Mobile IT-Forensik

Dipl.-Kfm. Lutz Ressmann

- Technik und Analyse der forensischen Auswertung mobiler Endgeräte
- Leistungen des IT-Sachverständigen als Forensic Expert

www.lressmann.de / www.experts4handys.de

Urheberrechte, Bildnachweis und Impressum:
Die vorliegende Broschüre ist in all ihren Teilen urheberrechtlich geschützt. Alle Rechte sind vorbehalten, insbesondere das Recht der Übersetzung, des Vortrags, der Reproduktion, der Vervielfältigung auf fotomechanischem oder anderen Wegen und der Speicherung in elektronischen Medien. Ungeachtet der Sorgfalt, die auf die Erstellung von Text, Abbildungen und Programmen verwendet wurde, kann weder *Dipl.-Kfm. Lutz Ressmann* noch Autor, Herausgeber oder Übersetzer für mögliche Fehler und deren Folgen eine juristische Verantwortung oder irgendeine Haftung übernehmen. Die in dieser Broschüre wiedergegebenen Fachbegriffe, Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. können auch ohne besondere Kennzeichnung Marken sein und als solche den gesetzlichen Bestimmungen unterliegen.

Dipl.-Kfm. Lutz Ressmann hat sich bemüht bzw. bemüht sich laufend, alle Rechte Dritter zu berücksichtigen. Wenn solche Rechte in Einzelfällen übersehen wurden, werde ich mich unverzüglich bemühen, den Fehler zu korrigieren. Ein Großteil der Abbildungen wurde mir freundlicherweise von der Firma *CelleBrite GmbH* zur Verfügung gestellt. Das Titelfoto habe ich selbst aufgenommen, ebenso das Foto des Kabelsatzes.

Copyright © 2011 by *Dipl.-Kfm. Lutz Ressmann*. Developed and designed in Recklinghausen, Germany. All rights reserved. No other part of this brochure may be reproduced in any form or by any electronic or mechanical means including information storage and retrieval systems without permission in writing from the company.

Impressum & Kontakt
Dipl.-Kfm.
Lutz Ressmann
Sixtusstr. 56
45721 Haltern am See
Telefon: +49 (2364) 7486
Telefax: +49 (2364) 7671
E-Mail: info@crmkonzept.de
Web: www.lressmann.de

weitere Informationen:
Von der Deutschen Sachverständigen Gesellschaft mbH (DESAG) geprüfter und anerkannter EDV-Sachverständiger für Systeme und Anwendungen der Informationsverarbeitung im kaufmännisch-administrativen Bereich sowie Datenschutz (Datenschutzbeauftragter). Mitglied im Berufsfachverband für das Sachverständigen- und Gutachterwesen (BSG).

Ust-IdNr.: DE199834176
Redaktion: Lutz Ressmann
Diplom-Kaufmann, verliehen durch die UGH-Essen, Bundesrepublik Deutschland (Germany)
Design & Layout: Lutz Ressmann
Graphiken: Hauseigene Bilder; CelleBrite GmbH

Inhalt

Motivation

Mobilfunkgeräte wie Handys, Smartphones, PDAs oder Tablet-PCs (letztlich fallen auch Laptops bzw. Notebooks in diese Kategorie) sind feste Bestandteile unseres Alltags geworden. Durch den rasanten technologischen Fortschritt entwickeln sie sich immer mehr von reinen Telefonen hin zum zentralen Alltagsgegenstand. Wir organisieren unsere Termine und Kontakte mit ihnen, machen Fotos und Videos, schreiben SMS/MMS und E-Mails und können inzwischen gewaltige Datenmengen auf ihnen speichern, darunter auch sehr persönliche. Nahezu täglich kommen neue Geräte auf den Markt, der diese Technik geradezu "gierig" aufnimmt. Heute sind statistisch gesehen über 60 % der Weltbevölkerung mit Mobiltelefonen ausgestattet. Dies weckt Begehrlichkeiten aus allen Richtungen und ist auch von datenschutzrechtlicher Relevanz (nicht zuletzt Brisanz).

Mobiltelefone, speziell deren wachsende Möglichkeiten, sind eine darüber hinaus relativ junge Erscheinung, die bisher nicht umfassend von der klassischen **IT-Forensik** abgedeckt wird. Es gibt z.Z. nur wenige Sachverständige, die sich dieses Themas angenommen haben.

Besonders Smartphones sind heute beliebtes Accessoire für Kriminelle. Es ist ein ideales Werkzeug, um Fotos oder Informationen aufzunehmen, sei es für Erpressungszwecke, Stalking, Mobbing, zur Datenspionage oder einfach um mit ihren Aktivitäten anzugeben, also aus bloßem Spaß heraus.

Diese Umstände machen mobile Endgeräte aber auch für Strafermittler, Revisoren oder sonstige mit forensischen Analysen Betraute zu begehrten, potentiellen Beweisstücken. Forensiker können mit den sichergestellten (GPS) Daten mitunter aussagekräftige Persönlichkeits- und Bewegungsprofile erstellen.

Damit gelangen auch immer mehr Unternehmensdaten auf diese Gerätschaften, da mobile Endgeräte in jeder Form zur Grundausstattung eines jeden Mitarbeiters gehören und die Mitarbeiter auch von außen auf zahlreiche Geschäftsprozesse zugreifen können, die Teil interner Netzwerke sind. Die Kommunikationsgewohnheiten verlagern sich zudem zunehmend von schnurgebundenen Anwendungen hin zu drahtlosen Technologien. Zu wissen, was sich von diesen Systemen und Anwendungen auf "unorthodoxen Wegen" und ohne Einbezug und Hilfe ihres Besitzers auslesen lässt, ist sowohl für die Einschätzung des Gefahrenpotenzials im Verlustfall, als auch für Zwecke der Datenrettung und mögliche interne Ermittlungen bedeutsam. Forensische Analysen können somit auch durchaus prospektiv, ohne Vorliegen eines aktuellen Sicherheitsvorfalls zum Einsatz kommen. Sie bilden somit eine empirische, belastbare Grundlage sowohl für die Anklage, als auch für die Verteidigung.

Dabei ist nahe liegend, dass auch mobile Geräte gezielt zur Spionage, wirtschaftskriminelle Handlungen, Erpressungen und allerlei weitere Straftaten genutzt werden und sei es nur unterstützend. Mit den hierbei verfügbaren Funktionen ist es grundsätzlich möglich, kritische Informationen unauffällig aus Unternehmen, Behörden und sonstigen Organisationen zu schaffen. Damit werden gleichsam auch die Themen **IT-Sicherheit** und **Datenschutz** berührt.

Um Verdachtsfälle und Vorkommnisse dieser Art aufklären zu können, biete ich Ihnen explizit die Dienstleistung **Mobile IT-Forensik** an (als Teilgebiet der **IT-Forensik**). Wenn Sie an Details dieses neuartigen Sachgebietes interessiert sind und wissen wollen, wie Ihnen das von Nutzen sein kann, lesen Sie bitte weiter ...

Mobile IT-Forensik - Auswertung mobiler Endgeräte

Die **Computer-Forensik / IT-Forensik** und speziell auch die **Mobile IT-Forensik**, ist ein junges Fachgebiet der Beweissicherung in der EDV/IT. Es ist die Wissenschaft der Wiederherstellung und Sicherung digitaler Beweise und Beweisspuren unter forensisch einwandfreien Bedingungen mittels anerkannter Methoden. Bei der Mobilen IT-Forensik handelt es sich um die rückwirkende Aufklärung von Sicherheits-Vorfällen und möglichen Straftaten im Zusammenhang mit mobilen Endgeräten. Hierbei kommen Technologien zum Einsatz, welche häufig auch den direkten Zugriff auf den Hauptspeicher und bereits gelöschte Daten (*physikalische Analyse*) oder auf Inhalte des Dateisystems, wie Inhalte von Speicherkarten, Dokumente, Programme, Digitalfotos, Videos usw. erlauben (*logische Analyse*). Multimediale Daten, wie Inhalte von Speicherkarten, Fotos, Videos, usw. können zusätzlich mit den üblichen Werkzeugen der IT-Forensik ausgewertet werden, i.d.R. softwaregestützt. Dadurch wird ein umfassender Blick auf eine mögliche Tat frei und die Aufklärung nachhaltig unterstützt.

Abb.1: UFED Touch : Hardware Device zur mobilen Endgeräteauswertung

Meine Leistungen als IT-Sachverständiger im Bereich Mobile IT-Forensik:

- Kosten-/Nutzen-Analysen (lohnt sich der Aufwand?)
- Untersuchung aller in mobilen Endgeräten. aktuell eingesetzter Betriebssysteme und Apps (Applikationen)
- Untersuchung auf Schadprogramme / Malware
- Datenrettung (soweit möglich)
- Sichern und Identifizieren der Beweismittel
- Beweissichere Analyse und Verifikation der gesammelten Daten
- Bewertung der Ergebnisse
- Dokumentation und Präsentation der Ergebnisse
- Erstattung von Gerichts- oder Privatgutachten
- Erstellen von Sicherheitskonzepten speziell für mobile Endgeräte
- Zeugenaussage vor Gericht, falls erforderlich

Worin bestehen die besonderen Herausforderungen der Mobilen IT-Forensik?

- Es besteht die Notwendigkeit spezieller Schnittstellen, sowie Hard- und Software zur Datenextraktion
- Auf der Flash-Technologie basierende Mobiltelefon-Speicher unterscheiden sich von gewöhnlichen PC-Festplatten (HDDs)
- Es besteht eine große Anzahl von Herstellern, Betriebssystemen, Dateisystemen sowie propitärer Schnittstellen
- Sehr hohe Innovationsgeschwindigkeit auf Hardware-, Betriebssystem- und Applikationsseite
- Die Hersteller verwenden die unterschiedlichsten Chipsätze
- Fast täglich neue Telefonmodelle

Was ist bei mobilen Geräten von Interesse? Was ist möglich bei der Analyse von mobilen Geräten? Wo gibt es Einschränkungen?

Es lassen sich im Grundsatz 2 Faktoren bei der Analyse und Identifikation von mobilen Endgeräten und Mobiltelefonen heranziehen:

- die *SIM-Karte* (= Subscriber Identity Modul)
- die *IMEI* (= International Mobile Equipment Identifier)

Für die forensische Untersuchung eines Mobiltelefons ist zunächst von großem Interesse, ob eine SIM-Karte vorhanden ist oder nicht. Die SIM-Karte ist eine entfernbare Karte, die in ein Mobiltelefon oder ein mobiles Endgerät (wie z.B. ein Tablet-PC wie das iPad) gesteckt wird und speziell für den Einsatz in GSM-Netzen spezifiziert wurde (im Gegensatz zu CDMA-Netzen). Ohne SIM-Karte kann ein Mobiltelefon im GSM-Netz nicht funktionieren. Die Funktionen der SIM werden direkt vom mobilen Endgerät übernommen. Die SIM macht es möglich, alle Transaktionen auf Seiten des Providers nachvollziehbar zu machen.

Die SIM-Karte verfügt u.a. auch über internen Speicherplatz, der dann auch für forensische Untersuchungen von Relevanz ist. Die SIM ist i.d.R. durch einen 4-stelligen Code vor unerwünschtem Zugriff geschützt. Diese Sperre kann im Normalfall nur durch einen 8-stelligen PUK-Code, der vom Provider vergeben wird, umgangen werden. Mittels entsprechender Werkzeuge ist es aber ebenso möglich, diese Sperre zu umgehen.

Die IMEI erfüllt die Aufgabe, das eigentliche mobile Endgerät identifizierbar zu machen. Mitunter sind auf den sichergestellten Mobiltelefonen keine Typkennzeichen ausfindig zu machen, wohl aber kann mittels Code die IMEI identifiziert werden. Die IMEI nutzt der Forensiker wiederum, um das Mobiltelefon genau zu spezifizieren, um die Daten mit entsprechenden Werkzeugen korrekt auslesen zu können. Mobilfunkprovider prüfen darüber hinaus bei Datenübertragungen jeweils die IMEI, um gegebenenfalls ein Gerät zu blockieren (z.B. bei Diebstahl, Verlust), auch wenn eine neue SIM eingesetzt wurde.

Abhängig von der genauen Fragestellung sind bei der Analyse mobiler Endgeräte u.a. folgende Fragen und deren Antworten von Interesse:

Allgemein

- Um welches Gerät handelt es sich?
- IMEI?
- ISMI (= International Mobile Subscribe Identity) mit Zuordnung zur SIM-Karte?
- Kann das Gerät möglicherweise physikalisch ausgelesen werden (Speicher-Dump)? Können gelöschte Daten wiederhergestellt werden?
- Welches Betriebssystem wird verwendet? Android, iOS, usw.
- Welche Dateistruktur weist das Endgerät bzw. das Betriebssystem auf? Welche Arten von Dateien befinden sich auf dem Gerät?
- Welche Applikationen werden verwendet? Bestehen Anbindungen in andere Netze?

- Internet-/E-Mail-Zugang möglich und konfiguriert (WLAN, UMTS, GRPS, WAP etc.)? Wie lauten die Konfigurations-Parameter?
- Werden Kontaktdaten verwaltet? Wann ja wie? Synchronisation, wenn ja womit?
- Können auf dem Gerät zusätzliche Speicherkarten verwendet werden? Wenn Ja, ist eine Karte eingesetzt? Welchen Typs ist sie? Befinden sich Daten auf der Karte, wenn Ja, welche?
- Wurden besondere Sprach- bzw. Regionaleinstellungen vorgenommen (z.B. auch Zeitzone)
- Sind Eigentümerinformationen vorhanden (z.B. auch in Form von Aufklebern, wie Equipment-Nummer, Anlagen-Nr.)?
- Wurden Notizen aufgezeichnet? Sind evtl. gar Sprachnotizen vorhanden?
- Kalender-Informationen vorhanden? Wenn Ja, welche?
- GPS-Informationen möglich, eingestellt und vorhanden (Bewegungsdaten)?
- Ist eine Kamera vorhanden, Fotos, Videos auf dem Gerät? Exif-Daten vorhanden)
- Mikrofon verbaut, Audioaufzeichnungen vorhanden?
- Enthält das Gerät Schadprogramme?
- Sind Favoriten, Bookmarks feststellbar?
- Handelt es sich um ein Privatgerät oder ein organisations- bzw. firmeneigenes Gerät?

Bei Mobiltelefonen zusätzlich

- Welche Telefon-Nr. ist dem Gerät zugeordnet?
- Welcher Provider wird genutzt?
- Welche Nummern wurden wann angerufen, welche empfangen? Eingehende, ausgehende Anrufe, Anruflisten, usw.?
- Wurden Kurzwahlnummern hinterlegt, wenn Ja, welche?
- Wurden SMS dauerhaft gespeichert? Welche SMS oder auch MMS wurden wann empfangen oder gesendet? Wurden Templates dabei verwendet?
- Können gelöschte Dateien oder Nachrichten ausgelesen werden (Speicher-Dump)?

Zusätzlich können auch noch Abgleiche mit den bei den Mobilfunkprovidern vorliegenden Daten vorgenommen werden.

Prozess der Mobilfunkuntersuchung

Der Ablauf einer jeden Mobilfunkuntersuchung bzw. forensischen Analyse mobiler Endgeräte lässt sich allgemein wie folgt beschreiben:

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

Basis ist dabei stets die bekannte Regel der Computer-Forensik "Sichern-Analysieren-Präsentieren" (*SAR-Modell*).

Abb.2: UFED Touch™ - Kabelsatz

Eingesetzte Tools bei der Analyse mobiler Endgeräte

Zur Auswertung mobiler Endgeräte können verschiedenste Tools zum Einsatz kommen. Teilweise kann man zum Auslesen von Speicherkarten, die gleichen Tools einsetzen, die auch bei der klassischen IT-Forensik zum Einsatz kommen, z.B. *EnCase™* oder *X-Ways-Forensics™*. Speziell zur Untersuchung von Mobiltelefonen existieren softwaregestützte Werkzeuge wie z.B. die *Oxygen Forensic-Suite™* sowie frei zugängliche Werkzeuge.

Ich selbst nutzte im Regelfall einen "Koffer" mit einem speziellen Device der Firma ***Cellebrite™*** (*UFED Touch™*), zum Auslesen von Daten aus mobilen Endgeräten, die überwiegend auf der Flash-Technologie basieren. Selbstverständlich steht auch die entsprechende Software zur Analyse und Aufbereitung der ausgelesenen Daten zur Verfügung. Der Koffer bietet den zusätzlichen Vorteil, dass auch sämtliche erforderliche Kabel und sonstige nützliche Hardware sowie Accessoires enthalten sind, was sich besonders im Feldeinsatz (am Tatort) bewährt. Häufig ist schnelle Reaktion erforderlich, und die ist mit einem solchen Kit sicher leichter zu realisieren, als mit einem stationären Forensik-Lab (das natürlich weiterhin seine Berechtigung hat). Selbst Clone-SIMs können erstellt werden. Der Koffer wird in Deutschland fast ausschließlich von einigen Ermittlungsbehörden verwendet. Ich dürfte z.Z. einer der wenigen freien IT-Sachverständigen in DE sein, der Ihnen diesen Service (auch zur Erstellung von Privatgutachten oder unabhängiger Gerichtsgutachten) bieten kann.

Eigenschaften und Möglichkeiten des *UFED-Touch™* im Einzelnen

Nachfolgend gebe ich Ihnen eine kleine Einführung in die Möglichkeiten forensischer Analysen sowie die von mir diesbezüglich eingesetzten Werkzeuge. Sie können sich dann sicher besser ein Bild davon machen, was möglich ist und was nicht, und wie ich Ihnen helfen kann.

Abb.3: Extraktion mit dem UFED Touch™

Im Rahmen von Analysen der Mobilen IT-Forensik verwende ich i.d.R. das Device ***UFED-Touch™*** der Firma *Cellebrite™*. Es handelt sich dabei um eine portable, all-in-one Lösung, zur logischen und physikalischen Extraktion von Daten aus mobilen Endgeräten. Der *UFED Touch™* erlaubt einzigartige Extraktions-Methoden und Analyse-Techniken, wie Extraktion aus physikalischem Speicher (Speicher-Dump), Dateisystem-Extraktion sowie Passwort-Extraktion. Mit dem Gerät können z.Z. mehr als 2.300 mobile Endgeräte physikalisch und knapp 5.000 mobile Endgeräte logisch analysiert werden.

Die Lösung inkludiert den *UFED Physical-Analyser™*, eine leistungsfähige Software, die zahlreiche Methoden zur Entschlüsselung sowie Analyse aufweist. Daneben beinhaltet die Lösung den *UFED Phone Detective™*, zur schnellen Identifikation von Mobiltelefonen.

Der *UFED Touch™* unterstützt alle Betriebssystem-Plattformen von Mobiltelefonen und ist mit allen mobilen Einheiten kompatibel.

Die von mir eingesetzte "Ruggedized Edition" befindet sich in einem Hartschalen-Koffer und ist auf besonders hohe Belastungen ausgelegt. Damit können erste forensische Untersuchungen auch im rauen Feldeinsatz, z.B. auch am Tatort, erfolgen. Der Koffer ist zudem mit zahlreichen nützlichen Accessoires ausgestattet, wie faradeyeschem Beutel, Akku mit Laufzeit von bis zu 5 Stunden, externem Handy-Akku, Kartenlesegerät und natürlich allen benötigten Anschlusskabeln. Auch die Bluetooth-Schnittstelle kann angesprochen werden.

Der *UFED* Touch nutzt nur den internen Speicher (RAM) zur Zwischenspeicherung ausgelesener Inhalte, bevor diese auf das Zielmedium geschrieben werden. Am Ende des erfolgreichen

Extraktionsprozesses, bei Unterbrechung der Stromzufuhr oder nach einer angezeigten, nicht erfolgreichen Extraktion wird der interne Speicher immer gelöscht. Das heißt, die Extraktion erfolgt beweissicher und die Verwendung eines "Write-Blockers" ist bei diesem Verfahren nicht erforderlich!

Möglichkeiten forensischer Untersuchungen im Rahmen der Mobilen IT-Forensik

- Erzeugen physikalischer sowie logischer & Datei-System Extrakte
- Ziel-Medium können USB-Sticks oder PCs sein
- komplette Datenextraktion vorhandener, versteckter oder gelöschter Daten, einschließlich Anruf-Historie, Text-Nachrichten, Kontakte, E-Mail, Chat, Media-Daten, Geotags, Passwörtern und mehr
- Physikalische Extraktion und Passwort-Wiederherstellung von iOS 4.X Geräten wie: iPhone4™, iPAD™, iPOD Touch 3G/4G™
- Erstellen von Clone-SIMs
- Software zur Datenanalyse und Report-Generierung *UFED Physical Analyser™* sowie *UFED Phone Detective™*.
- physikalische Extraktion von GPS-fähigen Geräten
- Entschlüsselung zahlreicher GPS-Informationen
- Extraktion von Zugriffspunkten (wie WiFi, Mobilfunkzelle und Navigations-Anwendungen) von iPhone- und Android-Systemen
- Veranschaulichung von Geotags mit Hilfe Google Earth/Google Maps
- Erstellung von Berichten im Format, PDF, HTML, XMS sowie XML
- MD5 & SHA256 anerkannte Hash-Signaturen
- Reports können Firmenlogo und -Layout, enthalten
- Der Report-Generator enthält frei editierbare Felder, wie Fall-Name/Nummer, Ermittlername und mehr

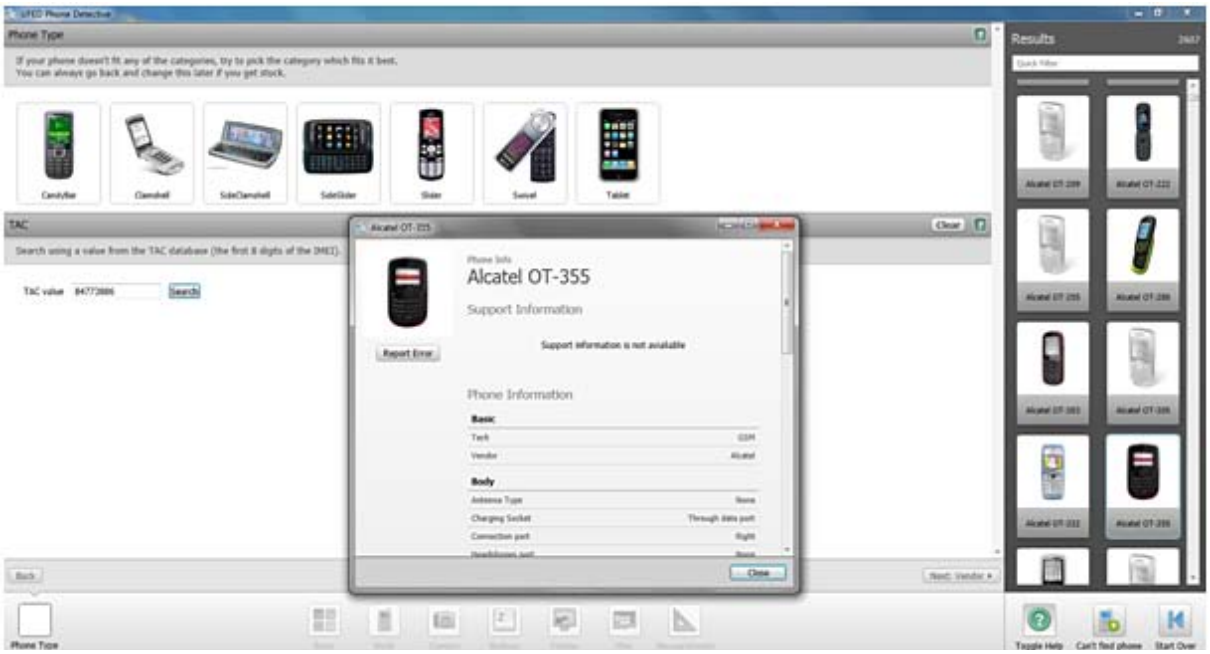

Abb4: Identifikation mit UFED Phone Detective™

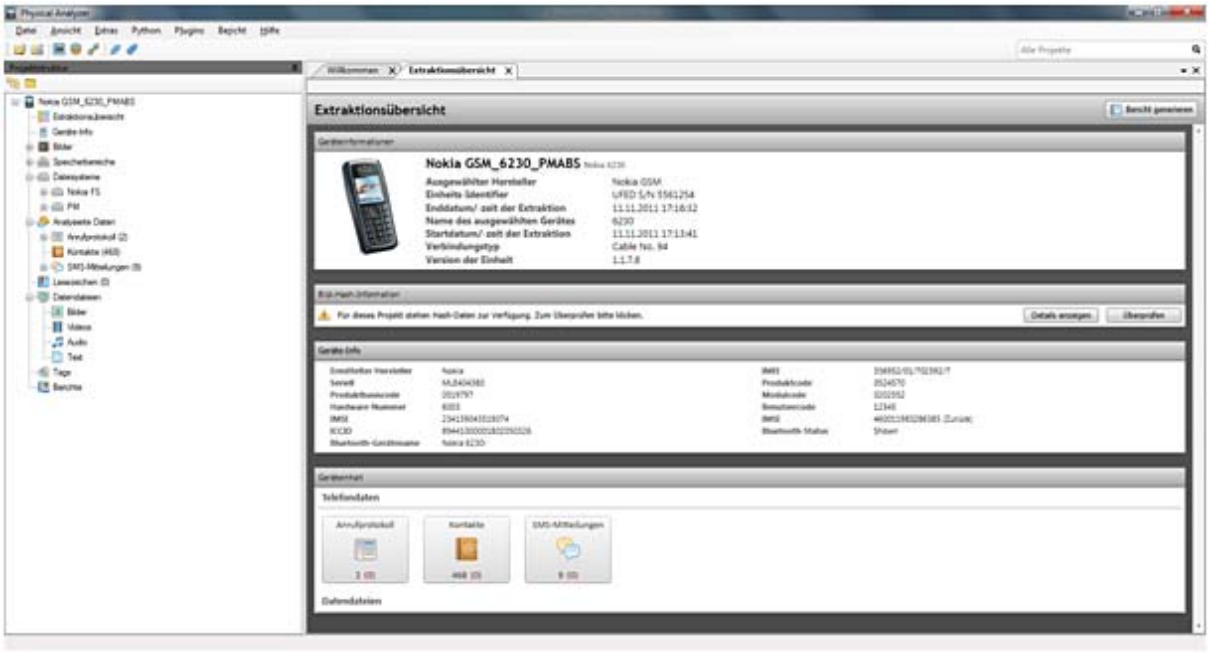

Abb.5: Analyse mit UFED Physical Analyser™

Auch mittels der Lösung *UFED Touch™* können selbstverständlich nicht alle Geräte analysiert werden. Es gibt, wie in vielen anderen Disziplinen der Analyse, auch hier gewisse Grenzen, letztlich auch hinsichtlich Aufwand und Kosten. Dazu ist der Markt auch zu schnelllebig. Aus diesem Grunde wird die Lösung in regelmäßigen Abständen aktualisiert, es werden regelmäßige Updates aufgespielt.

Sollte es mit dieser Lösung einmal nicht funktionieren, nutze ich die angesprochenen rein softwaregestützten Methoden. Aber auch dann ist es immer noch möglich, dass ein bestimmtes Gerät nicht ausgelesen und damit forensisch analysiert werden kann. Mitunter hilft dann nur noch ein Auslöten des Chips und ein Auswerten auf noch spezielleren Geräten, weshalb man sich dann genau überlegen sollte, ob man eine derartige Analyse dann noch in

Auftrag geben sollte. Der Aufwand dafür ist sehr groß und kann den Nutzen um ein Vielfaches übersteigen. Hier wird man dann ein Spezial-Labor einschalten müssen.

Sollte ich einmal ein Gerät nicht analysieren können, werde ich Ihnen dass natürlich sagen und selbstverständlich auch nicht in Rechnung stellen.

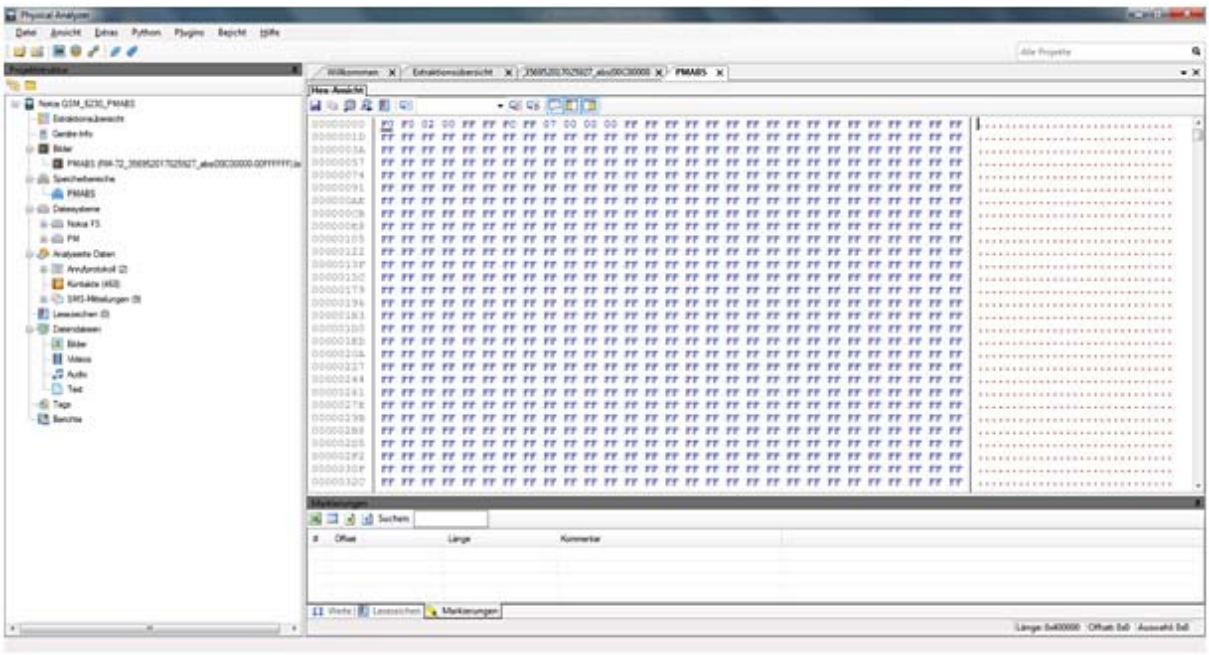

Abb.6: Analyse mit UFED Physical Analyser™ - Hex-Ansicht

Fazit:

Inzwischen ist es sehr gut möglich, Daten auf mobilen Endgeräten sicherzustellen. Eine pauschale Lösung gibt es dabei jedoch nicht. Vorrangig muss für forensische Analysen, wie üblich, gewährleistet sein, dass keine Daten auf den Geräten verändert werden.

Der fachliche und monetäre Aufwand zur forensischen Untersuchung eines mobilen Endgerätes hängt stark vom vorliegenden System und den zur Verfügung stehenden Werkzeugen ab, sowie dem Aufwand, den man bereit ist einzugehen. Gerade im innovationsfreudigen Mobilfunkmarkt muss notwendiges Wissen nicht selten durch zeitintensives und kostenträchtiges Reverse Engineering gesammelt werden. Verfügbare Werkzeuge & Methoden sind daher nicht für alle Modelle nutzbar. Es hat sich für mich jedoch gezeigt, dass man durch Verwendung kommerzieller Werkzeuge, mit einer Vielzahl von Modellen zurechtkommt, vor allem, wenn die Updates regelmäßig installiert werden.

Schwierigkeiten ergeben sich häufig auf dem Gebiet der "Wegwerfhandys" (und nicht nur dort). Überall dort, wo kaum Software und Informationen von den Herstellern zur Verfügung gestellt werden. Dieser Mangel birgt die Gefahr in sich, dass forensische Analysen im Bereich der Mobilen IT-Forensik entweder nicht ordnungsgemäß durchgeführt werden können oder grundlegende Regeln forensischer Analysen gebrochen werden, ohne, dass dies einem Er-

mittler bewusst werden muss. Dieses Risiko kann jedoch durch Verwendung leistungsfähiger Hard- und Software minimiert werden.

Gleichzeitig zeigen meine Erfahrungen aber auch, wie schlecht sensitive Daten in mobilen Endgeräten vor unbefugtem Zugriff geschützt sind. Es ist daher dringend anzuraten, auch auf solchen Geräten bei entsprechendem Schutzbedarf (vor allem bei Firmenhandys/Smartphones) zusätzliche Sicherheitssysteme einzusetzen, wie es im Falle stationärer Systeme schon lange Usus sein sollte, jedoch leider noch immer nicht durchgängig praktiziert wird. Explizit sind hier die Themen *IT-Sicherheit*, *Mobile-Security* und *Datenschutz* angesprochen.

Zielgruppen der Mobilen IT-Forensik

- *Staatsanwaltschaften / Strafermittler* (im Rahmen von Ermittlungen und Verfahren)
- *Gerichte* (im Rahmen von Verfahren)
- *Kriminalbehörden/Polizei* (im Rahmen von Ermittlungen und Verfahren)
- *Zollbehörden* (im Rahmen von Ermittlungen und Verfahren)
- *Privatermittler* (im Rahmen von Ermittlungen, Observationen und Verfahren)
- *Rechtsanwälte und -Kanzleien* (im Rahmen von Ermittlungen und Verfahren, Gegengutachten, Entlastungen von Mandanten)
- *Steuerberater* (im Rahmen von Ermittlungen und Verfahren, Gegengutachten, Entlastungen von Mandanten, vor allem im Hinblick auf Steuerfahndungen)
- *Wirtschaftsprüfer* (im Rahmen von Ermittlungen und Verfahren, Unterstützung bei Prüfungen)
- *Revisionisten/interne Ermittler* (im Rahmen von Ermittlungen und Verfahren, Unterstützung bei Prüfungen, außergerichtliche Ermittlungen, Sicherheits-Lösungen)
- *Unternehmen/Organisationen* (im Rahmen von Ermittlungen und Verfahren, Gegengutachten, außergerichtliche Ermittlungen, Sicherheits-Lösungen)
- *Privatpersonen* (im Rahmen von Ermittlungen und Verfahren, Gegengutachten, Entlastungen, Sicherheits-Lösungen)

Wie Sie sehen, sind zahlreiche Anwendungsmöglichkeiten der Mobilen IT-Forensik denkbar, so unterschiedlich sind die Situationen, bei denen sie zum Einsatz kommen kann. Angefangen bei strafrechtlichen Verfahren, bei denen es sowohl um die Belastung, aber auch die Entlastung eines Beschuldigten gehen kann, über privatrechtliche Ermittlungen z.B. im Rahmen der großen Themen "Kriminalität am Arbeitsplatz" oder "Wirtschaftskriminalität", der Klärung und Verhinderung von Sicherheitsvorfällen, Wirtschafts-/Datenspionage, Computerbetrug und steuer-/wirtschaftsprüfungsrelevanter Fragestellungen, bis hin zu zivilrechtlichen Auseinandersetzungen wie z.B. Scheidungsverfahren. Diese Aufzählung lässt sich leicht fortsetzen.

Ich unterstütze Sie gerne in allen Phasen der computerforensischen Ermittlung, hier der forensischen Analyse mobiler Endgeräte, von der Beweissicherung vor Ort, bis hin zur Analyse und Präsentation der Ergebnisse. Selbstverständlich erstatte ich auch in diesem Bereich qualifizierte Gutachten, sowohl für Privatpersonen, als auch Gerichte.

Mein Baustein **Mobile IT-Forensik** hilft Ihnen entstandene Schäden aufzuklären, Täter zu ermitteln, Taten aufzuklären und Sicherheits-Vorfällen durch gezielte Maßnahmen vorzubeugen. Zudem werden auch Entlastungen im Falle unrechtmäßiger Beschuldigungen und Ansprüche möglich. Dazu steht ein modernes und leistungsfähiges Arsenal an Werkzeugen zur Verfügung. Diese Dienstleistung können Sie nicht "an jeder Ecke" kaufen. Ich habe keine Kosten und Mühen gescheut, Ihnen diese Leistung anbieten zu können. Deshalb zögern Sie nicht, mich im Fall der Fälle anzusprechen, sinnvollerweise noch bevor ein Sicherheitsvorfall vorliegt, Ermittlungen notwendig werden oder bereits eingeleitet wurden.

Zu dieser Thematik biete ich übrigens auch einen **Workshop: "Mobile-IT-Forensik"**

Weitere und aktuelle Informationen finden Sie auf meiner Seite

www.experts4handys.de .

Kontakt

Dipl.-Kfm.
Lutz Ressmann

Büro Nord: **Sixtusstraße 56**
45721 Haltern am See

Büro Süd: **Steinheimer-Str. 34/1**
71642 Ludwigsburg

Tel.: +49 2364/7486
Fax: +49 2364/7671
E-Mail: lur@lressmann.de

Bürozeiten:

Mo-Fr. 10:00-13:00 Uhr und 14:00-17:00 Uhr

sowie nach Vereinbarung

www.experts4handys.de
www.lressmann.de

Bitte haben Sie Verständnis dafür, dass ich Informationen (Referenzen) über meine abgewickelten Projekte, Expertisen und Gutachten aus Geheimhaltungs- und Datenschutzgründen nicht für die geschäftliche und werbliche Außendarstellung verwende. Gerne erteile ich Ihnen jedoch auf Anfrage nähere Informationen!