FAST-DETECT bietet Ihnen für die schnelle und effiziente Aufklärung von dolosen Handlungen folgende Leistungen an:

- Extraktion von relevanten Daten aus verschiedensten Systemen, wie Buchungs-, ERP, CRM- und Dokumentenmanagement-Systemen
- Aufbereitung von Daten für die weitere Analyse durch Sachbearbeiter
- Vollständige Analyse durch FAST-DETECT zur Aufklärung eines Sachverhalts

CYBERCRIME

Cybercrime oder Computerkriminalität ist zu einem Massenphänomen geworden – insbesondere was den Teilbereich der Internetkriminalität angeht.

Angriffe können sowohl einen hohen monetären Schaden als auch Reputationsschäden verursachen.

Hierzu zählen neben Angriffen von Außen zum Beispiel zum Zweck der Industriespionage auch von Mitarbeitern verursachte Datenlecks sowie mittels Computern durchgeführte Betrugsdelikte.

Bei der forensischen Aufbereitung eines Cybercrime-Vorfalls stehen folgende Ziele im Vordergrund:

- Sicherung aller relevanten Daten
- Schnelle Identifikation des Modus Operandi, um den oder die Täter zu identifizieren
- Identifikation des Geldflusses und Durchführung von De-Anonymisierungsmaßnahmen
- Identifikation der Täter und der Opfer

CYCERCRIME IST EINE WESENTLICHE HERAUSFORDERUNG DES 21. JAHRHUNDERTS

Spuren in der digitalen Welt zu identifizieren, sicherzustellen und die richtigen Schlüsse daraus zu ziehen bedarf einer enormen Expertise. FAST-DETECT kann Sie zeitnah mit den richtigen Experten unterstützen. Dabei bereiten wir alle sachverhaltsrelevanten Befunde auch für IT-Laien einfach und verständlich auf.

BEISPIELE FÜR CYBERCRIME

FAKE-SHOPS

Ein unbekannter Täter bietet gefälschte oder nicht vorhandene Smartphone-Modelle in diversen Webshops weit unter dem Marktwert an. Hierfür hat er eine umfassende Werbekampagne erstellt und setzt auf modernste Technik, so dass die Webshops kaum von validen Shops zu unterscheiden sind.

FAST-DETECT führt eine Beweissicherung durch. Auf Basis von direkt im Anschluss durchgeführten Analysen der Webshop-Datenbanken lassen sich Opfer schnell identifizieren und kontaktieren. Außerdem kann der Schaden anhand der im Webshop protokollierten Verkäufe beziffert werden.

Darüber hinaus können anhand der Webshop-Zugriffsprotokolle und der Metadaten gesicherter E-Mails häufig die Täter identifiziert werden.

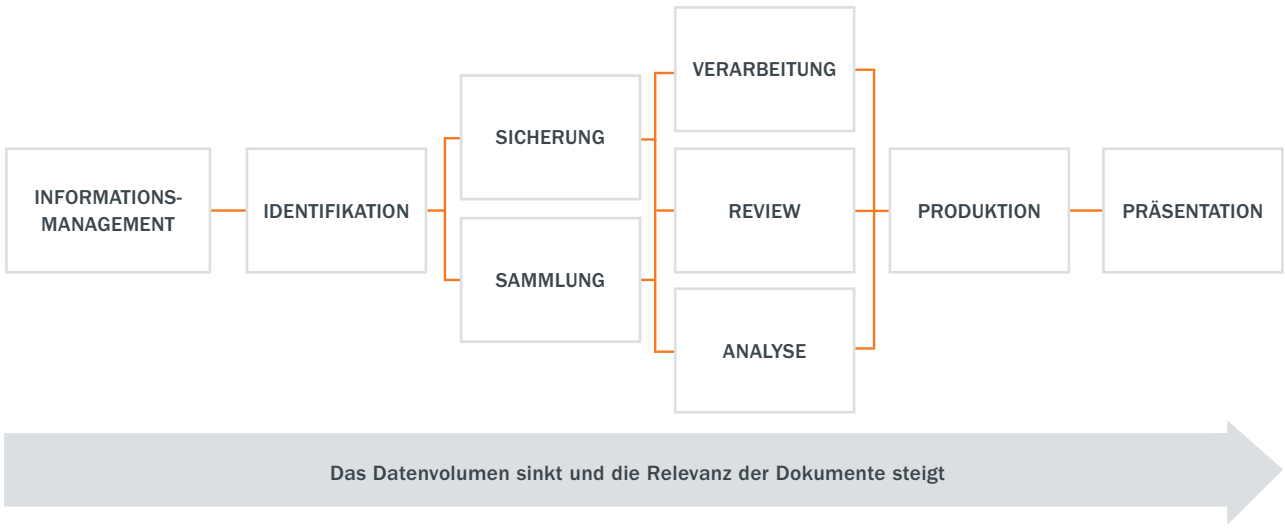
BITCOIN-FORENSIK

Die Cryptowährung Bitcoin hat sich in den letzten Jahren als bevorzugtes Zahlungsmittel im Bereich Cybercrime etabliert. Sowohl das Senden als auch das Empfangen von Zahlungen ist völlig anonym möglich. Im Gegensatz zum klassischen Zahlungsverkehr sind sämtliche Transaktionen jedoch öffentlich für jedermann einsehbar.

Bei der IT-forensischen Auswertung von Bitcoin-Wallets auf sichergestellten Beweismitteln lassen sich daher Aussagen zur Größenordnung der über das Konto transferierten Geldbeträge treffen. Entsprechende Bitcoin-Konten können auch aus gelöschten Speicherbereichen wiederhergestellt werden. Sofern das Wallet noch Bitcoins enthält können diese ggf. beschlagnahmt werden. Durch die Analyse von eingehenden und ausgehenden Transaktionen (Verfolgen des Geldstroms) lassen sich unter Umständen Empfänger oder Absender von Zahlungen identifizieren.

WICHTIGE FAKTEN

- FAST-DETECT besitzt mehr als 10 Jahre Erfahrung im Bereich Cybercrime.
- FAST-DETECT kann im DACH-Gebiet schnell Experten und Teams zur Unterstützung und Aufklärung von Cybercrime Fällen zur Verfügung stellen.



Electronic Discovery Reference Modell – Rahmen für die standardisierte Realisierung von Dokumentenreviews

eDISCOVERY

BEGRIFFSKLÄRUNG

Der Begriff eDiscovery stammt aus dem Angelsächsischen und beschreibt den Prozess der Identifikation, Durchsuchung, Erfassung, Sicherung und Aufbereitung elektronischer Daten im Hinblick auf die Nutzung als Beweismittel in einem Zivil- oder Strafverfahren. Er wird somit häufig verwendet, wenn in einer Untersuchung eine Vielzahl an Dokumenten, wie z.B. Office Dokumente und E-Mails, durchsucht und gesichtet werden muss.

Insbesondere in umfangreichen Fällen muss eine große Anzahl an Dokumenten und Kommunikationsdaten verschiedenster Personen zielgerichtet ausgewertet und aufbereitet werden. Hierfür bietet die eDiscovery eine optimale Möglichkeit, die Datenflut effizient zu bewältigen.

UNSER LEISTUNGSSPEKTRUM

Wir folgen den Phasen des EDRM Modells (siehe Grafik) und bieten dem Auftraggeber eine optimierte Infrastruktur, um Daten selbst oder in Teams durchsuchen, filtern und analysieren zu können, ohne dass dazu spezielle Hardware, Software oder tiefergreifendes technisches Know-how beim Auftraggeber vorhanden sein muss.

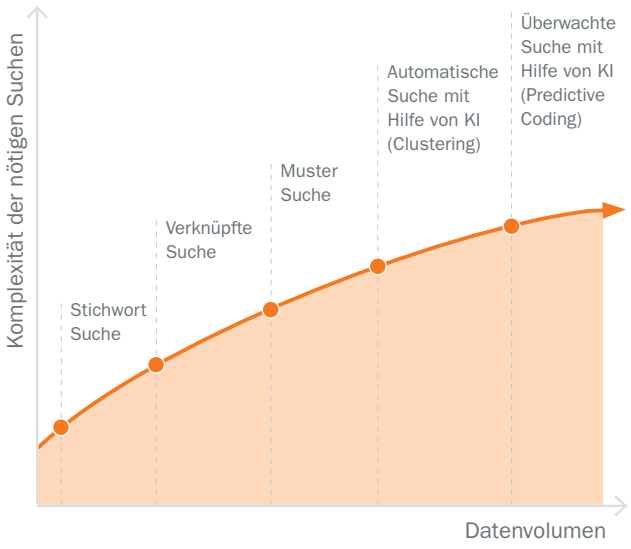
Das EDRM Modell definiert einen einheitlichen Rahmen für die unterschiedlichen Phasen von eDiscovery bzw. Dokumentensichtungsprojekten. FAST-DETECT begleitet den Auftraggeber bei allen Phasen des Modells von der Identifikation bis zur Präsentation und ermöglicht somit eine sehr effiziente und zielgerichtete Analyse von Massendaten.

TECHNISCHE MÖGLICHKEITEN DER DOKUMENTEN-SICHTUNG BEI FAST-DETECT

Die große Herausforderung beim Umgang mit Massendaten ist die effiziente Suche und Filterung zur Identifikation potenziell relevanter Dokumente. Die von FAST-DETECT bereitgestellte Software bietet alle Möglichkeiten des Suchens bis hin zum Predictive Coding – einem Verfahren, mit dem anhand von Beispieldokumenten durch die Software selbstständig weitere relevante Dokumente identifiziert werden (siehe Grafik).

Die durch die Suchen identifizierten Dokumente können so auch in größeren Teams durchgesehen werden – unabhängig vom Ursprungsformat der Daten. Während der Durchsicht können Dokumente in unterschiedliche Kategorien einsortiert und einem mehrstufigen Reviewprozess zugeführt werden.

Darüber hinaus werden weitere wichtige Funktionen unterstützt. Hierzu zählen das Schwärzen von Dokumentenpassagen, die Durchführung von Zeitstrahlanalysen und die Visualisierung von Kommunikationsdaten.



Steigendes Datenvolumen erfordert immer komplexere Suchtechnologien

WICHTIGE FAKTEN

- Die Datenspeicherung erfolgt bei FAST-DETECT oder ausschließlich in deutschen, speziell gesicherten Rechenzentren oder bei den Auftraggebern vor Ort
- Die Software ist auf die Nutzung durch Nicht-Techniker ausgelegt
- Vielzahl an Möglichkeiten zur Durchsuchung und Darstellung von Dokumenten

VEREINBAREN SIE EINE LIVE-DEMONSTRATION MIT UNS.

KINDERPORNOGRAFIE

Kinder sind aufgrund ihrer Unfähigkeit zur Gegenwehr häufig Opfer sexueller Gewalt. Neben den Fällen der organisierten Kriminalität (z.B. Sextourismus), kommen die Täter im überwiegenden Teil der Fälle aus dem näheren Bekannten- oder Verwandtenkreis des Opfers. Die meist männlichen Täter finden sich in allen gesellschaftlichen Schichten – vom Arbeitslosen bis zum Spitzenpolitiker. Während die Gesamtzahl der Missbrauchsfälle gemäß der polizeilichen Kriminalstatistik relativ konstant bleibt, werden die Taten aufgrund der steigenden Verfügbarkeit digitaler Kameras immer häufiger zum Gegenstand kinderpornografischer Schriften gemacht. Zudem sorgt allein die Kenntnis der Existenz von Missbrauchsaufnahmen beim Opfer für eine fortgesetzte Traumatisierung und im Fall der Verbreitung im Internet für eine kontinuierliche Viktimisierung.

DAS GESETZ

Zum Schutz von Kindern gibt es in den meisten Ländern neben den Gesetzen gegen Kindesmissbrauch auch Gesetze, die nicht nur den Tausch kinderpornografischer Schriften sondern auch deren Besitz unter Strafe stellen. Studien zeigen eine große Überschneidung zwischen Missbrauchstätern und Konsumenten von Kinderpornografie. So geben ca. 25 % der Konsumenten von Missbrauchsabbildungen an, selbst schon einmal ein Kind missbraucht zu haben[1].

DIE SITUATION DER KRIMINALPOLIZEI

Die personellen und technischen Ressourcen der Kriminalermittlungsbehörden sind begrenzt bzw. lassen sich vielerorts nicht schnell genug an die stetig steigenden Anforderungen anpassen.

Dies führt in vielen Bundesländern zu Engpässen und Abarbeitungsrückständen bei Ermittlungen, Sicherstellungen und in der IT-forensischen Auswertung mit zum Teil gravierenden Folgen.

BEGRIFFSERKLÄRUNGEN

Pädophilie ist eine schicksalhafte Ausprägung der Sexualpräferenz, die keinerlei Rückschlüsse auf das Sexualverhalten eines Betroffenen zulässt.

Pädokriminalität bezeichnet das kriminelle Verhalten im Zusammenhang mit dem sexuellen Kindesmissbrauch, Kinderhandel, Kinderprostitution und Kinderpornografie.

Pädosexualismus ist das ideologische Eintreten für die Bagatellisierung und Legalisierung von sexuellen Kontakten zwischen Erwachsenen und Kindern.

[1] Mikado Studie, Module Mik1, Mik4, A1, D01, D02, 2015

FAST DETECT

ENTLASTUNG DURCH PERSONELLE UNTERSTÜTZUNG

- Für die Auswertung gebundene Ressourcen der Polizei werden wieder frei für Ermittlungen.
- Sicherstellungen können wieder zeitnah erfolgen, so dass sich die Sachverhalte häufiger auf der vom Beschuldigten aktuell genutzten Hardware nachvollziehen lassen.
- Tatbeteiligungen Dritter lassen sich durch zeitnahe Folgeermittlungen häufiger aufklären.
- Die Verfahrensdauer lässt sich insgesamt verkürzen und ausgesprochene Strafen entfalten aufgrund ihres engeren zeitlichen Bezugs zur Tat eine bessere präventive Wirkung.
- In Missbrauchsfällen wird ein früheres Intervenieren zur Beendigung des Missbrauchs sowie zur Verhinderung der Verbreitung von Missbrauchsaufnahmen ermöglicht.
- Durch kürzere Auswertungszeiten kann bei falschen Verdächtigungen die Zeitspanne begrenzt werden, für die ein Beschuldigter der Stigmatisierung im Kontext der Kinderpornografie ausgesetzt ist.

ENTLASTUNG DURCH UNSERE BESONDERE EXPERTISE

- Bei der Sicherstellung wird eine vollständige Beweissicherung gewährleistet. Dabei werden auch verschlüsselte und in der Cloud abgelegte Daten bestmöglich mit einbezogen.
- In der IT-forensischen Auswertung werden die Beweismittel zuverlässig und mit der gebotenen Sorgfalt und Auswertungstiefe ausgewertet. Komplexe Sachverhalte und Befunde werden in einer für Laien verständlichen Form im Gutachten dokumentiert.
- In der Verhandlung wird das Gutachten erstattet und es kann die Plausibilität von Einlassungen des Beschuldigten eingeschätzt werden.

ENTWICKLUNG

- Die Menge an kinderpornografischen Schriften und deren „Qualität“ (Auflösung, Abspiellänge, Härtegrad) sowie deren Tausch über das Internet nehmen rapide zu.
- Verschlüsselungen, Anonymisierungsdienste, kleinste Speichermedien, Cloud-Speicherdienste, spezielle passwortgeschützte Foren oder Chatrooms und Anonymisierungsnetzwerke werden immer häufiger genutzt und erschweren sowohl die IT-forensische Auswertung als auch die Ermittlung von Tätern.
- Die auszuwertenden Datenmengen sowie die Komplexität der Auswertungen nehmen zu und führen zu einer sehr langen Verfahrensdauer.
- Bis vor wenigen Jahren haben sich die meisten Gerichte oft nur mit Besitz und offensichtlichen Bezugs- und Weitergabehandlungen auseinandergesetzt. Mittlerweile verlangen die in Kinderpornografie-Verfahren technisch versierteren Prozessparteien zunehmend nach detaillierten Informationen zur Kenntnis und zum willentlichen Umgang des Computernutzers mit kinderpornografischen Schriften.

FALLZAHLEN IN DEUTSCHLAND

- Die Fallzahlen (im Bereich Besitz / Verschaffung und Verbreitung kinderpornografischer Schriften) liegen im Mittel konstant bei ca. 6.200 Fällen pro Jahr[1].
- Kinderpornografie zählt zu den Kontrolldelikten, deren Auftreten meist erst durch Kontrollen von Polizei und Sicherheitspersonal festgestellt wird. Dabei spiegeln die statistisch erfassten Fallzahlen die Kontrolldichte wieder und lassen aufgrund der hohen Dunkelziffer meist keine Rückschlüsse auf die tatsächlichen Fallzahlen zu.

[1] PKS Bundeskriminalamt, 2010 -2014

FAST DETECT

KINDERPORNOGRAFIE

UNSER VORGEHEN

Wir suchen nach kinderpornografischen oder in diesem Kontext anderweitig auffälligen Schriften und werten Rechnernutzungsspuren – insbesondere relevante Programme aus, wie z.B.:

Webbrowser, E-Mails, (Video)-Chat- und Messengerprogramme, Peer-to-Peer- und Friend-to-Friend-Tauschbörsen, soziale Netzwerke, Cloud-Speicherdienste und Nachrichtenboards im Internet.

KOSTENBEWUSSTSEIN

Wir nutzen eigene, etablierte und sehr effiziente Prozesse und Wissensdatenbanken, einschließlich großer Hashwert-Datenbanken und selbst entwickelter Softwareprogramme.

Zudem halten wir gezielt Rücksprache, um unseren Auftraggebern über die Steuerung der Auswertungstiefe eine maximale Kostenkontrolle zu ermöglichen.

VORGEHEN BEI MISSBRAUCHSVERDACHT

Durch unsere spezielle Missbrauchsauswertung erkennen wir Missbrauchstaten, identifizieren Tatmehrheiten und helfen bei der Identifizierung von Tätern und Opfern.

Falls bei der Beauftragung bereits ein Missbrauchsverdacht vorliegt oder im Rahmen der Auswertung ein solcher entsteht, werten wir in der Regel nach Rücksprache alle Beweismittel vollständig aus.

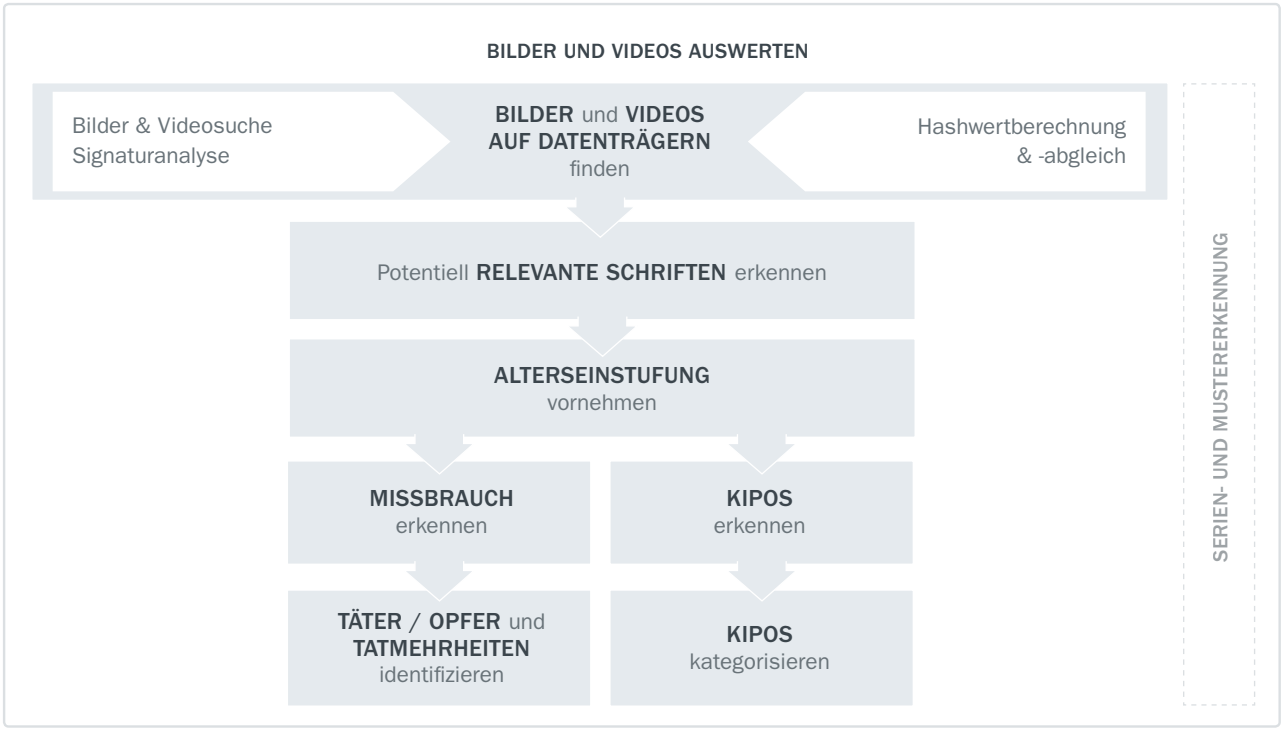
ERGEBNISSE DER AUSWERTUNG

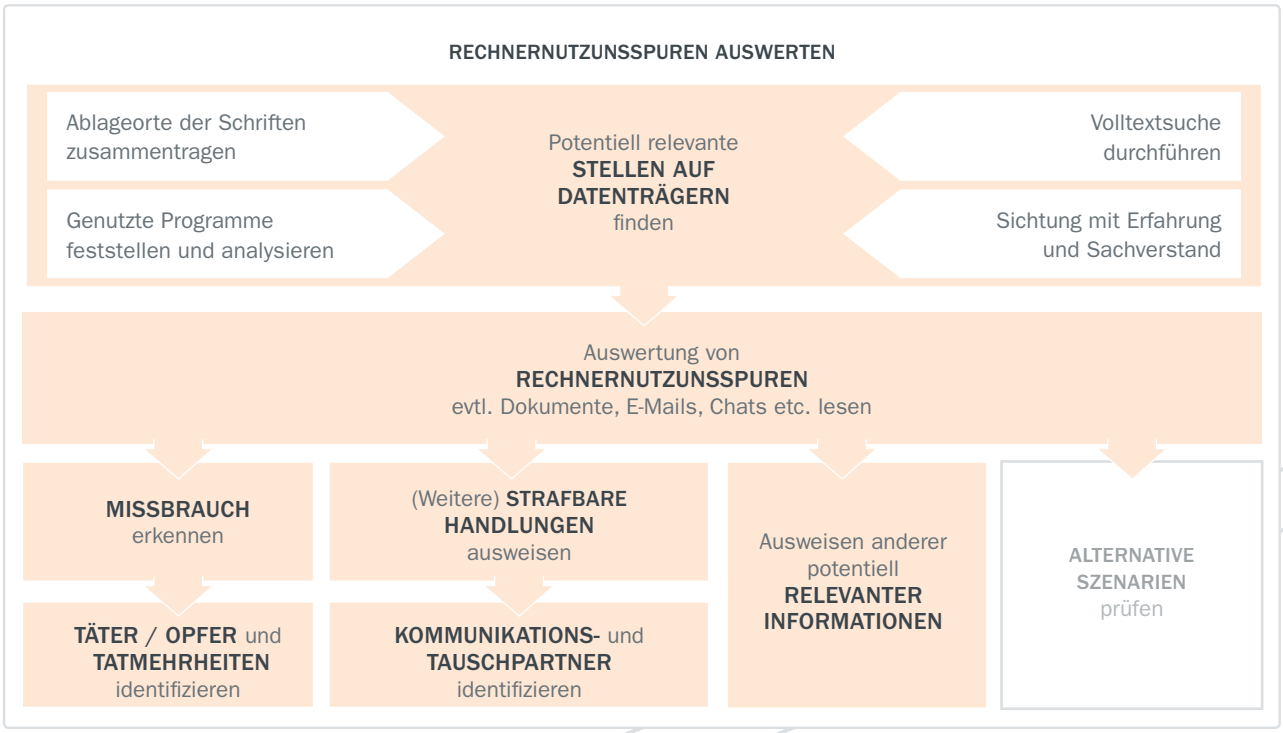
- Wir identifizieren und kategorisieren kinderpornografische Schriften (z.B. nach Alter, Darstellung).
- Wir listen alle Informationen zu festgestellten kinderpornografischen Schriften sowie zu strafbaren Handlungen auf – z.B. Zugänglichmachungs-/Verbreitungs-, Weitergabe-, Bezugs- oder Vorbereitungshandlungen.
- Wir ermöglichen den Gerichtsparteien eine eigene Einschätzung darüber,
  - wie bewusst/gezielt ein Umgang mit kinderpornografischen Schriften stattgefunden hat und
  - wie plausibel bestimmte Einlassungen in diesem konkreten Fall sind.
- Wir weisen Missbrauchshandlungen durch den Beschuldigten oder gegebenenfalls identifizierbare Dritte aus und unterstützen die Identifizierung von Opfern und Tathandlungen.
- Wir ermöglichen Folgeermittlungen.

UNSERE ERFAHRUNGEN UND ERFOLGE

- Über 3.000 Auswertungen im Kinderpornografie-Kontext
- In 6 % der Fälle Missbrauchserkennung – inkl. Täter-, Opfer- und Tat-Identifizierung. In der Hälfte dieser Fälle war der Missbrauch vorher nicht bekannt
- In ca. 70 % der Fälle Ausweisen von strafbaren Handlungen
- Nachweis von Verbreitung in 30 %, Bezug in 50 % und Weitergabe in 15 % aller Fälle
- Einsatz von Verschlüsselung durch den Beschuldigten in über 30 % der Fälle. In 25 % dieser Fälle konnten die Daten entschlüsselt werden.

FAST DETECT


BILDER UND VIDEOS AUSWERTEN
Bilder & Videosuche
Signaturanalyse
BILDER und VIDEOS AUF DATENTRÄGERN finden
Hashwertberechnung & -abgleich
Potentiell RELEVANTE SCHRIFTEN erkennen
ALTERSEINSTUFUNG vornehmen
MISSBRAUCH erkennen
KIPOS erkennen
TÄTER / OPFER und TATMEHRHEITEN identifizieren
KIPOS kategorisieren
SERIEN- UND MUSTERERKENNUNG


RECHNERNUTZUNSSPUREN AUSWERTEN
Ablageorte der Schriften zusammentragen
Genutzte Programme feststellen und analysieren
Potentiell relevante STELLEN AUF DATENTRÄGERN finden
Volltextsuche durchführen
Sichtung mit Erfahrung und Sachverstand
Auswertung von RECHNERNUTZUNSSPUREN
evtl. Dokumente, E-Mails, Chats etc. lesen
MISSBRAUCH erkennen
(Weitere) STRAFBARE HANDLUNGEN ausweisen
Ausweisen anderer potentiell RELEVANTER INFORMATIONEN
ALTERNATIVE SZENARIEN prüfen
TÄTER / OPFER und TATMEHRHEITEN identifizieren
KOMMUNIKATIONS- und TAUSCHPARTNER identifizieren

FAST DETECT

KINDERPORNOGRAFIE

ALTERSEINSTUFUNG

Wenn es Bild- und Videomaterial zulassen, orientieren wir uns zur Alterseinstufung an den Tanner-Stadien (Marschall, Tanner: Variations in pattern of pubertal changes in girls and boys, 1969/1970), die die Entwicklung vor, während und nach der Pubertät in fünf Phasen beschreiben (siehe Grafik).

Diese beschreiben für jedes Pubertätsstadium die eindeutig erkennbare Entwicklung der primären Geschlechtsmerkmale, die sich für die weitaus überwiegende Anzahl an Kindern zeitlich sehr genau eingrenzen lässt.

Da in kinderpornografischen Schriften abgebildete Personen nur dem Anschein nach Kinder sein müssen, eignen sie sich hervorragend zur Identifikation derartiger Schriften.

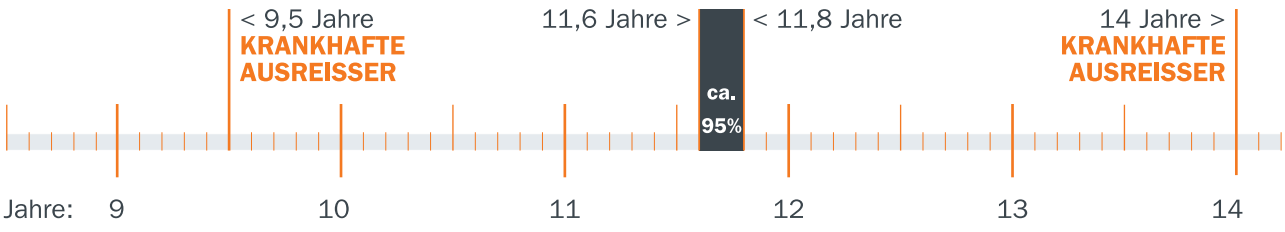
Eine intuitive, sehr unterschiedliche und meist willkürliche Alterseinstufung wird damit vermieden.

TANNER STADIEN

ABGRENZUNG ZUR JUGENDPORNOGRAFIE

Aufgrund der begrenzt objektiven Erkennbarkeit jugendpornografischer Schriften werden hierunter meist nur Schriften aus dem Grenzbereich zur Kinderpornografie subsumiert.

BEISPIEL: EINTRITTSALTER IN DAS STADIUM III BEI MÄDCHEN



KENNTNIS-NACHWEISE

Häufig wird die Täterschaft bei Besitz und dem sich Verschaffen von kinderpornografischen Schriften geleugnet, indem die Beschuldigten angeben, von den festgestellten kinderpornografischen Schriften keine Kenntnis zu haben.

Wir weisen deshalb unter anderem aus, wenn kinderpornografische Schriften ...

- in sehr großer Anzahl vorliegen oder einen hohen Prozentsatz innerhalb anderer Bild- und Videodateien einnehmen,
- nachweislich betrachtet wurden,
- auf mehreren Datenträgern in unterschiedlichsten Ablageorten bzw. in mehreren Backups liegen,
- über einen längeren Zeitraum (evtl. über mehrere Rechnergenerationen) erstellt und kopiert wurden,
- aus einschlägigen Quellen oder über mehrere unterschiedliche Rechner, Kanäle und Programme bezogen wurden oder in Chats bzw. E-Mails angefordert bzw. kommentiert wurden,
- regelmäßig, immer zu bestimmten Zeiten, sofort nach dem Anmelden oder parallel zu anderen dem Nutzer zuzuordnenden Aktionen bezogen, weitergegeben oder zugänglich gemacht wurden,
- leicht zugänglich sind, in eindeutig benannte Ordner sortiert oder in Ordnern mit Privatfotos oder eigenen Dokumenten abgelegt wurden,
- gezielt gesucht, bearbeitet, zusammengefasst, in andere Dokumente eingebunden, verschleiert oder verschlüsselt wurden,
- auf CD / DVD gebrannt bzw. auf externe Datenträger kopiert wurden.

VORWEGNAHME VON ÜBERPRÜFUNGEN

Wir weisen ohne großen Mehraufwand stets die Summe der Indizien aus, die für die Kenntnis des Rechnernutzers von den Daten bzw. einen gezielten Umgang dessen damit sprechen. Dadurch nehmen wir eine Vielzahl an Überprüfungen vorweg, die sonst später zur Beurteilung von in der Gerichtsverhandlung vorgebrachten Einlassungen zum Sachverhalt erforderlich wären. Unter anderem lassen sich so Einlassungen, wie dass z.B. ein Trojaner für den Befund verantwortlich sei, schnell und zuverlässig bezüglich Glaubhaftigkeit beurteilen.

NACHTRÄGLICHE ERGÄNZENDE GUTACHTEN

Falls sich später vorgebrachte Einlassungen nicht ausreichend anhand des bereits erstellten Gutachtens beurteilen lassen, besteht die Möglichkeit, zusätzliche Fragen des Gerichts und der am Verfahren beteiligten Anwälte durch ein Ergänzungsgutachten zu klären.

Dadurch fallen Kosten für zusätzliche Überprüfungen seltener Einlassungen nicht standardmäßig sondern erst im Rahmen ergänzender Auswertungen an.

KINDERPORNOGRAFIE

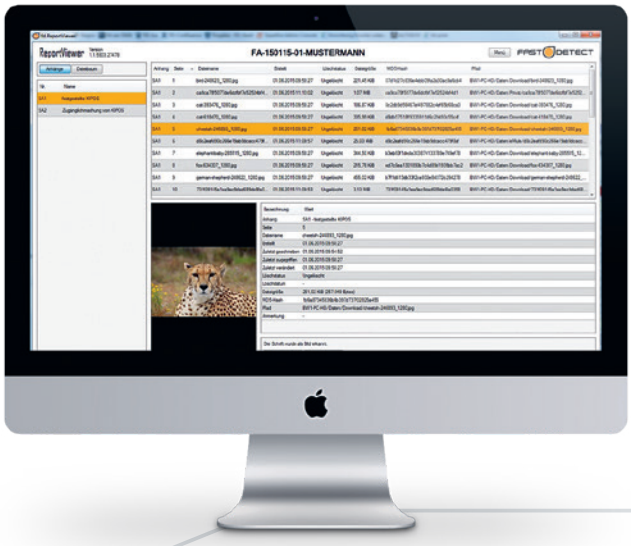
UMFANG UNSERER AUSLIEFERUNG

Die Auslieferung unserer Arbeitsergebnisse umfasst folgende Punkte:

1. Gutachten, das den Befund, unsere Einschätzung und unser Vorgehen gerichtsfest und hilfreich beschreibt.
2. Zu den festgestellten kinderpornografischen Schriften:
   - Separate Anhänge und Dateien
   - Software zum Anzeigen der festgestellten Schriften mit allen Metadaten
   - Metainformationen als EXCEL-Dokument zur effizienten Weiterverarbeitung mit direkter Verlinkung zum ReportViewer.
3. Auf Wunsch können Informationen für Folgeermittlungen in separaten Berichten und auf separate Rechnung ausgewiesen werden.

BESONDERHEITEN UNSERER GUTACHTEN

Neben den hohen Anforderungen, die wir an unsere IT-Forensik-Gutachten stellen, zeichnen sich unsere Kinderpornografie-Gutachten zusätzlich dadurch aus, dass wir sie unter technischen Gesichtspunkten und ohne juristische Wertung nach Straftatbeständen gliedern und Stichtage von Gesetzesänderungen berücksichtigen. Hierdurch ermöglichen wir dem Gericht die juristische Bewertung und Einordnung der festgestellten technischen Befunde.



DER REPORTVIEWER

Die von FAST-DETECT entwickelte Spezialsoftware „ReportViewer“ erlaubt unseren Auftraggebern eine einfache Betrachtung der von uns kategorisierten kinderpornografischen Schriften sowie aller vorhandenen Metainformationen mit Verweisen in die ausgedruckten separaten Anhänge.

AUSWERTUNG MOBILER GERÄTE

ZUNEHMENDE RELEVANZ

Smartphones und Tablet-PCs ersetzen herkömmliche Computer zunehmend sowohl im Privat- als auch im Berufsleben. Sie werden immer mitgeführt, sind immer online, werden ständig zur Kommunikation und zum Fotografieren und Filmen genutzt und speichern häufig Geolokalisationsdaten. Entsprechend wichtig sind mobile Geräte insbesondere im Rahmen der Strafverfolgung.

UNSERE LÖSUNGSANSÄTZE

Aufgrund der großen Relevanz mobiler Geräte verfügen wir über ein eigenes Team, das sich ausschließlich auf die Aufbereitung von auf mobilen Geräten gespeicherten Daten spezialisiert hat. Für die Datensicherung von neuen oder stark abgesicherten mobilen Geräten greifen wir zusätzlich auch auf spezielle Verfahren und selbst entwickelte Software zurück.

Häufig ist für jedes neue Gerät und jede neue Betriebssystem-Version die Identifikation neuer Angriffsvektoren nötig, um eine Umgehung entsprechender Sperren zu ermöglichen.

UNSER LEISTUNGSUMFANG

FAST-DETECT bietet dem Auftraggeber zwei Möglichkeiten im Bereich der mobilen Auswertung:

1. FAST-DETECT extrahiert und interpretiert die Daten und stellt sie dem Auftraggeber für weitere Analysen zur Verfügung.
2. Die ausgelesenen Daten fließen in die weitere IT-forensische Analyse und die Gutachtenerstellung durch FAST-DETECT mit ein.

TECHNISCHE HERAUSFORDERUNG

- Täglich erscheinen neue Apps und Betriebssystemversionen
- Standardmäßig hohe Sicherheitsmechanismen, wie gesetzte Codesperren, Verschlüsselung und vollständige Löschung
- Proprietäre Systeme und Schnittstellen sowie fest verbaute Massenspeicher. Für das Auslesen ist daher i.d.R. spezielles Equipment nötig, welches aktuelle Modelle allerdings oft nur zeitverzögert unterstützt
- Mobile Geräte können aus der Ferne gelöscht werden

BEWEISSICHERUNG UND SICHERSTELLUNG

WIR UNTERSTÜTZEN VOR ORT

FAST-DETECT unterstützt Ermittlungsbehörden bei der Sicherstellung von Beweismitteln und der Sicherung von Daten vor Ort – auch parallel an mehreren Standorten. Wir verhindern somit, dass wichtige Beweismittel übersehen, nicht als solche erkannt oder unsachgemäß behandelt werden.

WIR SIND AUSGERÜSTET

Eine Sicherstellung erfordert das geeignete Equipment. Dieses beinhaltet professionelle IT-forensische Software, ausreichend dimensionierte Hardware sowie spezielle Zusatzgeräte, wie z.B. Schreibschutzgeräte oder Hardware zur Sicherung mobiler Geräte.

Wir sind geschult im Umgang mit Cloud-Speicherdiensten und der Beweissicherung in sehr komplexen oder standortübergreifenden IT-Landschaften.

Eine speziell auf die Anforderungen von Sicherstellungen zugeschnittene und selbst entwickelte Software ermöglicht uns eine lückenlose Protokollierung aller wesentlichen Maßnahmen vor Ort.

WIR SICHERN DATEN IM LAUFENDEN GESCHÄFTSBETRIEB

Wir sind in der Lage, Daten so zu sichern, dass der laufende Geschäftsbetrieb in Firmen nicht oder nur geringfügig beeinträchtigt wird. Bei Bedarf können wir eine Live-Auswertung durchführen. Gerade geöffnete, verschlüsselte Container und Daten auf Servern im Internet können oft nur im laufenden Betrieb gesichert werden; würde der Rechner erst heruntergefahren oder ausgeschaltet, wäre der Zugriff auf die Nutzdaten meist nicht mehr möglich.

WIR SIND SCHNELL

Von großer Bedeutung ist häufig die zeitnahe Sicherstellung, da sich aufgrund einer zeitlich beschränkten Speicherung der Daten bestimmte Sachverhalte nicht mehr rückverfolgen oder nachvollziehen lassen. Unsere Spezialisten können deutschlandweit mit kürzester Vorlaufzeit eingesetzt werden.

FAST DETECT


FAST DETECT
Werner Poppitz
Start
RÄUME
Serverraum
Büroraum 1
Büroraum 2
BEWEISMITTEL
Tower Thermaltake links
Laptop Sony Vaio rechts
Laptop Dell Vostro
Windows 8
Synology
Datensicherung NAS
2,5" Samsung Evo


ALTOSCIR

EINZIGARTIGES KNOW-HOW

SPEZIALISIERTE MITARBEITER

Alle in der Auswertung tätigen Mitarbeiter sind hervorragend ausgebildete IT-Forensiker. Sie zeichnen sich zusätzlich durch eine Spezialisierung auf bestimmte Teilbereiche der IT-Forensik aus. Hierdurch verfügt FAST-DETECT über einzigartiges Fachwissen auch in Spezialbereichen wie z.B. Internetkommunikationsprotokolle, Kryptografie oder Live Hacking.

SOFTWARE-ENTWICKLUNG

Spezielle, von unseren IT-Experten programmierte Werkzeuge ermöglichen oder verbessern die Auswertung und Dokumentation relevanter Daten und Spuren. So können wir die Bearbeitungszeit beträchtlich verkürzen und uns gleichzeitig einen technologischen Vorsprung sichern.

WISSENSDATENBANK

Alle Mitarbeiter können auf eine wertvolle Datenquelle zugreifen – die FAST-DETECT-Wissensdatenbank. Hier sind aktuelle Rechts- und Technikinformationen, ein Großteil unseres dokumentierten Know-hows sowie alle Prozessbeschreibungen, Checklisten und Vorlagen abgelegt. Diese gesammelten Daten lassen uns einheitlich, schnell und effektiv arbeiten und halten uns stets auf dem neuesten Stand.

KOOPERATION MIT RENOMIERTEN FORSCHUNGSEINRICHTUNGEN

Wir pflegen intensiven Kontakt zu renommierten Forschungseinrichtungen. Wir halten Gastvorträge, beteiligen uns an Forschungsvorhaben und vergeben Abschlussarbeiten. So sorgen wir für einen stetigen Zustrom von neuem Wissen, aktuellen Entwicklungen und zukunftsweisenden Ideen in unser Unternehmen.

TECHNISCHE AUSSTATTUNG

MODERNE ARBEITSPLÄTZE

Alle Mitarbeiter von FAST-DETECT verfügen über eine hochmoderne technische Ausstattung, die kontinuierlich den steigenden Anforderungen angepasst wird. Hierunter fallen beispielsweise Schreibschutzsysteme für Datenträger oder Spezialsoftware und Spezialhardware für die Auswertung von Mobiltelefonen und Navigationsgeräten.

GETRENNTE NETZWERKE

FAST-DETECT betreibt zwei getrennte Netzwerke: Sämtliche Auswertungsprozesse finden aus Sicherheits- und Datenschutzgründen in einem vom Internet physikalisch getrennten Auswertungsnetzwerk statt.

Daneben hat jeder Mitarbeiter die Möglichkeit, über einen zweiten Rechner technische Sachverhalte im Internet zu recherchieren.

STATE-OF-THE-ART SERVER UND ÜBERWACHUNG

Hochleistungsserver und sehr große Speicherkapazitäten ermöglichen FAST-DETECT die zeitgleiche Abwicklung umfangreicher Projekte. Zur Vermeidung von Datenverlusten setzen wir auf ausfallsichere RAID-Verbundsysteme und ein mehrstufiges Backup-Konzept.

Unsere moderne Serverlandschaft wird permanent und vollautomatisch durch Spezialsoftware überwacht. Durch den Einsatz solider Verschlüsselungstechnologien sind alle vertraulichen Daten jederzeit sicher gespeichert.

SOFTWARE

Wir setzen ausgereifte Software und Eigenentwicklungen ein, wie z.B.:

- Weltweit von Polizei- und Finanzbehörden eingesetzte IT-Forensik-Lösungen
- Spezielle Tools zur Auswertung von Nutzungsspuren bestimmter Programme wie E-Mail- und Tauschbörsen- oder Chat-Anwendungen
- Leistungsfähige Spezialsoftware zur Wiederherstellung von gelöschten und fragmentierten Daten.
- Leistungsfähige Cluster-Lösungen für gezielte Kryptografie-Angriffe
- Ein selbst entwickeltes Auftragsverwaltungssystem zur lückenlosen Dokumentation aller auftragsbezogenen Vorgänge vom Eingang der Beweismittel bis zum Versand des Gutachtens

QUALITÄT, SICHERHEIT UND DATENSCHUTZ

Wir setzen durch unser hohes Sicherheitsbewusstsein und unsere vorbildlichen Datenschutz- und Sicherheitsmaßnahmen Standards in unserer Branche.

GESCHULTES UND ÜBERPRÜFTES PERSONAL

- Die Auswahl neuer Mitarbeiter erfolgt mit größter Sorgfalt und unter Zuhilfenahme strenger Auswahlkriterien.
- Alle Mitarbeiter mit Zugang zu unseren Geschäftsräumen werden regelmäßig einer umfangreichen und weitgehenden polizeilichen Sicherheitsüberprüfung unterzogen.
- Verbindliche ISO-konforme Sicherheitsrichtlinien, Geschäftsprozesse und Rollenbeschreibungen sind mit allen Mitarbeitern vertraglich fixiert.
- Alle Mitarbeiter werden regelmäßig zu den Themen Sicherheit, Informationssicherheit, Datenschutz, Qualitätsmanagement sowie in Bezug auf wichtige Strafvorschriften geschult.

ÜBERWACHTE RÄUMLICHKEITEN

Alle Räume, in denen sich vertrauliche Daten befinden, sind einbruchgeschützt, videoüberwacht und mit einer Alarmanlage der Klasse C gesichert.

- Eine polizeiliche Überprüfung und die Abnahme unserer Räume und baulichen Sicherungsmaßnahmen erfolgen regelmäßig und unangekündigt.
- Die Zugänge zu Sicherheitszonen sind durch eine moderne Schließanlage und ein effektives Kontrollsystem abgesichert.

Übergabe der ISO 27001 und ISO 9001 Zertifikate durch Herrn Hoffmann, TÜV Süd (links im Bild)

TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN GEMÄSS BUNDESDATENSCHUTZGESETZ

Unsere Tätigkeiten schließen fast immer den Umgang mit äußerst vertraulichen Daten, Gerichtsakten und Beweismitteln ein. Ein umfangreiches Paket an technischen und organisatorischen Sicherheitsmaßnahmen sowie eine regelmäßige Überprüfung nach den Vorgaben des BDSG sind daher die unabdingbare Basis für unsere Arbeit.

NACHWEIS DURCH ZERTIFIZIERUNGEN

FAST-DETECT erfüllt die ISO-Normen 27001 bezüglich Informationssicherheit und 9001 bezüglich Qualitätsmanagement. Diese Zertifizierungen und regelmäßig stattfindende Audits stellen sicher, dass unser hohes Qualitätsniveau auch in Phasen des Wachstums erhalten bleibt und belegen unseren verantwortungsvollen und sicheren Umgang mit sensiblen Daten.

Für unsere Auftraggeber ist dies Bestätigung und Garantie für ein Höchstmaß an Zuverlässigkeit, Vertraulichkeit und Integrität im Umgang mit Beweismitteln und sensiblen Informationen.

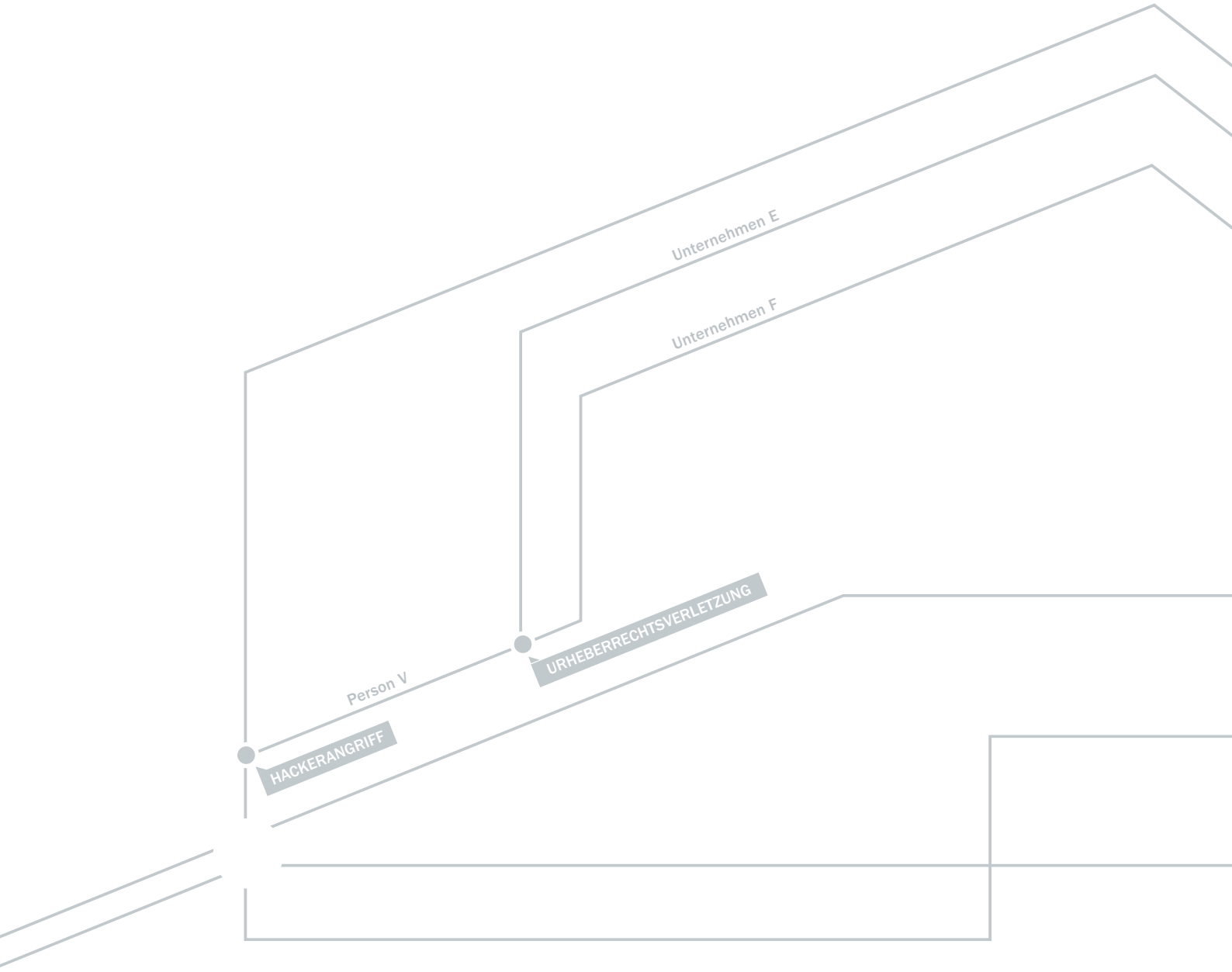
SEHEN SIE SICH UNSER DIENSTLEISTUNGS-VIDEO AN

www.fast-detect.de/video

LERNEN SIE UNS PERSÖNLICH KENNEN

Gerne zeigen wir Ihnen die Vorteile einer Zusammenarbeit mit FAST-DETECT persönlich auf, stellen Ihnen unsere Experten vor und informieren Sie vor Ort über unsere Sicherheitsvorkehrungen.

Rufen Sie uns an.
Tel +49 89 204040-0



FAST DETECT

Gerne senden wir Ihnen
detailliertes Informationsmaterial
zu bestimmten Geschäfts-
oder Themenbereichen zu.

FAST-DETECT GmbH

Inselkammerstraße 12
82008 Unterhaching
Tel +49 89 204040-0
Fax +49 89 204040-299
Mail info@fast-detect.de
Web www.fast-detect.de

10/2018