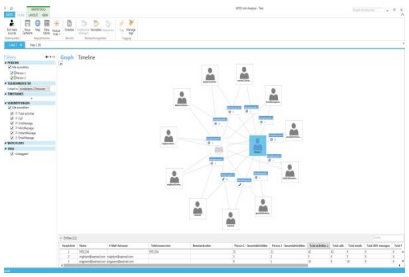
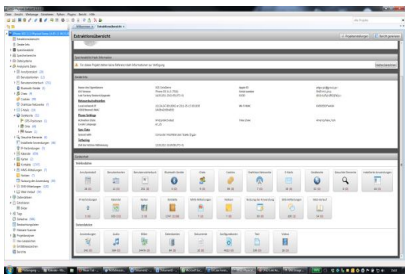
Im Einsatz – im Thema.
POLIZEI PRAXIS

FORENSIK MOBILER ENDGERÄTE





Mobile Endgeräte erfreuen sich einer zunehmenden Beliebtheit im privaten, aber auch im beruflichen Umfeld. Daraus ergibt sich allerdings auch eine strafrechtliche Bedeutung, denn häufig nutzen Straftäter mobile Endgeräte z.B. zur Verabredung einer Straftat, oder sie führen diese Geräte bei der Begehung einer Straftat mit sich. Umstände die für Ermittlungsbehörden durchaus sehr wichtig sind. Gerade Smartphones können über den Aufenthaltsort Auskunft geben oder beinhalten Informationen als SMS oder Messenger Nachrichten. Straftäter wissen häufig um die Möglichkeiten, die Smartphones bieten und nutzen sie. Aus diesem Grund gibt es auch unterschiedliche hohe Aufkommen an Daten aus mobilen Endgeräten, in den verschiedenartigen Deliktsbereichen. Planung und/oder die Verabredungen zu Straftaten werden häufig über altbekannte Kommunikationswege getätigt, wie z.B. über Kurzmitteilungen (SMS). Wichtig bei den diversen Deliktsbereichen sind auch eingehende und ausgehende Anrufe, denn diese zeigen deutlich, wer mit wem in Kontakt stand. Die Straftäter fühlen sich oftmals sicher, wenn sie derartige Daten, die sie möglicherweise einer Tat überführen könnten, löschen. Jedoch trügt dieses Sicherheitsgefühl. SIM-Karten unterschiedlichster Größen werden in den europäischen Breitengraden nach wie vor in mobilen Geräten eingesetzt, was nicht überall auf der Welt der Fall ist. Aber auch diese enthalten eine Fülle an Daten, die für Ermittler von enormer Bedeutung sein können. Für eine Auswertung ist es somit wichtig, dass Rufnummern einem Beschuldigten zugeordnet werden können.
Es gibt ausreichend dokumentierte Beispiele dafür, dass Straftäter ihre Taten mit Fotos dokumentieren, um es dem Freundeskreis oder Gleichgesinnten belegend kundzutun, oder um sich im Internet besonders hervorzutun. Andere Straftäter zeichnen Videos auf, die dann im Internet zum Kauf angeboten werden, insbesondere kommt dies häufig im Bereich der Kinderpornografie oder anderen Missbrauchsdelikten vor. Chats und Kurzmitteilungen eignen sich in einer Beweiskette ausgezeichnet, um die Planung oder Verabredung zu einer Straftat und somit einen etwaigen Vorsatz nachweisen zu können. Für die Polizei, die meist als erstes an einem Tatort eintrifft ist es daher wichtig zu wissen, worauf es bei der Sicherstellung von mobilen Endgeräten ankommt.

Tipp: Zu mobilen Endgeräten zählen bei der mobilen Forensik auch Navigationsgeräte, die eine Vielzahl an Positionsdaten aufzeichnen und mittels forensischer Software ausgelesen werden können.

Bei der Sicherstellung von mobilen Endgeräten ist eine sehr bedachte Vorgehensweise notwendig, da viele Geräte über Funktionalitäten verfügen, dass z.B. Daten vom betroffenen Gerät aus der Ferne gelöscht oder verändert werden können. Smartphones lassen sich auch aus der Ferne sperren, so dass Polizeibeamte anschließend keinen Zugriff mehr auf das Gerät haben. Bei der Sicherstellung von mobilen Geräten sollten deshalb die Beamten einige Dinge beachten: 1. Das betroffene Gerät sollte von einem Beschuldigten nicht mehr benutzt werden dürfen. 2. Bei Smartphones ist es wichtig, den Flugmodus zu aktivieren, damit keine Verbindung mehr aufgebaut werden kann. Dies sollte nur durchgeführt werden, wenn das Gerät eingeschaltet ist. Hierzu kann man einen Funktionstest durchführen, in dem man kurz den Power Knopf bedient. 3. Im Idealfall sollte ein Beschuldigter zu Sperrcodes vom Telefon sowie die SIM-PIN befragt werden. Je nachdem, wie ein Gerät genutzt wurde (privat oder geschäftlich), sind weitere Parameter von Bedeutung, die erfragt oder selbständig geprüft werden sollte: 1. Ist das Gerät in ein Mobile-Device-Management eingebunden? (Bei vielen Firmengeräten ist das der Fall.) 2. Sichtprüfung, in welchem Ladezustand sich das Gerät befindet. Es empfiehlt sich auch das Ladekabel des Gerätes sicherzustellen. 3. Wenn möglich, das Betriebssystem des Gerätes notieren. 4. Von SIM-Karten sollten die Seriennummer notiert werden, sofern einzelne SIM-Karten vorgefunden wurden.

Tipp SIM-Karten-PIN: Bisher ist es rein technisch nicht möglich, mittels forensischer Hardware die PIN einer SIM-Karte zu brechen, um an die geschützten Daten auf einer SIM-Karte zu gelangen. Darunter fallen z.B. die gespeicherten Kontakte und auch die gesendeten und empfangenen Kurzmitteilungen (SMS). Der Sicherheitsmechanismus der SIM-Karten lässt nur eine dreimalige Falscheingabe der SIM-PIN zu. Sollte dies geschehen, wird die SIM-Karte gesperrt und kann nur mit der PUK entsperrt werden. Hier kommt die Seriennummer der SIM-Karte zum Einsatz. Mit dieser ist es möglich die PUK vom Provider anzufordern.

5. Die IMEI-Nummer des Gerätes sollte notiert werden, sofern diese einsehbar auf der Gehäuserückseite ist. 6. Wurde das Gerät mit einem Computer oder Notebook synchronisiert, sind diese Geräte ebenfalls von Interesse. Auch ist darauf zu achten, ob etwaige Backups von mobilen Endgeräten vorhanden sein, die auf einem Computer, einer externen Festplatte, oder einem Memory-Stick abgelegt worden sind. 7. Nutzt der Beschuldigte Cloud Dienste, ist festzustellen welche das sind. 8. Grundsätzlich sollte der allgemeine Gerätezustand festgehalten werden. Idealerweise dokumentiert mittels eines Fotos. Für die Beantwortung dieser oben genannten Fragen, ist es also durchaus von Belang, dass eine kooperative Situation zwischen dem Beschuldigten und den Polizeibehörden bei einer Sicherstellungsmaßnahme hergestellt wird. Auch wenn die heutigen technischen Möglichkeiten sehr viel weitreichender sind, um Daten IT-forensisch auszulesen und auszuwerten, gilt dennoch: Umso mehr der Beschuldigte bereit ist, Auskunft zu geben, umso besser ist das Resultat bei der Datenextraktion und –analyse von Daten aus mobilen Endgeräten. Sind Geräte in einem Mobile-Device-Management eingebunden, bedeutet dieser Umstand meist, dass die Daten in einem „Tresor“ abgelegt und verschlossen sind. In so einem Fall ist zu überlegen, ob das Herantreten an die jeweilige Sicherheitsabteilung zielführend ist, um an Daten heranzukommen. Bei einem kritischen Ladezustand mancher mobiler Geräte kann es entscheidend sein, das Gerät aufzuladen, damit es sich nicht abschaltet. Manche abgeschalteten Geräte können nicht problemlos ausgelesen werden. Auch Informationen über das vom mobilen Endgerät genutzte Betriebssystem ist wichtig und hilfreich, um schnell die Daten auszulesen.

Tipp: Es ist möglich, ein gesperrtes iPhone zu entsperren, selbst wenn ein Beschuldigter sich nicht kooperativ zeigt und den Gerätesperrcode nicht preisgeben will. Einzig wichtig dafür ist, dass man den Laptop oder den Computer des Beschuldigten ebenfalls beschlagnahmt, mit dem sich das iPhone einmalig oder permanent

synchronisiert hat. Vorteil für jeden Ermittler ist, dass es ein Backup des Files gibt, welches den Sperrcode beinhaltet. Diese Datei, eine *.plist-Datei, kann man dann in einer speziellen Software dem iPhone während der Extraktion zuführen, um so die Sperre des Gerätes aufzuheben. Sofern das Backup - respektive die *.plistDatei - nicht ebenfalls verschlüsselt ist.

Es gibt verschiedene Wege, Daten aus mobilen Endgeräten zu extrahieren, um sie später analysieren zu können. Eine häufig genutzte technische Lösung bei der forensischen Datengewinnung ist der Zugriff über so genannte Wartungs- oder Service-Modi, den die meisten Hersteller von mobilen Geräten vorsehen, um im Service-Fall Zugriff zu erhalten. Mit forensischer Software gibt es grundsätzlich vier Möglichkeiten der Datenextraktion von mobilen Geräten: o Physical Extraction o Filesystem Extraction o Advanced Logical Extraction o Logical Extraction Welche der Extraktionsmöglichkeit möglich oder genutzt wird, ist abhängig von der technischen Machbarkeit, der technischen Ausgangssituation des Gerätes und der vorliegenden Informationen vom Beschuldigten. Letztlich wird die optimale Extraktion gewählt, mit der höchst möglichen Datenausbeute. Das Entschlüsseln von Informationen und die lesbare Darstellung von Daten aus mobilen Endgeräten ist keine leichte Aufgabe. Die hohe Anzahl von Herstellern, unterschiedlichen Systemen und Schnittstellen zur Datengewinnung ist eine enorme Herausforderung für Hersteller von forensischer Software und Hardware. Hersteller von mobilen Endgeräten benutzen unterschiedliche Betriebssysteme (z.B. iOS, BlackBerry OS, Android, Symbian), Filesysteme (z.B NTFS, HFS, Ext) und Speichermethoden, um Daten aus den Geräten verfügbar zu machen. Daraus resultieren unterschiedliche Kodierungen für die Darstellung von Inhalten und auch der Ort und die Art der Ablage von Daten. Zumeist sehr interessant und wichtig, um eine Beweiskette zu schließen ist, gelöschte Daten wiederherzustellen. Dies ist meistens möglich, wenn Speicherbereiche noch nicht mit neuen Daten überschrieben wurden. In sehr vielen Fällen ist dieser Umstand nutzbar und die Daten können problemlos rekonstruiert werden. Leider gibt es dafür keine Garantie. Auch bei SIM-Karten ist es möglich, dass gelöschte Informationen wiederhergestellt werden können. Der Fachbereich Forensik für mobile Geräte ist noch recht jung im Vergleich zur herkömmlichen Computerforensik. Er wächst jedoch und verändert sich stetig, wie auch die technologischen Entwicklungen der mobilen Endgeräte. Einige Hersteller von forensischer Software und/oder Hardware für mobile Endgeräte sind am Markt zwar vorhanden, es gelingt jedoch nur wenigen, eine universell einsetzbare und vollumfängliche Lösung anzubieten. Bilder: CONTURN, Bild SIM: Fotolia Text: Marko Rogge, Head of Research & Development Mobile-Forensic bei CONTURN Analytical Intelligence Group GmbH

Alle Artikel dieser Kategorie

Folgen Sie uns!