

- IT-Forensik
- IT-Sachverständige
- Datenextraktion IT-Systeme & Mobilfunk
- Verfahrensbegleitung
- Auswertung von Smartphones & Tablets
- Beweismittelsicherung & Datenwiederherstellung

INFORMATIONSBROSCHÜRE IT-FORENSIK

WWW.CWIT.DE



- Analyse von Datenspuren
 - Beweismittelauswertung
 - Forensische Sonderuntersuchungen
 - Cloud-Forensik
 - Datenrettung/-wiederherstellung
 - Sichere Datenlöschung
 - Datenextraktion
 - Datenaufbereitung
- aktuelle Werkzeuge und Methoden
 - schnell und kosteneffizient
 - sicher und zuverlässig
 - neutral und unabhängig
 - Wissen und Erfahrung durch zahlreiche Beauftragungen/Hinzuziehungen durch Ermittlungsbehörden, Gerichte und weiteren Institutionen von Justiz, Polizei und Zoll

CWIT GmbH

IT-FORENSIK / IT-SACHVERSTÄNDIGE / IT-SICHERHEIT / DATENSCHUTZ

Seit nunmehr zehn Jahren führen die Experten von CWIT IT-forensische Untersuchungen und Auswertungen ausschließlich im Auftrag von Ermittlungsbehörden durch. Als Sachverständigenbüro sind wir mit den Anforderungen unserer Auftraggeber bestens vertraut und wissen durch verständliche und nachvollziehbare Schriftstücke dem technischen Laien einen umfassenden Einblick, sowie Überblick zu verschaffen.

CWIT wertet jährlich 400 Smartphones und Tablets, 300 Festplatten, sowie 380 weitere Datenträger aus, extrahiert die Datenbestände und übergibt sie aufbereitet an die Sachbearbeitung. Die hieraus resultierende Expertise im Bereich Informationstechnik und Mobilfunk stellen wir regelmäßig als technische Prozessbegleitung im Rahmen von Gerichtsverhandlungen zur Verfügung.

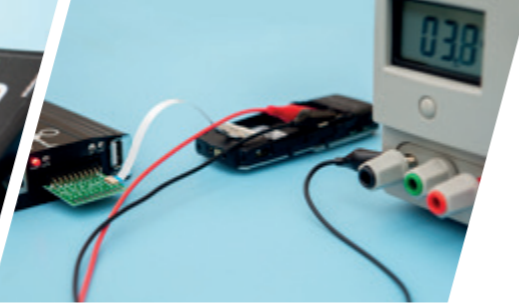
Auf den folgenden Seiten stellen wir unsere Leistungen im Bereich IT-Forensik vor.

Gerne stehen wir für ein persönliches Gespräch zur Verfügung und erläutern unsere Erfahrungen und Referenzen.

Für eine erste Kontaktaufnahme stehen wir Ihnen telefonisch unter 0 24 21 - 9 90 08-00 oder per E-Mail unter kontakt@cwit.de gerne zur Verfügung.



*Tobias Lieven und
Martin Rösler
(IT-Forensiker,
IT-Sachverständige)*



Beweismittelsicherung

Die IT-Forensik-Experten von CWIT sichern und werten folgende Geräte aus:

- Festplatten und Solid-State-Disks
- RAID-Systeme aus Servern / Storage
- USB-Sticks
- Speicherkarten (SD, CF, MMC)
- Mobiltelefone, Smartphones
- Digitalkameras
- Telefonanlagen
- Router, Switches und andere Netzwerkkomponenten
- Navigationsgeräte
- Virtuelle Server / Virtuelle Maschinen
- Datenbank-Server
- Mail-Server
- Magnetbänder
- Flash-Speicher

Die Sicherung und Aufbereitung der Daten von beschädigten oder zugriffsgeschützten Geräten zählen zu den Kernkompetenzen unserer IT-Forensiker. Hierzu steht ein eigenes Labor zur Verfügung, das mit modernster Ausstattung betrieben wird und regelmäßigen Aktualisierungen unterliegt.

- Sicherung und Auswertung von Datenträgern oder Geräten **während** oder im unmittelbaren Anschluss an Durchsuchungsmaßnahmen
- Vor-Ort-Sicherungen (mobile Auswertungsgruppe): Vermeidung von Ausfallzeiten
- Entlastung der IT-Ermittlungsunterstützung/IUK-Abteilung der Polizeibehörden
- Sachgemäße Behandlung von Beweismitteln
- Sichere Verpackung und geschützter Transport von Asservaten
- Gerichtverwertbare Datenaufbereitung
- Dokumentation einer lückenlosen Beweiskette

Arbeitsweisen und Ausstattung

- Alarmgesicherte Arbeitsräume
- Brandmeldeanlage
- Asservatenaufbewahrung in Datensicherungstresoren
- Konstante Umgebungstemperaturen
- Getrennte Netzwerkumgebungen, separiertes Auswertungsnetzwerk ohne Internetzugriff
- Alle Auswertungssysteme und Datenspeicher sind verschlüsselt
- Mitarbeiter, die mit Auswertungsarbeiten betraut sind, verfügen über eine Sicherheitsüberprüfung nach SÜG
- Alle Arbeiten unterliegen der steten Kontrolle des Vier-Augen-Prinzips
- Die Mitarbeiter verfügen über umfangreiche Kenntnisse in den Bereichen IT-Sicherheit und Datenschutz
- Regelmäßige Zertifizierungen und Fortbildungen
- Langjährige Mitarbeitertreue
- Nachvollziehbare und aufwandsgerechte Abrechnungen der Leistungen gemäß JVEG



Sicherung und Auswertung

MOBILE ENDGERÄTE (SMARTPHONES / TABLETS)

- Sicherung und Aufbereitung der Speicherinhalte mobiler Endgeräte
- Bereitstellung von Kommunikationsprotokollen von SMS, Whatsapp, Viber, Snapchat und anderen Messengern
- Extraktion von Bildern / Videos
- Chronologische Aufbereitung von Anruflisten
- GPS-Koordinaten
- Erstellung von Bewegungsprofilen
- Aufheben oder Umgehen von PIN-Sperren

Mithilfe verschiedener Techniken sind wir in der Lage, auch zugriffsgeschützte Smartphones und Tablets auszulesen:

JTAG

JTAG (Joint Test Action Group) ist ein eine Prüfmethode für elektronische Schaltungen. Moderne Mobiltelefon, Smartphones und Tablet-PCs verfügen herstellerseitig über diese Vorrichtung, sodass es möglich ist, über das JTAG-Verfahren den Datenspeicher des Endgerätes auszulesen und forensisch aufzubereiten. JTAG wird vielfach bei Endgeräten eingesetzt, bei denen der Zugriff durch PIN- oder Bildschirmsperren verhindert wird.

CHIP-OFF

Eine weitere Methode des Datenzugriffs, ist das Auslesen der Speicherbausteine. Chip-Off kommt immer dann in Betracht, wenn andere Auswertungsmaßnahmen zu keinem Erfolg geführt haben. Die Speicherbausteine / Datenträger der mobilen Endgeräte werden dabei von den Platinen gelöst, mit einer speziellen Vorrichtung ausgelesen und aufbereitet.

ENTSCHLÜSSELUNG

Aktuelle Smartphones und Tablet-PCs verfügen über eine standardmäßige Verschlüsselung, die im Zweifel den Zugriff auf verfahrensrelevante Daten verhindert. Mithilfe von Entschlüsselungstechnologien und entsprechender Rechenleistung ist in vielen Fällen eine Entschlüsselung der Daten möglich.



Sicherung und Auswertung

VIRTUALISIERTE SERVER UND DATENBESTÄNDE AUS CLOUD-SYSTEMEN

Aktuelle Serversysteme befinden sich heute in virtualisierten Umgebungen oder gleich in sogenannten Cloud-Speichern von Rechenzentren. Eine Sicherung dieser Daten erfordert Erfahrung und das Wissen über die Funktionen solcher Umgebungen.

CWIT verfügt in diesem Bereich bereits über eine Erfahrung von mehreren Jahren und hält entsprechende Werkzeuge zur Sicherung vor.

Sicherung von Netzwerken

Die Gesamtsicherung von Netzwerken, oder das Durchsuchen von Netzwerkumgebungen nach inkriminierten Daten zählt ebenso zu den Leistungen von CWIT, wie die Auswertung großer Datenmengen, die zuvor gesichert wurden.

Methoden und Werkzeuge werden in eigener Forschung und Entwicklung verfeinert und für den aktuellen Anwendungsfall vorbereitet.

Themenfelder

VERFAHRENSBEGLEITUNG/BEGLEITUNG VON HAUPTVERHANDLUNGEN IN DEN FOLGENDEN BEREICHEN:

- Allgemeine Computerkriminalität
- Wirtschaftskriminalität
- Telekommunikation und Mobilfunknetze
- Tauschbörsen, Filesharing, Streaming-Portale (Urheberrechtsverletzungen)
- Straftaten im Zusammenhang mit virtuellen Zahlungssystemen (BitCoin, LiteCoin, PPCoin)
- Betrug unter Verwendung von Kommunikationstechnik
- Computersabotage, Manipulation/ Datenveränderung
- Insolvenzdelikte
- Kinderpornografie
- Verstöße gegen UWG
- Ausspähen von Daten

INFORMATIONSBROSCHÜRE IT-FORENSIK



CWIT GmbH
Am Buschfeld 3
52399 Merzenich

0 24 21 - 9 90 08-00
kontakt@cwit.nrw
www.cwit.nrw