Mobilfunkforensik

Studienbrief 1: Mobilfunkforensik

Studienbrief 2: Das Android-Betriebssystem

Studienbrief 3: Android-Forensik

Studienbrief 4: Das iOS-Betriebssystem

Studienbrief 5: iOS-Forensik

Studienbrief 6: Android-Applikationen

Autoren:
Dr.-Ing. Michael Spreitzenbarth
Dr.-Ing. Ben Stock

---

5. Auflage

Friedrich-Alexander-Universität Erlangen-Nürnberg

Department Informatik
Martensstr. 3
91058 Erlangen

5. Auflage (20. August 2019)

Didaktische und redaktionelle Bearbeitung:
Friedrich-Alexander-Universität Erlangen-Nürnberg

Um die Lesbarkeit zu vereinfachen, wird auf die zusätzliche Formulierung der weiblichen Form bei Personenbezeichnungen verzichtet. Wir weisen deshalb darauf hin, dass die Verwendung der männlichen Form explizit als geschlechtsunabhängig verstanden werden soll.

Inhaltsverzeichnis

Einleitung zu den Studienbriefen

I. Abkürzungen der Randsymbole und Farbkodierungen

Beispiel	B
Definition	D
Exkurs	E
Kontrollaufgabe	K
Quelltext	Q
Übung	Ü

II. Zu den Autoren

Dr.-Ing. Michael Spreitzenbarth hat an der Universität Mannheim Wirtschaftsinformatik mit den Schwerpunkten IT-Sicherheit und digitale Forensik studiert. Von 2010 bis 2013 arbeitete er als Doktorand an der Universität Erlangen-Nürnberg. Seine Forschungsschwerpunkte waren die forensische Analyse von Smartphones (hauptsächlich Android-basierte Geräte) und deren Erkennung sowie die automatisierte Analyse von mobiler Malware und anderen potenziell unerwünschten Anwendungen. Während dieser Zeit arbeitete er als freiberuflicher Berater in zahlreichen IT-Sicherheits-Projekten für verschiedene Kunden.

Neben dem Dr.-Ing. hält Michael Spreitzenbarth weitere Zertifizierungen im Bereich *Mobilfunkforensik* (GASF), *Mobile Application Hacking* (GMOB), *IT-Sicherheit* (CISSP, CISM, CISA, ISO/IEC 27001 Lead Auditor) und IT-Sicherheit im Bereich *Industrial Control Systems* (GRID).

Michael Spreitzenbarth war im Zeitraum von April 2013 bis Oktober 2016 für das Siemens CERT tätig und beschäftigt sich schwerpunktmäßig mit der Absicherung mobiler Endgeräte, Incident Response und der Analyse geschäftskritischer sowie potenziell bösartiger mobiler Anwendungen für iOS und Android. In den darauf folgenden Jahren beschäftigte er sich im Auftrag des Siemens CustomerCERT damit den Endkunden bei IT-Sicherheitsvorfällen zu unterstützen und die Sicherheit in den Kundenanlagen zu erhöhen. Nach einem knappen Jahr als Auditor im internen Red-Team der Siemens AG wechselte er im Oktober 2018 zur Munich Re wo er seitdem als Cyber Security Specialist im Bereich Cyber-Versicherung Risikoanalysen durchführt.

In seiner Freizeit berät er weiterhin im Bereich Mobile Security und hält Vorträge und Vorlesungen zur Sicherheit mobiler Applikationen sowie zur digitalen Forensik von Smartphones an verschiedenen Universitäten und Hochschulen in Deutschland.

Dr.-Ing. Ben Stock absolvierte sein Bachlor-Studium an der Universität Mannheim mit Fokus auf IT-Sicherheit und Forensik. Anschließend wechselte er für einen Master in IT-Security an die Technische Universität Darmstadt, wo er u. a. sein Wissen in dem Bereich Android-Sicherheit vertiefte.

Zwischen Februar 2013 und Oktober 2015 promovierte er am Lehrstuhl für IT-Sicherheits-Infrastrukturen an der Universität Erlangen-Nürnberg über client-seitige Web-Sicherheit. Zwischen Oktober 2015 und Juni 2017 war er als Postdoc am Center for IT-Security, Privacy and Accountability an der Universität des Saarlandes angestellt. Seit Juni 2017 leitet er am zukünftigen CISPA Helmholtz-Zentrum für Informationssicherheit die Arbeitsgruppe *Secure Web Applications*.

Neben seiner Forschung, die regelmäßig auf akademischen und nicht-akademischen Top-Konferenzen publiziert wird (z.B. BlackHat, OWASP AppSec, USENIX Security, ACM CCS), lehrt er an der Universität des Saarlandes Grundlagen der IT-Sicherheit, spezialisierte Web-Sicherheits-Kurse sowie das offensive *Hacking Seminar*, in denen Studierenden die Angreiferperspektive deutlich gemacht wird. Während seiner Promotion betreute er zudem das IT-Sicherheits-Praktikum sowie die Übungen zu den Veranstaltungen *Reverse Engineering* und *Angewandte IT-Sicherheit*. Dazu veranstaltet er regelmäßig Workshops, die den Teilnehmern in kurzer Zeit eine ausführliche Einführung in verschiedene Themen der offensiven IT-Sicherheit bietet.

III. Modullehrziele

Sie verstehen den Aufbau und die Funktionsweise von den mobilen Betriebssystemen Android sowie iOS. Sie kennen nach erfolgreichem Absolvieren dieses Moduls die grundlegenden Methoden zur Vorbereitung einer forensischen Analyse von Android- und iOS-Mobiltelefonen und können diese auch durchführen. Die Werkzeuge zur Analyse des Telefons sowie dessen Applikationen können sie anwenden und deren Vor- und Nachteile sind Ihnen bekannt. Ebenso wissen Sie, wo sich auf einem Android- oder iOS-basierten Endgerät interessante Daten für eine forensische Untersuchung befinden und wie Sie an diese gelangen können.

Im Rahmen dieses Moduls haben Sie kommerzielle wie auch Open-Source-Werkzeuge kennengelernt, die Ihnen bei diesen Aufgaben hilfreich sein können, aber Sie wissen auch, wie diese Tools unter der Haube funktionieren und wie Sie ähnliche Aktionen manuell durchführen können. Dies hilft Ihnen beim Erläutern und Verteidigen von komplexen Vorgängen, die Ihnen im realen Alltag die Tools abnehmen, deren Funktion aber oft hinterfragt wird.

Sie kennen nach Abschluss dieses Moduls die gängigen Tools und Techniken zur Analyse von potentieller Malware basierend auf dem Android-Betriebssystems und können einfache Applikationen für Android programmieren und analysieren und sind mit der sicherheitskritischen Betrachtung dieser Applikationen vertraut. Sie verstehen die potentiellen Gefahren, die in mobilen Applikationen stecken können nicht nur aus der Sicht eines Nutzers, sondern auch aus der Sicht eines Ermittlers der im Rahmen von forensischen Analysen auf diese Applikationen stoßen kann.

Einleitung

In den letzten Jahren stiegen die Absatzzahlen von Smartphones enorm und der Trend wandelte sich von altmodischen Handys mit nur geringer Funktionalität hin zu leistungsfähigen und funktionsreichen Smartphones. Nach letzten Hochrechnungen gibt es aktuell deutlich mehr mobile Endgeräte auf er Welt als Menschen (7.5 Milliarden Menschen gegenüber rund 8 Milliarden mobilen Endgeräten). Die Google-Smartphone-Plattform *Android* ist dabei das beliebteste Betriebssystem geworden und überholte *Symbian*- und *iOS*-basierte Telefone und Tablet-PCs.

Smartphones sind allgegenwärtig und spielen daher eine zunehmend wichtige Rolle für Beweise in forensischen Untersuchungen. Dabei spielt die Wiederherstellung von digitalen Spuren oft eine wesentliche Rolle bei der Prüfung und Klärung der Fakten im Rahmen von Straftaten. Obwohl es bereits einige Werkzeuge und Vorgehensbeschreibungen in diesem Bereich gibt, besteht weiterhin eine starke Nachfrage nach Methoden und Werkzeugen für die forensische Extraktion und Analyse von Daten, die auf Smartphones gespeichert sind. Dieser Bedarf wird durch das schnelle Wachstum und die steigende Diversifikation im Bereich des Mobilfunktmarktes geweckt.

Durch die hohe Verbreitungsrate und steigende Popularität werden Smartphones nicht nur bei Straftaten verwendet, sie geraten auch als Angriffsziel zunehmend in den Fokus von Kriminellen. Für das bessere Verständnis der damit verbundenen Bedrohungen für Endnutzer, ist es wichtig, bösartige Software zu analysieren und zu identifizieren. Die exponentiell wachsenden Zahlen der Android-Malware in den vergangenen Jahren verlangen eine Automatisierung des Analyseprozess, um dem schnell wachsenden Datenaufkommen gerecht zu werden.

In diesem Modul werden die Spezifikationen und Besonderheiten von Android- sowie iOS-Smartphones beschrieben. Des Weiteren wird auf Möglichkeiten zur forensischen Analyse von Smartphones eingegangen und es wird gezeigt, wie man Bewegungsprofile von Smartphone-Nutzern generieren und anhand dieser Profile den Aufenthaltsort eines Smartphones über einen gewissen Zeitraum in der Vergangenheit nachweisen kann. Dieser Schritt könnte vor allem bei der Aufklärung von Straftaten, bei denen es um eine spezifische Zeit-Ort-Kombination geht, eine wichtige Rolle spielen. Ein Beispiel für eine solche Fragestellung ist: „Befand sich der Verdächtige zum Zeitpunkt des Einbruchs in der Nähe der ausgeraubten Villa?“ Im Zusammenhang mit der Aufklärung von Straftaten kommt es auch immer wieder zu dem Punkt, an dem ein Ermittler sich die Frage stellen muss: „Wurde die Aktion auf dem Smartphone durch den Eigentümer ausgeführt, oder war das Mobiltelefon manipuliert?“ Um bei der Beantwortung dieser Frage Hilfestellung zu geben, wird im dritten Studienbrief der Fokus auf die Analyse von mobilem Schadcode gelegt.

Rückmeldungen

Trotz zahlreicher Verbesserungsvorschläge verschiedener Personen (vor Allem auch der Studierenden aus dem ersten Durchlauf) enthält dieser Text sicherlich noch Fehler, seien sie inhaltlich, konzeptionell, sprachlich oder stilistisch. Die Herausgeber freuen sich deshalb über jede konstruktive Rückmeldung, die wir in zukünftigen Versionen unseres Textes gerne berücksichtigen.

Dr.-Ing. Michael Spreitzenbarth
Dr.-Ing. Ben Stock

Studienbrief 1 Mobilfunkforensik

Zu Beginn dieses Moduls wollen wir ein generelles Verständnis für forensisches Vorgehen und die vorhandenen Daten erlangen. In den folgenden Abschnitten werden wir daher auf das wichtigste Modell – den sogenannten *Investigative Process* nach Casey – und die unterschiedlichen Vorgehensweisen, um an die Daten zu gelangen, eingehen.

Abschnitt 1.1.1 beschreibt einen kompletten Ablauf einer möglichen Untersuchung. Hierbei starten wir mit dem eigentlichen Vorfall, gehen weiter über die Sicherung und Auswertung der vorhandenen Daten und enden bei der Präsentation vor Gericht. Im Anschluss versuchen wir zu verdeutlichen, warum die herkömmliche und ausgereifte Forensik nicht „1:1“ auf die Welt der Smartphones übertragen werden kann, weshalb sie aber nichtsdestotrotz genauso wichtig ist. Im Weiteren werden wir auch Besonderheiten bei der Analyse von Smartphones aufzeigen, wie wir sie aus der PC-Welt nicht kennen, die bei der Aufklärung von Straftaten aber eine wichtige Rolle spielen können.

1.1 Einführung in die Mobilfunkforensik

Sobald es um Ermittlungen zum Zwecke der Strafverfolgung oder zur Aufklärung von Vorfällen geht, ist es wichtig, bestimmte zuvor festgelegte Prozesse zu beachten, um im Nachhinein sauber dokumentierte und nachvollziehbare Ergebnisse zu liefern. Dies ist auch in der Mobilfunkforensik nicht anders. Im Folgenden werden wir auf einen solchen Prozess eingehen und aufzeigen, wo es Besonderheiten hierbei gibt, wenn der zu analysierende Gegenstand ein Smartphone ist. In den Studienbriefen 3 und 5 werden wir hierauf aufbauen und diskutieren, welche Wege es für einen Ermittler gibt, die beschriebenen Sicherheitsmechanismen der Android- und iOS-Platform zu umgehen, um ein möglichst ungetrübtes Bild des Smartphones zu erhalten.

1.1.1 Der klassische Investigative Process

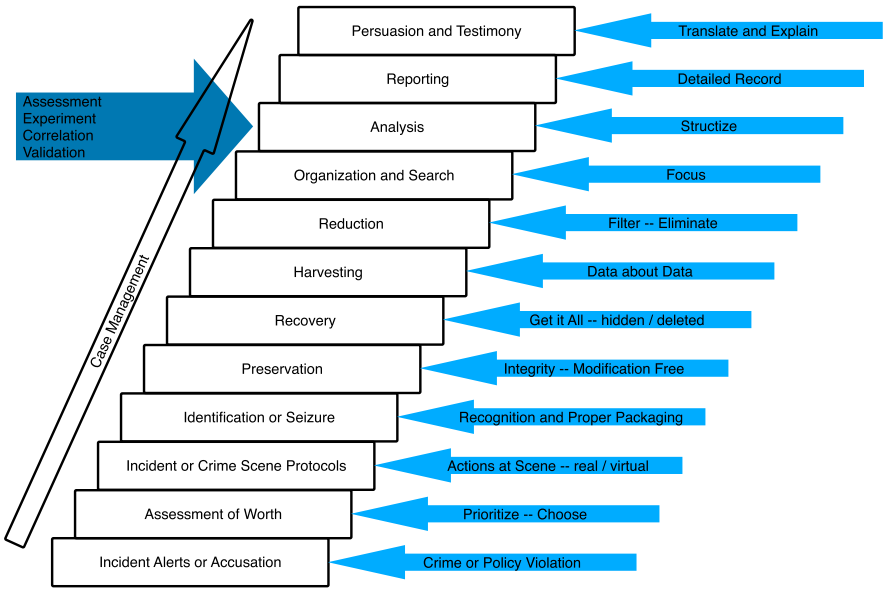

Abb. 1.1: Phasen des *investigative Process* von Casey [Casey, 2011].

Der *investigative Process* von Casey [Casey, 2011] stellt ein allgemeines Vorgehensmodell für digitale Untersuchungen dar, das auch klassische Polizeiaufgaben

einschließt, nicht nur die Aufgaben eines forensischen Experten. Der investigative Prozess ist heute in vielen Ländern ein De-facto-Standard.

Der Prozess besteht aus insgesamt 12 Phasen, die als Treppe visualisiert werden, beginnend mit der Alarmierung auf der untersten Stufe, bis hin zur Präsentation vor Gericht am Ende der Treppe (siehe Abbildung 1.1). Im Folgenden betrachten wir alle Phasen im Einzelnen und beziehen uns dabei auf die Übersetzung der einzelnen Begriffe nach Dornseif [Dornseif, 2004].

Anschuldigung (Incident Alerts or Accusation) Die Anschuldigung ist das Startsignal für den gesamten Prozess. In dieser Phase werden zunächst die Quellen eingeschätzt und erste Erkundigungen eingeholt.

Güterabwägung (Assessment of Worth) Im Rahmen der Güterabwägung wird das Interesse an der Verfolgung den Kosten, die bei der Verfolgung entstehen würden, gegenüber gestellt. Für Unternehmen fällt eine solche Abwägung (zumindest bei kleineren Vorfällen) meist gegen eine Verfolgung aus. Für eine Verfolgung sprechen neben der Chance auf Schadensersatz auch die Verbesserung der eigenen Sicherheit sowie eine gewisse Abschreckungswirkung. Gegen eine Verfolgung hingegen sprechen der Ressourcenverbrauch, unter Umständen die downtime, in der die zu untersuchenden Systeme nicht produktiv eingesetzt werden können, und meist eine negative Öffentlichkeitswirkung.

Tatortsicherung (Incident or Crime Scene Protocols) In der klassischen Kriminalistik wird immer gefordert, den Tatort weiträumig abzusperren. Für verschiedene Arten digitaler Spuren muss im Einzelfall überprüft werden, wie das Vorgehen des Einfrierens genau aussieht. Insgesamt gilt es jeweils, die Gefahren der Verfälschung von Spuren so weit wie möglich einzudämmen.

Beschlagnahme (Identification or Seizure) Bei einer traditionellen Beschlagnahme werden alle Gegenstände mitgenommen, die als Beweismittel dienen könnten. Wichtig ist hierbei, nichts an den Beweismitteln zu verändern. Aber auch die Umgebung der gesicherten Beweismittel kann von großer Relevanz sein. Mit der Beschlagnahme beginnt die *Chain of Custody*. Eine gute Lektüre zur Durchführung von Beschlagnahmen ist die vom US-Department of Justice/National Institute of Justice herausgegebene Broschüre Electronic Crime Scene Investigation: A Guide to First Responders [Department of Justice and National Institute of Justice, 2001]. Sie gibt ausführliche und genaue Hinweise auch für nicht-technisches Personal. Eine weitere gute Quelle ist das Dokument *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* vom United States Department of Justice [Department of Justice, 2002].

Sicherung (Preservation) Bei der Sicherung der Beweismittel gilt es sicherzustellen, dass diese unverändert bleiben. Daher werden alle Beweismittel dokumentiert, fotografiert, versiegelt und anschließend weggeschlossen. Bei digitalen Spuren bedeutet das in der Regel, zuerst Kopien der Beweismittel zu erstellen und weitere Untersuchungen nur auf den Kopien durchzuführen. Zum Nachweis der Echtheit von Beweismittelkopien kommen kryptographische Hashfunktionen zum Einsatz. Außerdem ist es wichtig, ausschließlich vertrauenswürdige Software zu gebrauchen. Bei der Sicherungsphase beginnt die Arbeit von Informatik-Spezialisten.

Bergung (Recovery) Casey [Casey, 2011] beschreibt die Bergung als *throwing out a large net*. Insbesondere umfasst diese Phase die Bergung von Daten, die gelöscht, versteckt, getarnt oder anderweitig unzugänglich gemacht wurden. Hier empfiehlt es sich, Synergien mit anderen Beweismitteln zu

nutzen. Beispielsweise ist es sinnvoll zu prüfen, ob ein Zettel mit Passworten am Tatort gefunden wurde, wenn verschlüsselte Daten gelesen werden müssen.

Auswertung (Harvesting) Bei der Auswertung ist vor allem eine gute Organisation der üblicherweise großen Datenmenge erforderlich. Hierzu sollte zunächst eine Untersuchung von Metadaten anstatt der eigentlichen Daten vorgenommen werden. Beispielsweise können Daten nach Dateityp oder Zugriffszeiten gruppiert werden. Dies führt direkt zur nächsten Phase, der Reduktion.

Reduktion (Reduction) Aufgabe der Reduktion ist es, irrelevante Daten zu eliminieren. Hierzu kann auch weiterhin auf Metadaten gearbeitet werden. Zum Beispiel können die Daten aufgrund des Datentyps reduziert werden. Ein Szenario hierfür wäre bei entsprechender Anschuldigung die Reduktion aller Dateien auf Bilddateien. Das Ergebnis dieser Phase ist nach Casey *the smallest set of digital information that has the highest potential of containing data of probative value*, also die kleinste Menge digitaler Information mit der größten Wahrscheinlichkeit, beweiskräftige Daten zu enthalten. Hilfreich sind hier Hash-Datenbanken von bekannten Dateien, wie zum Beispiel*The NIST National Software Reference Library* [National Institute of Standards and Technology, 2011], um bereits bekannte Dateien ausschließen zu können. Weitere Teilaspekte der Reduktion sind die Strukturierung der Daten sowie die Durchsuchbarmachung, um die Daten nach der Reduktion zu organisieren. Hierzu werden häufig Indizes und Übersichten erstellt. Dies vereinfacht die Referenzierung der Daten in den nachfolgenden Schritten.

Organisation (Organization and Search) Weitere Teilaspekte sind die Strukturierung der Daten sowie die Durchsuchbarmachung, um die Daten nach der Reduktion zu organisieren. Hierzu werden häufig Indizes und Übersichten erstellt. Dies vereinfacht die Referenzierung der Daten in den nachfolgenden Schritten.

Analyse (Analysis) stichwort*Analysis Diese Phase beinhaltet die Detailanalyse unter Beachtung der Dateiinhalte. Unter anderem müssen Verbindungen zwischen Daten und Personen hergestellt werden, um Verantwortliche zu ermitteln. Weiterhin erfolgt die Bewertung von Inhalt und Kontext nach Bedeutung, Motivation und Gelegenheit. Experimente sind in dieser Phase hilfreich, um undokumentiertes Verhalten zu ermitteln und neue Methoden zu entwickeln. Alle Ergebnisse müssen durch wissenschaftliche Methodik überprüft werden und überprüfbar sein.

Bericht (Reporting) Aufgabe des Berichtes ist es, nicht ausschließlich Ergebnisse zu präsentieren, sondern auch darzulegen, wie diese erlangt wurden. Hierzu sollten immer auch die befolgten Regeln und Standards im Bericht dokumentiert werden. Alle gezogenen Schlüsse müssen begründet und auch alternative Erklärungsmodelle erörtert werden.

Bezeugen (Persuasion and Testimony) Schlussendlich kommt es zur Bezeugung als Sachverständiger vor Gericht. Wichtigster Punkt ist die Glaubwürdigkeit des Bezeugenden. Problematisch können hierbei ein technikfeindliches Publikum oder problematische, beispielsweise vom Verteidiger angeführte, Analogien sein.

1.1.2 Der Investigative Process für Smartphones

Der Investigative Process, wie im vorherigen Abschnitt beschrieben, wurde so generisch wie möglich gehalten. Wenn im Rahmen einer forensischen Untersuchung Computer zur Auswertung stehen, sind alle Schritte dieses Prozesses gut

von Casey [Casey, 2011] beschrieben und inzwischen auch standardisiert. Geht es jedoch um Smartphones, so ist es deutlich schwerer, die einzelnen Schritte an diesen Leitfaden anzupassen. Ein Ermittler benötigt für fast jede Smartphone-Familie seine eigenen Tools und Leitfäden. Ein Android-Telefon aus dem Hause Samsung muss anders analysiert und ausgewertet werden als eines aus dem Hause HTC und komplett unterschiedlich zu einem Apple iPhone. Dies betrifft im Besonderen die Punkte Datensicherung und Analyse. Sehr oft unterscheiden sich die entsprechenden Vorgehensweisen auch von der herkömmlichen Forensik (z. B. das Sichern des internen Speichers eines Telefons ist im Ablauf sehr unterschiedlich zur Sicherung einer Festplatte aus einem PC).

Es existieren viele verschiedene Leitfäden für die forensische Analyse von Mobiltelefonen, die dem angehenden Analysten bei der täglichen Arbeit hilfreich sein können. Einer der bekanntesten und ausführlichsten Leitfäden stammt vom National Institute of Standards and Technology [National Institute of Standards and Technology, 2007]. Dieser wurde in der aktuellen Fassung, jedoch vor der Zeit der Smartphones (Android und iOS) verfasst, und kann daher nur noch für generelle Verhaltensanweisungen herangezogen werden. Aktuell wird an einer neuen Version dieses Leitfadens gearbeitet, der auch die neueren Generationen der Mobiltelefone unterstützt [National Institute of Standards and Technology, 2013].

In Bezug auf die Platform iOS gibt es ein Werk von Zdziarski, das sich in den letzten Jahren als Standardwerk etabliert hat: „iPhone Forensics: Recovering Evidence, Personal Data, and Corporate Assets“ [Zdziarski, 2008]. Zdziarski ist einer der bekanntesten und angesehensten Forscher auf dem Gebiet der forensischen Analyse von iOS-Geräten. Da sich Android und iOS in ihrem Aufbau und der Funktionalität stark unterscheiden, kann dieses Werk leider nicht so einfach auf die Android-Platform übertragen werden.

Ein erster Versuch, einen ähnlichen Leitfaden für Android zu erstellen, wurde von Andrew Hoog im Jahre 2011 unternommen [Hoog, 2011]. Leider wurde dieses Buch für die Android-Version 1.4 geschrieben und viele der darin beschriebenen Techniken sind inzwischen nicht mehr anwendbar. So hat sich zum Beispiel die Art und Weise, wie man den RAM des Telefons untersuchen kann, in Android 2.3 essenziell geändert. Dazu kommt noch die Tatsache, dass sich Hoog stark auf die Analyse spezifischer Android-Apps fokussiert hat und sich deren Datenbanken mit fast jedem Release ändern.

In den folgenden Abschnitten wird versucht, eine generischere Herangehensweise mit alternativen Techniken und deren Vor- und Nachteilen darzustellen. Beginnen wollen wir hierbei mit zwei wichtigen Fragen, die in der Vergangenheit immer wieder gestellt wurden: *Warum ist Mobilfunkforensik wichtig?* und *Was ist das Besondere an Mobilfunkforensik?* Im Anschluss daran werden wir beschreiben, an welchen Stellen der Investigative Process von Casey [Casey, 2011] angepasst werden muss oder wo ein Analyst ein anderes Vorgehen an den Tag legen muss. Hierbei sind die Schritte *„Beschlagnahmung und Aufbewahrung“* sowie *„Wiederherstellung und Auswertung von Daten“* diejenigen mit den gravierendsten Änderungen. Zudem werden wir auch auf die Rolle des Mobilfunk-Providers eingehen, der bei forensischen Analysen und der Aufklärung von Straftaten eine wichtige Rolle spielen kann.

Warum ist Mobilfunkforensik wichtig?

In den vergangenen Jahren sind Smartphones ein beliebtes Kommunikationsmittel geworden. Gemäß Greif [Greif, 2010] ist der dazugehörige Kommunikationsmarkt

einer der weltweit am schnellsten wachsenden Märkte. Unter allen Mobilfunk-Standards ist GSM (Global System for Mobile Communications) mit 75 % der am meisten genutzte Standard. GSM wird in 200 Ländern genutzt und hat mehr als 1,2 Milliarden Nutzer in mehr als 630 mobilen Netzwerken (eine detaillierte Übersicht findet sich bei Schiller [Schiller, 2003]).

Da Smartphones eine zunehmend größere Vielfalt durch erweiterte Funktionen bieten, steigt auch die Menge an sensiblen Daten, die auf einem Gerät generiert und gespeichert werden. Durch die weit verbreitete Nutzung von Smartphones, steigt ebenfalls die Anzahl an Geräten, die im Rahmen forensischer Analysen von privaten Organisationen oder Strafverfolgungsorganen untersucht werden. Nach einem internen Report [German Federal Criminal Police Office (BKA), 2012], untersuchte die TESIT (eine Abteilung des Deutschen Bundeskriminalamts) allein im Jahr 2011 mehr als 1.200 Mobiltelefone[1].

Solche Organisationen müssen in der Lage sein, Daten, die auf Smartphones gespeichert sind, auszulesen und zu analysieren. Deshalb herrscht ein großer Bedarf an Methoden und Tools, die es ermöglichen, die zuvor erwähnten Aufgaben auf eine forensisch korrekte Art durchzuführen. Darüber hinaus macht es die schnelle Weiterentwicklung von Smartphone-Technologien nötig, Methoden häufig zu überprüfen und an neue Gegebenheiten anzupassen. Des Weiteren müssen kontinuierlich neue Methoden und Tools entwickelt werden, die im Bereich der forensischen Analyse von Smartphones Verwendung finden.

Was ist das Besondere an Mobilfunkforensik?

Während sich die forensische Analyse von Standard-Computer-Hardware – wie beispielsweise Festplatten – in einen stabilen Wissenschaftszweig mit einer Vielzahl an Referenzarbeiten entwickelt hat (siehe zum Beispiel Carrier [Carrier, 2009]), gibt es im Bereich der Analyse von Nicht-Standard-Hardware oder flüchtigen Beweisen noch immer eine große Diskussion über Analysetechniken. Obwohl Smartphones eine zunehmend größere Rolle bei digitalen Untersuchungen spielen, werden sie noch immer nicht als Standard aufgrund ihrer Heterogenität angesehen. Im Rahmen aller Untersuchungen ist es nötig, grundlegende forensische Prinzipien zu berücksichtigen. Die zwei Hauptprinzipien sind folgende:

1. Es muss größte Sorgfalt darauf verwendet werden, dass der Beweis so wenig wie möglich manipuliert oder verändert wird.
2. Die Vorgehensweise einer digitalen Untersuchung muss verständlich und überprüfbar sein. Bestenfalls sind die Ergebnisse einer Untersuchung durch unabhängige Analysten reproduzierbar.

Besonders das erste Prinzip stellt, wenn es um Smartphones geht, eine Herausforderung dar; die meisten Smartphones verwenden spezifische Betriebssysteme und Hardware-Schutzmechanismen, um uneingeschränkten Zugang zu Daten auf dem System zu verhindern.

Die Erhaltung von Daten auf Festplatten ist in den meisten Fällen ein einfacher und bekannter Prozess. Der Ermittler entfernt die Festplatte vom Computer oder Notebook, verbindet es mittels eines „Write Blockers“ (bspw. Tableau's TK35 [Guidance Software Inc.]) mit seinem Arbeitsplatzrechner und beginnt die Festplatte mit bekannten und zertifizierten Softwarelösungen zu analysieren. Vergleicht man dieses Vorgehen mit der Smartphone-Welt, wird klar, dass es hierfür kein solches Standardvorgehen gibt. Fast jedes Smartphone hat seine eigene Art, Daten zu

[1] Leider gab es seid dieser Zeit keine offiziellen Zahlen mehr.

speichern. Daher braucht auch der Ermittler für jedes Smartphone eine eigene Vorgehensweise, um ein Speicherabbild zu erstellen (einige Möglichkeiten sind im Abschnitt 1.1.2 beschrieben). Während es dadurch bedeutend schwieriger ist, Daten von einem Smartphone zu bekommen, bekommt man allerdings eine größere Vielfalt an Daten geliefert. Smartphones speichern, neben allgemeinen Daten (z. B. Bilder und Dokumente) auch Daten, wie bspw. GPS-Koordinaten oder die Position der Funkzelle, mit der das Smartphone verbunden war, bevor es ausgeschaltet wurde.

Bedenkt man die daraus resultierenden Möglichkeiten, stellt man fest, dass der zusätzliche Ermittlungsaufwand durchaus gerechtfertigt ist.

Die Rolle des Mobilfunk-Providers

Nach dem Terroranschlag 2004 in Madrid hat die Europäische Union eine Direktive [European Parliament and the Council of the European Union, 2006] ausgegeben, um die Regelungen in den EU-Mitgliedsstaaten für Vorratsdatenspeicherung, die von öffentlich verfügbaren elektronischen Kommunikationsservices generiert wurden, zu harmonisieren. Die Direktive soll es Strafverfolgungsbehörden ermöglichen, auf Traffic-Daten zuzugreifen, die zu einem Verdächtigen gehören (z. B. mit wem der Verdächtige kommuniziert hat und welchen digitalen Service er verwendet hat). Gemäß dieser Direktive müssen die folgenden Daten für einen Zeitraum von 6 Monaten bis zu 2 Jahren gespeichert werden:

- Kommunikationsquelle (subscriber ID oder Telefonnummer);
- Kommunikationsziel (subscriber ID oder Telefonnummer);
- Datum, Zeit und Dauer der Kommunikation;
- Art der Kommunikation (SMS, MMS oder Telefonanruf);
- Kommunikationsgerät (z. B. die IMEI des Geräts);
- Ort des Geräts für die mobile Kommunikation (z. B. GPS-Daten oder zumindest der Ort der Mobilfunkzelle, der genutzt wurde);

Gemäß der EU-Direktive müssen diese Daten in speziellen Fällen für „kompetente“ nationale Behörden zur „Untersuchung, Aufklärung und Verfolgung ernsthafter Verbrechen – wie im Bundesgesetz des jeweiligen Mitgliedstaates definiert“, zugänglich sein. Auch wenn diese Direktive in jedem Mitgliedsland eingeführt werden muss, wird sie doch häufig kontrovers diskutiert und wurde nach aktuellem Stand nicht überall eingeführt (bspw. in Deutschland).

Daten, die von einem Mobilfunk-Provider gespeichert werden, könnten sehr wichtig für Ermittler sein, sollten diese weitere Informationen über Kontakte und den Aufenthaltsort eines Verdächtigen benötigen. Wie im Abschnitt 3.4 sowie im Rahmen der Bewertung gezeigt werden, sind diese Daten allerdings aber auch höchst kritisch, wenn es um persönlichen Datenschutz unbescholtener Nutzer geht. Mit Hilfe dieser Daten ist es möglich, Smartphone-Nutzer und die gesamte mobile Kommunikation 24/7 innerhalb eines Radius von einigen Metern zu verfolgen.

Stellt man sich dieses Szenario vor, wird schnell deutlich, dass diese Daten durch Gesetze und Regelungen geschützt werden müssen.

K

Kontrollaufgabe 1.1: Vorratsdatenspeicherung

Nehmen wir an, Herr Maier telefoniert an einem Freitagabend gegen 21 Uhr von seinem Smartphone aus mit Herrn Müller (Anruf erfolgte unter dessen Mobilfunknummer) und sendet ihm im Anschluss noch wichtige Daten per SMS.

Welche Informationen werden bei dieser Kommunikation im Rahmen der Vorratsdatenspeicherung aufgezeichnet?

Beschlagnahmung und Aufbewahrung

E

Exkurs 1.1: Fragen die vor einer Durchsuchung oder Beschlagnahme positiv beantwortet sein sollten:

Gibt es einen offiziellen Durchsuchungsbefehl oder hat der Beschuldigte der Durchsuchung zugestimmt?

Sind die Geräte die beschlagnahmt werden sollen im Durchsuchungsbefehl aufgeführt?

Wie sind die Besitzumstände des mobilen Endgerätes? – speziell im Firmenumfeld kann es einen Unterschied machen ob das Gerät dem Angestellten oder der Firma gehört.

Gibt es eine Firmenrichtlinie die eine Auswertung des mobilen Endgerätes erlaubt und gibt es eine Richtlinie zur Privatnutzung dieser Geräte?

Gemäß Casey [Casey, 2011] ist dieser Schritt der Beginn einer digitalen forensischen Analyse. In diesem Schritt werden Kopien des Originalbeweises erstellt. Diese Kopien werden nachfolgend für die Analyse genutzt, da das Originalmaterial während des Analyseprozesses keinesfalls verändert werden sollte. Um gemäß den Regeln einer forensischen Untersuchung zu handeln, muss der Originalbeweis, nachdem eine Kopie erstellt wurde, katalogisiert und angemessen an einem überwachten Ort aufbewahrt werden. Wie bereits im vorherigen Abschnitt erwähnt wurde, ist nicht eindeutig klar, wie ein Speicherabbild von einem modernen Smartphone erstellt werden kann. Im folgenden Abschnitt werden die verschiedenen Techniken und Herangehensweisen, um eine Arbeitskopiezu erstellen, diskutiert. Wichtig ist dabei zu beachten, dass bei iOS viele dieser Methoden nicht funktionieren, da die Speicherinhalte verschlüsselt sind und ein Entschlüsseln nur auf dem Gerät selbst funktioniert (Aufgrund der Verwendung von Crypto-Chips und TPM).

Verwendung von softwarebasierten Agenten

Im Rahmen der Mobilfunkforensik beschreiben softwarebasierte Agenten kleine Programme, die auf einem Mobiltelefon installiert oder dorthin kopiert werden, um lokal Daten zu sammeln und zu analysieren, oder die Daten unter Nutzung des Telefon-Interfaces für eine spätere Untersuchung zu exportieren. Zwei Beispiele softwarebasierter forensischer Agenten sind *Open Source Android Forensic*

Agent [Hoog, 2010] und *Panoptes* [Spreitzenbarth, 2010]. Beide Agenten werden auf dem Zielgerät installiert. Nach der Installation können sie direkt auf dem Gerät ausgeführt werden und liefern dem Ermittler in einer CSV-Datei vom Smartphone exportierte Daten bereits in einem editierten Format. Durch die Nutzung sogenannter *Content Provider* und den dazugehörigen Rechten, wird die Android-Sandbox ausgehebelt und direkt Zugriff auf Datenbanken anderer installierten Applikationen ist möglich. Aufgrund dieser Vorgehensweise können gespeicherte und geschützte Daten von installierten Applikationen ausgelesen werden.

Die Nutzung von softwarebasierten Agenten bringt einige Vorteile mit sich: So wird zum Beispiel nur wenig technisches Wissen benötigt, das Gerät muss nicht *gerootet* werden und es wird keine spezielle Hardware benötigt, um die Daten vom Gerät auszulesen. Mit Hilfe eines solchen Agenten ist es ebenfalls möglich, gelöschte Daten wiederherzustellen, solange diese noch in den Datenbankdateien sichtbar sind. Softwarebasierte Agenten haben jedoch auch einen gravierenden Nachteil: Durch das Kopieren oder Installieren des Agenten auf dem Smartphone werden im größeren Stil Daten verändert – dies ist gegen die forensischen Prinzipien.

Manuelles Auslöten des Flash-Speichers

Im Rahmen der forensischen Analyse ist es ein verbreitetes Vorgehen, den benötigen Speicherchip von der Platine des Geräts zu entfernen (eine detaillierte Erklärung findet sich bei Casey [Casey, 2009]). Dafür wird der Speicherchip ausgelötet und dann mittels spezieller Hardware, wie zum Beispiel PC-3000 Flash [Laboratory, 2011], aufgerufen. Der Vorteil dieses hardwarebasierten Ansatzes ist, dass keine Zwischenschicht den Lesezugriff auf die nicht geänderten Daten auf dem Chip manipuliert oder verhindert. Dadurch kann den ausgelesenen Daten ein hoher Grad forensischer Glaubwürdigkeit beigemessen werden. Trotzdem gibt es einen Nachteil dieser Methode: Der Aufwand ist relativ hoch, verglichen mit dem softwarebasierten Ansatz. Spezifisches technisches Equipment sowie Wissen über die Vorgehensweise sind nötig, um den Speicherchip auszulöten. Wird der Chip von der Platine entfernt, besteht ein erhöhtes Risiko, den Chip zu beschädigen oder zu zerstören, inklusive der sich darauf befindlichen Daten. Diese Vorgehensweise wird trotzdem häufig in der Praxis von Strafverfolgungsbehörden verwendet.

Nutzen des Boundary-Scans (JTAG)

Der Boundary-Scan ist eine Testmethode, um elektronische Komponenten wie Chips oder Platinen zu testen oder zu debuggen. Bei vielen modernen Smartphones ist der Boundary-Scan nutzbar. Diese besondere Scan-Methode wurde unter IEEE 1149.1 [IEEE Standards Association, 2001] standardisiert, sie ist jedoch bekannt unter dem Begriff *JTAG* (*Joint Test Action Group*), der auch der Gruppenname der Gründer ist.

Durch diesen Standard sind Mittel zum debuggen von Hardware und seiner Programme verfügbar. Geht es um die forensische Analyse von Smartphones, können über das entsprechende Interface der Smartphone-Platine vollständige Speicherabbilder erstellt werden. Gemäß Casey [Casey, 2009] haben Speicherchips normalerweise keine JTAG-Funktionalität. Da sie mit Daten und Adressbuses verbunden sind, kann JTAG trotzdem genutzt werden, um auf diese Chips zuzugreifen. Um das Interface aufzurufen, ist besondere Hardware nötig (z. B. RIFF-Box [Team, 2010]) sowie das entsprechende Datenblatt des Herstellers, um die richtigen Punkte zu identifizieren und um das Interface zu löten.

Diese Art des Datenzugriffs beherbergt, wie auch die zuvor beschriebene Methode, das Risiko, das Gerät zu beschädigen und dadurch ebenfalls Daten zu verlieren.

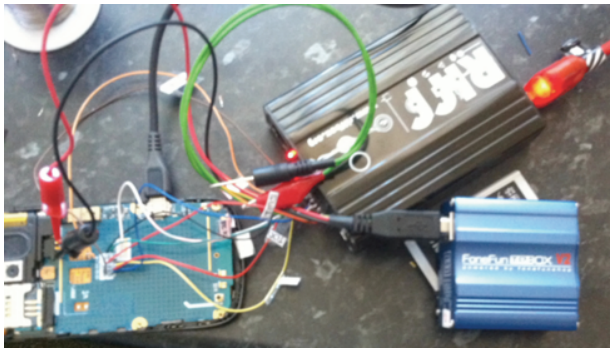

Abb. 1.2: Auslesen des Speichers eines HTC Smartphones mittels *Riff-Box* und *JTAG*.

Zudem ist tiefgreifendes technisches Verständnis nötig. Jedoch liegen die Anforderungen an den Ermittler und die Gefahren deutlich unter denen beim manuellen Auslöten des Speicherbausteins.

Nutzen eines Datenkabels oder der Entwickler-Schnittstelle

Um ein Datenabbild eines Android-Geräts zu erstellen, kann das Android Software Development Kit (Android SDK) verwendet werden. Das Android SDK beinhaltet die Android-Debug-Bridge (adb), ein Client-Server-Programm, das sich mit Android-Geräten verbindet und eine Vielzahl an Kommandos auf dem verbundenen Gerät ausführen kann. Deshalb muss eine Instanz des adb daemon auf dem Gerät laufen; dies ist möglich durch die Aktivierung der Option *USB-debugging* auf dem Zielgerät.

Eine zusätzliche Bedingung ist, dass Rechte auf dem Gerät einen Zugriff auf die zu kopierenden Dateien gewähren müssen. Da Rechte auf Android-Geräten im Production Mode den Zugriff auf Datenbanken via adb verweigern, muss das System modifiziert werden oder ein individuelles Recovery-Image muss genutzt werden um den Status des Geräts so zu verändern, dass diese Sicherheitsrestriktionen deaktiviert oder umgangen werden können (beide Ansätze werden in dem Abschnitt 3.2.1 behandelt).

Allgemein gesprochen, ist ein Kommunikationsansatz über die Entwicklungsschnittstelle ein softwarebasierter Ansatz. Es ist jedoch nicht nötig, neue Software auf dem Gerät zu installieren. Darüber hinaus werden einige Android-spezifische Einstellungen benötigt. Daher gilt dieser Ansatz als Mittelweg zwischen softwarebasierten und hardwarebasierten Vorgehensweisen. Dieser Ansatz wird später noch für das Analyse-Tool ADEL verwendet (mehr zu ADEL in Abschnitt 3.6) und findet auch seine Verwendung in den kommerziellen Tools von z. B. Cellebrite und XRY.

Diese Methode ist bei aktuellen iOS-Endgeräten die einzige Möglichkeit an Daten auf dem Endgerät zu kommen. Dazu wird meist ein funktionierender Jailbreak benötigt (abhängig davon ob man nur eine logische Auswertung möchte, d. h. nur das was auf dem Gerät auch für den Nutzer noch sichtbar ist, oder ob man auch gelöschte Daten wiederherstellen will) und die PIN bzw. das Passwort des Nutzers um das Gerät zu entsperren.

Kontrollaufgabe 1.2: Auslöten vs. JTAG

Worin besteht der Unterschied zwischen der Methode des manuellen Auslötens des Speicherbausteins und der Verwendung der JTAG-Schnittstelle?

K

K

Kontrollaufgabe 1.3: Softwarebasierte Agenten

Worin besteht das Problem bei der Verwendung von softwarebasierten Agenten zur forensischen Analyse?

Wiederherstellung und Auswertung von Daten

Diese Phase beinhaltet das Finden von Beweisen, die gelöscht, versteckt, maskiert oder auf eine andere Art unzugänglich gemacht wurden. Um diese Aufgabe zu erledigen, ist tiefgreifendes Wissen über das Dateisystem und weitere Datenstrukturen nötig.

Aus forensischer Perspektive sind Festplatten und Low-Level-Strukturen von verschiedensten Dateisystemen sehr gut analysiert und beschrieben (für Beispiele dazu siehe Carrier [Carrier, 2009]). Die Eigenschaften der NAND-Technologie und die Anzahl an wiederherstellbaren Daten auf mit dieser Technologie bestückten Speicherbausteinen ist dagegen bisher kaum forensisch analysiert worden. Durch die Tatsache, dass „Wear-Leveling-Techniken“ alte und eigentlich nicht mehr existente Daten überall auf dem Speichermedium zurücklassen, wird oft angenommen, dass es einfacher ist, gelöschte Daten auf einem NAND-Speicher wiederherzustellen und somit auch deutlich schwerer für Kriminelle, diese Daten sicher zu löschen. Sehr oft gibt es auf diesen Speicherbausteinen jedoch softwarebasierte Lösungen, die diesen „Leichen“ durch Techniken wie *Garbage Collection* entgegenwirken.

Eine weitere Methode, NAND-Flash-spezifisches Verhalten zu implementieren, besteht darin, speziell angepasste Dateisysteme zu verwenden. Diese Dateisysteme sind darauf spezialisiert, die Einschränkungen von Flash-basierten Speichern zu berücksichtigen, sobald sie auf diese Speicherbausteine lesend oder schreibend zugreifen. Diese Dateisysteme sind aus forensischer Sicht deutlich einfacher zu analysieren, da sie Techniken wie wear leveling in Software implementiert haben und nicht auf Hardwareebene. Eines der bekanntesten Beispiele eines solchen Dateisystems ist YAFFS2. YAFFS2 steht für “Yet Another Flash File System 2” und war das unter Android verwendete Dateisystem bis Ende 2010. Obwohl seid 2011 mit der Einführung von Gingerbread (Android 2.3) das verwendete Dateisystem auf EXT4(siehe hierzu Fairbanks et al. [Fairbanks, 2012, Fairbanks et al., 2010]) umgestellt wurde, gibt es immer noch eine hohe Anzahl an Telefonen mit Android-Versionen kleiner 2.3, die somit auch immer noch YAFFS2 verwenden.

Befasst man sich im Rahmen der Analyse mit einem iOS-Endgerät, so findet man als Dateisystem entweder das gut dokumentierte *HFS+* oder das neue, aber ebenfalls bereits ausführlich beschriebene *APFS*. HFS+ lässt sich mit gängigen Werkzeugen auch nach gelöschten Dateien und deren Fragmenten durchsuchen. *Garbage Collection* findet man auf diesen Endgeräten erst, wenn der komplette interne Speicher voll ist. Da die aktuellen Geräte schnell 128 GB und mehr an Speicher besitzen, tritt dieser Punkt erst sehr spät ein und die Wahrscheinlichkeit gelöschte Daten zu finden ist bei diesen Endgeräten deutlich höher als bei Android-Geräten. APFS unterstützt die Verschlüsselung ganzer Volumens, einzelner Dateien und sensibler Metadaten (dies ist einer der wichtigsten Unterschiede für uns im Vergleich zur reinen Verschlüsselung von Volumes wie es bei HFS+ der Fall war). Es unterstützt folgende Verschlüsselungsmethoden [apf, 2018]:

- *Single-key-Verschlüsselung*
- *Multi-key-Verschlüsselung* mit per-file-Schlüsseln für Daten und separatem Schlüssel für sensible Metadaten. Multi-key-Verschlüsselung gewährleistet

die Integrität der Benutzerdaten. Selbst wenn jemand die physische Sicherheit des Geräts kompromittierte und sich Zugang zum Geräteschlüssel verschaffte, könnte er die Benutzer-Dateien nicht entschlüsseln. Apple File System benutzt *AES-XTS* oder *AES-CBC* Verschlüsselungsmodi, abhängig von der Hardware.

Eine weitere wichtige „Struktur“ bei der Analyse von Android-Telefonen ist SQLite [Research, 2010],eine in Software gebaute Bibliothek, die ein SQL-Datenbanksystem für eingebettete Systeme implementiert. Android verwendet SQLite-Datenbanken zur Speicherung von Daten der Applikationen und auch für wichtige Systemdatenbanken wie z. B. Adressbuch, Anruflisten, GPS-Daten und SMS-Nachrichten. Diese Daten sind für eine forensische Analyse von Mobiltelefonen und deren Applikationen extrem wichtig.

Zur Verwaltung der SQLite-Datenbankdatei wird diese in Seiten (engl.: pages) fester Größe unterteilt. Die Seitengröße ist in den Kopfdaten (engl.: header) der Datenbankdatei gespeichert. Die Kopfdaten beinhalten 20 Felder unterschiedlicher Länge mit einer Kapazität von insgesamt 100 Bytes und stehen am Anfang (der ersten Seite) der Datei. Die ersten 16 Bytes der Kopfzeilen enthalten die null-terminierte Zeichenkette „SQLite format 3“, die jede SQLite-Datenbankdatei charakterisiert. Die weiteren Felder beinhalten Informationen über den allgemeinen Aufbau der Datenbankdatei, u. a. die Seitengröße. Diese Informationen dienen der Speicherverwaltung innerhalb der Datei (Verwaltungsstrukturen). Neben den Kopfdaten sind zwei weitere wichtige Verwaltungsstrukturen Bestandteil jeder SQLite-Datenbankdatei:

- In Form einer verketteten Liste werden Zeiger auf Seiten, die sich zum jeweiligen Zeitpunkt nicht in aktiver Verwendung befinden (ungenutzte Seiten), gespeichert (sogenannte Freelist).
- Die eigentlichen Inhalte der Datenbankdatei werden mit Hilfe einer vollständig sortierten Baumstruktur (B-Baum) gespeichert.

Anhand der in SQLite-Datenbankdateien gespeicherten Verwaltungsstrukturen ist es möglich, die Inhalte der Datenbank gezielt und unter forensischen Gesichtspunkten auszulesen.

Während der Analyse von Android-Smartphones kann der RAM-Inhalte zusätzliche Information für den Ermittler liefern. Beispielsweise können aus dem RAM-Benutzernamen und Passwörter für Social Networks oder E-Mail-Accounts ausgelesen werden und später für eine weitere Analyse verwendet werden.

In Abschnitt 3.4 zeigen wir, wie man durch Verknüpfung von Lokalisierungsdaten aus verschiedenen Apps und Systemdatenbanken ein aussagekräftiges Bewegungsprofil eines Smartphone-Nutzers erzeugen kann. Der größte Vorteil dieser Art der Erzeugung eines Bewegungsprofils im Vergleich zu den Daten, die ein Ermittler vom Mobilfunk-Provider bekommen kann, liegt in der Genauigkeit der eigentlichen Daten und der Tatsache, dass hierzu eine einfache Beschlagnahme des Mobiltelefons ausreichend ist.

Stichwörter