Mobile Geräte: Verbindungskabel zur Datenentnahme für die verschiedenen Schnittstellen.

Der Ausbau der Platine eines Mobiltelefons eines Mordopfers ermöglichte es, Daten auszuwerten.

Spuren im Gerät

Informationen und Daten in mobilen Geräten wie Handys, Smartphones und Tablets tragen immer öfter dazu bei, dass Straftaten aufgeklärt werden können.

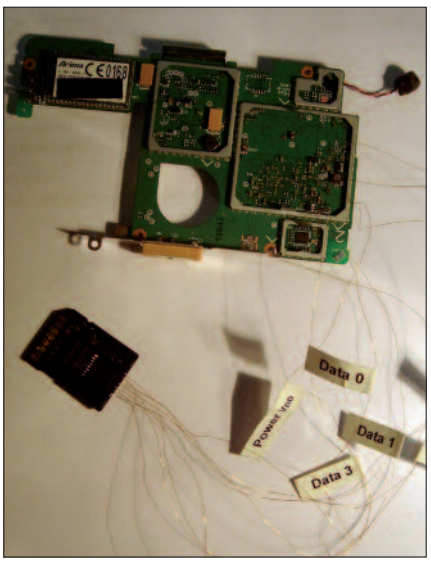
Mit Handys und Smartphones kann man nicht nur telefonieren und SMS verschicken, man kann mit ihnen auch im Internet surfen, E-Mails verschicken und navigieren. Das hinterlässt Spuren auf den Geräten – Spuren, die für die Polizei wichtig sein können, wenn solche Geräte bei den kriminellen Handlungen verwendet wurden.

Die Auswertung der Daten in Mobiltelefonen ist oft das einzige Mittel zur Erlangung von Beweisen oder als Ansatz für weitere Ermittlungen – wie bei der Klärung des „Silvestermordes“: Ein junger Wiener ermordete am Silvesterabend 2009 in Wien einen Bekannten, dem er vorgeworfen hatte, seine Verlobte mit K.-o.-Tropfen betäubt und vergewaltigt zu haben. Der Beschuldigte war jedoch freigesprochen worden. Die Auswertung von Rufdaten führte neben anderen Beweisen dazu, dass der Verdächtige den Mord gestand.

Auch bei der Klärung eines Mordanschlags im Mai 2009 in einem Sikh-Tempel in Wien spielte die Auswertung von Dutzenden Handys eine wichtige Rolle. Zum einem war auf einem Mobiltelefon ein Video gespeichert, auf dem der Anschlag gefilmt worden war, zum anderen konnten Verbindungen zwischen Personen aus dem Täterkreis nachgewiesen werden, die sonst nie zutage gekommen wären (Kontakte, Anruflisten, SMS).

Die Auswertung von mehreren Mobiltelefonen spielte bei der Klärung der Ermordung des tschetschenischen Asylwerbers Umar Israilov am 13. Jänner 2009 in Wien eine wesentliche Rolle. Zum Beispiel konnte der Nachweis erbracht werden, dass die Tatverdächtigen unmittelbar vor dem Mordanschlag miteinander telefoniert hatten.

Mit der Auswertung von Informationen in mobilen Endgeräten befassen sich die Mitarbeiter des Cyber-Crime-Competenz-Centers (C4) im Bundeskriminalamt. Es kommen Technologien zum Einsatz, die den direkten Zugriff auf den Hauptspeicher und bereits gelöschte Daten (physikalische Analyse) erlauben oder auf Inhalte von Speicherkarten, Dokumente, Programme, Digitalfotos, Videos (logische Analyse). „Wir sind vorwiegend als Assistenzdienst für die ermittelnden Kollegen tätig, eigene Amtshandlungen mit Ermittlungsmaßnahmen sind eher die Ausnahme“, sagt Chefinspektor Robert Lakits vom C4.



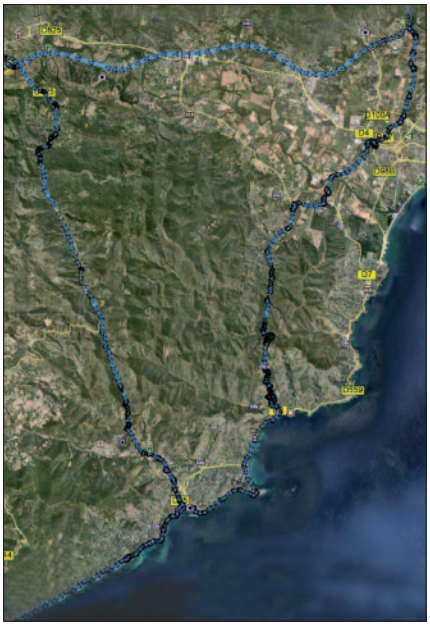
Durch Auslöten eines Chips kann ein Gerät ausgewertet werden.

Die Herausforderungen für die Ermittler in der mobilen IT-Forensik sind vielfältig. Es gibt verschiedene Hersteller von Geräten, einige Betriebssysteme und unterschiedliche Dateisysteme. Die Hersteller verwenden verschiedene Chipsätze und es gibt fast täglich neue Telefonmodelle. Die Speicher mobiler Endgeräte basieren meist auf der Flash-Technik und müssen besonders ausgewertet werden. Da jeder Hersteller seine eigenen Schnittstellen entwickelt, sind zur Datenentnahme verschiedene Verbindungskabel notwendig.

Daten werden im Gerätespeicher des Mobiltelefons gespeichert, auf Speicher- oder SIM-Karten (Subscriber Identity Module). Direkt im Gerät gespeichert sind das Betriebssystem (Firmware) und die Benutzerdaten. Die Analyse von Handydaten ist schwieriger als die forensische Auswertung der Festplatte eines Computers. Bei Handys gibt es kaum einheitliche Betriebs-

Fotos: Bundeskriminalamt, Egon Weissheimer

Mitarbeiter des Cyber-Crime-Competenz-Centers (C4) im Bundeskriminalamt: Mobile Endgeräte liefern immer öfter Hinweise zur Klärung von Verbrechen.



Auswertung eines Navigationsgeräts: Mit *Google Earth* veranschaulicht.

systeme, wie es sie bei Smartphones unter den Bezeichnungen iOS, Android oder Symbian gibt.

Speicherkarten lassen sich problemlos mit forensischen Werkzeugen untersuchen, die Ermittler auch für Festplatten nutzen. Gelöschte Daten können wiederhergestellt werden, solange sie nicht überschrieben worden sind.

Der schwierigste Teil bei der Untersuchung eines mobilen Endgerätes liegt in der Analyse der Daten, die sich im Flash-Speicher befinden. Derartige Untersuchungen sind nicht bei jedem Handy in gleicher Art und Weise möglich.

Bei einigen Modellen kann man direkt auf das Dateisystem des Mobiltelefons zugreifen, bei anderen Geräten muss zuerst mittels Spezialhardware ein Speicher-Abbild (Memory Dump) erzeugt werden, das anschließend extern zu untersuchen ist. „Wenn ein bestimmtes Gerät nicht ausgelesen und forensisch analysiert werden kann, dann kann man den Chip auslöten und mit speziellen Geräten auswerten“, erklärt Chefinspektor Lakits.

SIM-Karten. „Für die forensische Untersuchung eines Mobiltelefons ist wichtig, ob eine SIM-Karte vorhanden ist oder nicht“, sagt Lakits. Die SIM-Karte ist notwendig, damit man in einem GSM-Netz telefonieren kann. SIM-Karten werden dazu in ein Mobiltelefon oder ein mobiles Gerät (Tablet-PC oder iPad) gesteckt. Die SIM-Karte enthält ein Telefonbuch, den Speicher für SMS und eine Liste der zuletzt geführten Gespräche. Im Telefonbuch können Adressen, Geburtsdaten, Notizen, Bildverknüpfungen, Sprachbefehle und sonstiges gespeichert sein.

Gelöschte Daten auf der SIM-Karte können wiederhergestellt werden, wenn sie nicht überschrieben worden sind. Werden Kurznachrichten vom Anwender gelöscht, bleibt der Inhalt der SMS auf der SIM-Karte gespeichert und wird erst überschrieben, wenn kein weiterer freier Speicherplatz mehr zu Verfügung steht. Das Auslesen von SIM-Daten geschieht mithilfe spezieller Hardware. Für die Ermittler relevant sein können Informationen wie Sprach- oder Regionaleinstellungen, Notizen, Fotos, Videos, Exif-Daten, Anruf-Historie, Text-Nachrichten, Kontakte, E-Mails, Chats, Media-Daten, Geotags, Passwörter und mehr. Geotags können mit Hilfe von *Google Earth*/*Google Maps* veranschaulicht werden.

SIM- und Speicherkarten: Gelöschte Daten können oft rekonstruiert werden.

„Wir stellen bei Untersuchungen von mobilen Endgeräten immer wieder fest, wie schlecht sensible Daten vor unbefugtem Zugriff geschützt sind“, sagt Robert Lakits. Er empfiehlt, auch auf solchen Geräten Sicherheitssysteme einzusetzen. Dazu gehört neben Anti-Viren- und Firewall-Lösungen die Möglichkeit, gespeicherte Daten und geführte Gespräche zu verschlüsseln.

Die forensische Analyse mobiler Endgeräte besteht aus

- Identifikation (Eigenschaften des Endgerätemodells);
- Vorbereitung (Auswahl geeigneter Analyse-Werkzeuge);
- Isolierung („Abschneiden“ des Mobiltelefons vom Netz, z. B. Clone-SIM, Abschaltung);
- Datenextraktion (Auslesen der Daten vom Endgerät, logisch, Datei-System, physikalisch);
- Verifikation (Plausibilitätsprüfung, z. B. Vergleich der ausgelesenen Daten mit dem Gerät, weitere Analyse-Tools, Zeitstempel);
- Dokumentation (Lückenlose Dokumentation der Untersuchungsschritte, Untersuchungsbericht);
- Archivierung.

Siegbert Lattacher

Fotos: Bundeskriminalamt, Egon Weissheimer (2)