Hochschule Wismar
University of Technology, Business and Design
Fakultät für Ingenieurwissenschaften
Bereich Elektrotechnik und Informatik

Masterthesis

Analyse und Interpretation von auf Smartphones erzeugten Geodaten

Eingereicht am: 06. November 2021

von: Lena Ziegler

Anmerkung: Die in der Masterthesis enthaltenen Geodaten wurden für die Veröffentlichung teilweise anonymisiert.

Aufgabenstellung

Das Zuhause zu verlassen ohne das Smartphone bei sich zu haben ist für viele mittlerweile unvorstellbar. Das kleine Helferlein ersetzt und vereint Telefonzelle, Telefonbuch, Taschenkalender, Fotoapparat und viele weitere Gebrauchsgegenstände, die wir früher immer bei uns trugen oder aufsuchen mussten. Geräte, welche uns in unserem Alltag unterstützen, aber auch viel über uns erzählen können.

So werden die Geräte auch von Straftätern verwendet, die sich mit Hilfe des Smartphones beispielsweise zu Straftaten verabreden oder diese bei der Begehung einer Straftat mit sich führen. Die daraus resultierenden Daten sind für Ermittlungsbehörden besonders wichtig. So können neben den gespeicherten Rufnummern und versandten bzw. empfangenen Nachrichten auch Geodaten auf den Geräten vorhanden sein. Aufgrund der immer wichtiger werdenden Rolle der Geodaten in Ermittlungsverfahren sollen im Rahmen dieser Masterthesis die auf Smartphones erzeugten Geodaten analysiert und interpretiert werden.

Dazu werden die auf unterschiedliche Arten erzeugten Geodaten näher betrachtet und die Aussagekraft dieser Daten analysiert. Um die Analysen durchzuführen werden zwei Smartphones mit den Betriebssystemen Android und iOS als Testgeräte verwendet. Mit Hilfe verschiedener zuvor festgelegter Testszenarien werden Geodaten betrachtet, welche sowohl durch Anwendungen (engl. Applications, kurz „Apps“), als auch durch das Gerät selbst erzeugt werden.

Kurzbeschreibung

Neben den sichtbaren Spuren an einem Tatort gibt es auch die unsichtbaren, digitalen Spuren wie beispielsweise Spuren, welche von bzw. auf smarten Geräten erzeugt werden. Durch die immer größer werdende Menge an smarten Geräten nimmt die Bedeutung digitaler Spuren bei der Aufklärung von Straftaten zu und bildet bei den Ermittlungsbehörden einen festen Bestandteil in Ermittlungsverfahren.

Smartphones können hierbei mögliche Hinweise für eine Tatbeteiligung liefern. Nicht nur Telefonate und Chatnachrichten sind von großer Bedeutung, auch die auf dem Gerät gespeicherten Geodaten können ein erster Hinweis sein, dass der Nutzer des Smartphones möglicherweise an einem Tatort war.

Wann generieren Anwendungen Geodaten, wie werden diese gespeichert und wie genau sind diese? Fragen, die beantwortet werden müssen, damit die Daten richtig interpretiert werden können.

Abstract

Besides the visible traces at a crime scene, there are also the invisible digital traces. For example, traces that are produced by or on a smart device. Due to the ever increasing number of smart devices, the importance of digital traces in the investigation of crimes is also increasing. In an investigation, digital traces form an integral part in the investigative proceedings for the authorities.

Smart phones can provide possible indications about someone's participation in a criminal act. Not only phone calls and chat-messages are of great importance, but also geodata stored on the device can be the first hint that the user of the smart phone had probably been at the crime scene.

But when is geodata created by applications? How is it stored and how exact is it? These questions need to be answered in order to be able to interpret the data accurately.

Inhalt

1 Einführung

Vor fast 40 Jahren wurde durch den Mobiltelefonhersteller Motorola das erste Handy auf den Markt gebracht. 1983 war es erstmals möglich Anrufe auch von unterwegs zu tätigen. Ab 1992 war es dann auch in Deutschland möglich ein solches Handy zu erwerben. Zum Preis von 3.000 DM war es, inklusive Vertrag, bei D1 oder D2 erhältlich. Umgerechnet wären dies, unter Einbeziehung der Inflation, heutzutage etwa 2.500 €. Das erste Handy mit GPS-Modul[1] (Global Positioning System) wurde durch den finnischen Hersteller Benefon im Jahr 1999 vorgestellt, welches vor allem im Outdoor-Bereich auf Zuspruch stieß. [1]

Das erste Smartphone mit kapazitivem[2] Touchscreen wurde 2007 von LG vorgestellt, es enthielt jedoch noch kein GPS. Das erste iPhone, welches ebenfalls 2007 vorgestellt wurde, enthielt auch noch kein GPS. Erst ein Jahr später, im Juni 2008, wurde das Apple iPhone 3G vorgestellt, welches GPS enthält. [2]

Im Laufe der Jahre stieg der Anteil der privaten Haushalte, welche mindestens ein Mobiltelefon besitzen. 2020 waren es in Deutschland 97,5% der Haushalte. [3] Die Anzahl der Smartphone-Nutzer beträgt im Jahr 2020 60,7 Millionen Nutzer. Bei einer Einwohnerzahl von 83,16 Millionen Personen in Deutschland entspricht die Anzahl der Smartphone-Nutzer somit rund 73%. [4] [5]

Über 60 Millionen Geräte sind demnach deutschlandweit täglich im Einsatz und erzeugen bzw. speichern Daten. Eine schnelle Nachricht an einen Freund oder kurz einen Frisörtermin ausmachen - heutzutage kein Problem mehr, alles ist von diesem kleinen Gerät aus machbar. Auch Straftäter nutzen diese Möglichkeit, und so ergibt sich daraus ebenfalls eine Bedeutung

[1] Erklärung zu GPS in Kapitel 2.3

[2] Bei einem kapazitiven Touchscreen handelt es sich um einen Bildschirm, welcher die elektrischen Eigenschaften des menschlichen Körpers nutzt. Bei einer Berührung des Bildschirms wird an der Kontaktstelle eine kleine elektrische Leistung erzeugt, anhand dieser berechnet werden kann, wo der Kontakt erfolgt ist. [50]

für Ermittlungsverfahren. Verabredungen zu Taten oder das Navigieren zu einem Tatort – mit einem Mobilgerät kein Problem. Diese Daten können nach der Identifizierung der Täter jedoch in das Ermittlungsverfahren einbezogen werden und liefern stichhaltige Beweise um den Täter mit der Tat in Verbindung zu bringen.

Besonders interessant sind hier oftmals die Geodaten aus den Mobilgeräten. Diese können den Ermittlern beispielsweise Hinweise auf den Standort des Mobilgerätenutzers geben. Diese Daten können be-, aber natürlich auch entlastend in die Ermittlungsarbeit einfließen.

1.1 Motivation

Im Bereich der Strafverfolgung spielen Geodaten eine immer größer werdende Rolle und tragen oftmals maßgeblich zum Erfolg eines Verfahrens bei. Auf Mobilgeräten verwenden immer mehr Applikationen, kurz Apps, die Standortbestimmung – sei es bei der Navigation, bei Nachrichten-Apps für Nachrichten aus der Umgebung, bei Fitnesstrackern zum Aufzeichnen von gelaufenen Strecken, bei Lokationen-basierten-Spielen[3] oder Dating-Apps. Unter anderem die Verwendung dieser Apps führt zur Speicherung von Standortdaten auf dem Mobilgerät, welche in die Ermittlungsverfahren einfließen.

Die forensische Auswertung von Geodaten ermöglicht dem Ermittler die Feststellung des Standortes des Smartphones zu einem gewissen Zeitpunkt. So kann möglicherweise das Mobilgerät eines Tatverdächtigen mit einem Tatort in Verbindung gebracht werden und es besteht dadurch die Möglichkeit, dass der Tatverdächtige als Nutzer des Mobilgerätes somit ebenfalls am Tatort war.

Das Vorhandensein von Geodaten auf dem Mobilgerät beweist jedoch nicht zwingend, dass auch der Nutzer dieses Gerätes an diesem Ort war. Für die

[3] Beispiele für Lokation-basierte-Spiele: Pokémon Go und Harry Potter: Wizards Unite

Aussagekraft von Geodaten muss daher die Herkunft der Geodaten evaluiert werden.

Diese Masterthesis soll eine Hilfestellung für IT-Forensiker sein, welche sich mit Geodaten und deren Aussagekraft beschäftigen. Damit diese Daten in Ermittlungsverfahren eingesetzt werden können, darf es keine Zweifel an der Verwertbarkeit geben – hierfür soll diese Masterthesis einen wichtigen Beitrag leisten.

1.2 Definition der Forschungsfragen

Die Forschungsfragen der Masterthesis lauten:

- Wie genau sind die auf Smartphones erzeugten Geodaten?
- Was passiert mit Geodaten aus den Meta-Daten von Dateien bei deren Versand bzw. Übertragung?
- Wie können Geodaten interpretiert werden und welche Aussagekraft haben diese?

1.3 Vorgehensweise

Nach einer Einführung in diesem Kapitel werden in Kapitel 2 die Grundlagen von Geodaten erläutert. Neben einer Einführung in Geodaten wird der Begriff Georeferenzierung erklärt. Ein Fokus dieses Kapitels liegt auf der Erläuterung der Funktionsweise der Positionsbestimmung. Damit ein Smartphone ein Geodatum speichern kann, muss es zuerst wissen, wo es sich befindet. Erst dann können Geodaten im Gerät beispielsweise für die Navigation verwendet oder auch gespeichert werden.

Die IT-Forensik lässt sich in mehrere Teilgebiete untergliedern. Für die Masterthesis ist der Teilbereich der Smartphone-Forensik ein wichtiger Aspekt, auf welchen in Kapitel 3 eingegangen wird. Hierbei werden unter anderem die verschiedenen Möglichkeiten der Sicherungen von Smartphones erklärt.

Mit den durchzuführenden Testszenarien befasst sich das Kapitel 4. Es behandelt den Versuchsaufbau, definiert die Testszenarien und beschreibt die Software zur forensischen Sicherung, sowie die zu untersuchenden Anwendungen.

Die Auswertung und Evaluation der Testszenarien wird in Kapitel 5 vorgenommen. Die aus den Testszenarien gewonnenen Erkenntnisse werden dabei ebenfalls vorgestellt.

Den Abschluss dieser Masterthesis bildet Kapitel 6 mit einem Fazit über die Erkenntnisse, welche im Rahmen dieser Thesis gewonnen wurden. Ebenfalls soll ein Ausblick auf Weiterentwicklungen stattfinden und eine kurze Auseinandersetzung mit offengebliebenen Fragen erfolgen.

1.4 Abgrenzung

Das Ziel dieser Masterthesis ist die Erforschung der auf Smartphones erzeugten Geodaten. Diese sollen hinsichtlich ihrer Genauigkeit und Verfügbarkeit überprüft werden. Damit Smartphones Geodaten speichern können, müssen diese zunächst erzeugt werden. Die Funktionsweise der Positionsbestimmung wird im Allgemeinen erklärt, jedoch nicht wie die Daten in beispielsweise Bildern gespeichert werden. Ebenfalls nicht Bestandteil dieser Thesis wird die Funktionsweise des Geräteherstellers zur Speicherung von Geodaten im Gerät sein.

Für die Auswertung von Testszenarien, welche im Rahmen dieser Thesis angefertigt werden, müssen die Mobilgeräte mit Hilfe forensischer Software ausgelesen werden. Dabei werden neben den gewünschten Daten zu den Geodaten auch weitere Daten anfallen, welche jedoch nicht in diese Thesis und in die Auswertung einfließen. Auch wird auf die Vorgehensweise zur Erzeugung des Images nicht näher eingegangen.

Die Dissertation von Andreas Dhein von der Universität Koblenz-Landau aus dem Jahr 2018 beschäftigt sich mit dem Thema „Absicherung der ana-

lytischen Interpretation von Geolokalisierungsdaten in der Mobilfunkforensik“ [6]. Diese Arbeit thematisiert unter anderem die manuelle Untersuchung von Standortdaten auf Smartphones. Die vorliegende Arbeit untersucht jedoch vorher definierte Testszenarien unter Nutzung klassischer forensischer Software.

1.5 Stand der Forschung

Mit jedem neuen Gerät, jeder neuen Betriebssystemversion und jeder neuen App muss sich die IT-Forensik an die Neuerungen bzw. Änderungen anpassen. Daher gibt es in diesem Bereich regelmäßigen Forschungsbedarf und die Menge an Literatur ist groß.

Der Bereich der Smartphone-Forensik bildet hiervon keine Ausnahme. Die sich durch Neuerungen ergebenden Veränderungen sind hier sogar stärker ausgeprägt und von größerer Häufigkeit.

Ebenfalls sind für den Bereich Geodaten bzw. GPS viele Ausarbeitungen vorhanden. Diese beziehen sich dann auf die Geodäsie[4] im Allgemeinen oder aber beispielsweise auf deren Nutzung im Kontext von Smart Cities.

Auch im Bereich Social Media spielen Geodaten eine bedeutende Rolle, wenn es sich zum Beispiel um die zielgruppenorientierte Einblendung von Werbung etc. handelt.

Bezüglich der in der vorliegenden Masterthesis betrachteten Fragestellung, wann Geodaten auf Smartphones erzeugt werden, ob diese dort gespeichert sind und wie deren Interpretation zu erfolgen hat, gibt es jedoch bislang kaum Ausarbeitungen.

Neben der in Kapitel 1.4 vorgestellten Dissertation von Andreas Dhein konnten nur wenige Publikation im Bereich der forensischen Analyse von Geodaten auf Smartphones festgestellt werden. Diese waren auch bereits

[4] Die Geodäsie beschäftigt sich mit der Ausmessung und Abbildung der Erdoberfläche

älteren Datums, so dass deren Aktualität aufgrund der oben genannten regelmäßigen Veränderungen bei weitem nicht mehr gegeben sein dürfte.

In einer aus dem Jahr 2011 stammenden Publikation wurden gezielt Android-Geräte überprüft. 2016 wurden an einer koreanischen Universität die Spuren von Geodaten von Navigationsanwendungen untersucht und veröffentlich. Die dabei verwendeten Anwendungen sind jedoch aus dem asiatischen Raum und hier daher überwiegend unbekannt.

Hinsichtlich des Betriebssystem iOS konnte sogar ein komplettes Buch festgestellt werden. Dieses stammt allerdings bereits aus dem Jahr 2010.

Es kann daher bereits zu diesem Zeitpunkt festgestellt werden, dass es in diesem spezifischen Themengebiet noch großen Forschungsbedarf gibt.

2 Geodaten

Schätzungsweise 80 – 90% aller Daten weltweit können einem Ort zugeordnet werden und weisen somit einen Raumbezug auf. Sie werden daher als Geodaten bezeichnet. [7]

Die nachfolgenden Unterkapitel gehen auf die Definition von Geodaten, der Georeferenzierung und auf die Positionsbestimmung ein.

2.1 Definition

Geodaten sind Informationen, welche einer räumlichen Lage zugeordnet werden können. Man bezeichnet diese Zuordnung als Georeferenzierung.

Im täglichen Sprachgebrauch wird der Begriff Geodaten häufig mit dem Begriff Geoinformation synonym verwendet. Bei Geoinformationen handelt es sich wissenschaftlich gesehen jedoch um Informationen über Objekte und Sachverhalte mit Raumbezug, welche in Form von Geodaten elektronisch gespeichert werden. Durch Auswertung und Interpretation von Geodaten werden Geoinformationen gewonnen. [8] In einem GIS, dem Geoinformationssystem, werden Geoinformationen durch Geodaten repräsentiert. [9]

Geodaten bestehen aus verschiedenen Informationen:

- Geometriedaten: Lagebeschreibung des Objekts
- Topologiedaten: Beschreibung von Nachbarschaftsbeziehungen[5]
- Grafische Ausprägung: Signaturen, Beschriftungen
- Sachdaten: Semantische Beschreibungen[6], welche keinen geometrischen Bestandteil besitzen und erst durch die Zuordnung zu den raumbezogenen Daten einen Raumbezug erhalten.

[5] Die Topologie beschreibt Nachbarschaftsbeziehungen zwischen zwei Geoobjekten, wie zum Beispiel zwei Grundstücke, welche sich eine gemeinsame Grenze teilen.
[6] Sachdaten können zum Beispiel Informationen über die Art des Straßenbelags (Teer, Beton, Schotter) sein (http://www.giswiki.org/wiki/Sachdaten)

2.2 Georeferenzierung

Die Georeferenzierung beschreibt die Zuweisung raumbezogener Referenzinformationen zu einem Geodatensatz. Die Lage eines Objektes wird in ein definiertes Bezugssystem geschrieben und ist somit eindeutig verortet. [7]

Die Georeferenzierung kann über zwei Ansätze erfolgen:

- Direkte Georeferenzierung: Die Lage eines Objektes wird anhand von Koordinaten definiert. Es kann zum Beispiel eine zwei- oder dreidimensionale Verortung über x-, y-, und z-Koordinaten im Raum erfolgen. [7]
- Indirekte Georeferenzierung: Die Lage eines Objektes wird anhand eines administrativen Gebiets (Land, Stadt, Straße) definiert. Probleme ergeben sich hierbei bei Georeferenzierungen welche sich verändern können, wie zum Beispiel bei Postleitzahlen. [7]

2.3 Positionsbestimmung

Die Positionsbestimmung kann mit Hilfe verschiedener Systeme realisiert werden. So war es früher üblich, dass Seeleute ihren Kurs anhand der Sterne berechneten und auch in der Bibel wird von den drei Weisen aus dem Morgenland berichtet, die einem Stern nach Bethlehem folgten, um Jesus in der Krippe zu finden. Natürlich hat sich seither einiges geändert.

Es ist kein Geheimnis mehr, dass heutzutage die Positionsbestimmung bei Navigationsgeräten und Smartphones unter anderem mit Hilfe von Satelliten-Systemen durchgeführt wird. [10]

Die Erde wird hierbei von vielen Satelliten unterschiedlicher Systeme umkreist, welche permanent Signale aussenden. Mit Hilfe dieser Signale können an jeder Stelle der Erde mittels eines kompatiblen Empfängers die genauen Koordinaten bestimmt werden.

Das bekannteste Navigationssatelliten-System ist das amerikanische Global Positioning System, kurz GPS. Ursprünglich wurde es für militärische Zwecke unter dem Namen NAVSTAR GPS[7] entwickelt und ist seit den 1990er Jahren einsatzbereit. Für die zivile Nutzung war NAVSTAR GPS anfangs weniger geeignet. Das Ergebnis wurde mit Hilfe einer künstlich generierten Ungenauigkeit verschlechtert, sodass dabei Abweichungen von mehr als 100 Meter entstanden. Als im Jahr 2000 die künstliche Ungenauigkeit abgeschaltet wurde, war es für zivile Anwendungen möglich, Positionsbestimmungen mit einer Ungenauigkeit von unter zehn Metern zu erreichen. [11]

Ein weiteres, ebenfalls zu Beginn militärisch verwendetes System, ist das russische System GLONASS (Global Navigation Satellite System), welches einen Vorteil gegenüber GPS in der Genauigkeit der Positionsbestimmung und Geschwindigkeitsermittlung bietet. So weist GLONASS in der freien Variante eine Genauigkeit von vier bis acht Metern auf. Seit 2008 ist GLONASS für die zivile Bevölkerung nutzbar, nach technischen Schwierigkeiten zu Beginn ist GLONASS jedoch erst seit 2013 weltweit konstant abrufbar. [12]

Mit dem Satellitensystem Galileo ist das erste unter ziviler europäischer Kontrolle stehende System in Betrieb. Galileo arbeitet hierbei jedoch nicht konkurrierend, sondern mit GPS zusammen. Hierdurch soll eine genauere Positionsbestimmung möglich sein. Galileo befindet sich derzeit noch im Aufbau, so waren Anfang 2021 von 30 geplanten Satelliten erst 26 Galileo-Satelliten im Erdorbit. Galileo soll in zwei Varianten verfügbar sein: Die kostenpflichtige Version soll eine Toleranz von nur wenigen Zentimetern aufweisen, die kostenfreie Version soll auf etwa vier Meter genau sein. [12]

Seit 2020 ist das chinesische System BeiDou im Vollbetrieb. Es gilt als direkter Konkurrent zu dem europäischen System Galileo. Ursprünglich wurde das europäische System durch die Chinesen unterstützt, diese entschieden sich dann jedoch für den Aufbau eines eigenen Systems. Wie

[7] NAVSTAR GPS = **Nav**igational **S**atellite **T**iming **a**nd **R**anging **G**lobal **P**ositioning **S**ystem

auch bei Galileo gibt es hier Unterschiede in der Exaktheit der kostenpflichtigen zur kostenfreien Version: zehn Zentimeter zu zehn Meter. [12]

Die nachfolgende Abbildung zeigt die Logos der vier vorgestellten Navigationssatelliten-Systeme.

Bild 1: Darstellung der Logos von Navigationssatelliten-Systemen [7]

Der Begriff GPS wird in der Regel als Synonym für alle globalen Navigationssatelliten-Systeme verwendet. Die Erklärung der Funktionsweise von Satellitensystemen wird daher am Beispiel von dem Navigationssatelliten-System GPS erfolgen.

Um mit Hilfe von Satelliten eine Positionsbestimmung durchzuführen, werden eine gewisse Anzahl an Navigations-Satelliten benötigt. Das Navigationssatelliten-Systeme GPS umfasst 24-30 Satelliten, welche auf 6 Bahnebenen in ca. 20.200 km Höhe die Erde umkreisen. So werden mindestens vier, in der Praxis jedoch meist sechs bis acht Satelliten gleichzeitig empfangen.

„Die Satelliten haben hochpräzise Atomuhren an Bord und umkreisen die Erde zweimal pro Sterntag. Ein Sterntag dauert exakt 23 Stunden, 56 Minuten und 4,091 Sekunden.“ [11] Dadurch ergibt sich eine Geschwindigkeit der Satelliten von ca. 3,9 km/s. [11]

Bild 2: Schematische Darstellung der Satellitenbahnen [11]

Jeder Satellit besitzt eine individuelle Kennung. Diese sendet er mit der aktuellen GPS-Zeit und seinen Bahndaten fortlaufend zur Erde. Ein Empfänger kann aus diesen Informationen zu jedem Zeitpunkt die exakte Satellitenposition errechnen. Der Abstand des Empfängers zum Satelliten kann mit Hilfe der Laufzeit des Signals berechnet werden. Somit sind die wichtigsten Daten festgelegt. Der Empfänger hat die Information „wo sich der Satellit zu einem bestimmten Zeitpunkt befunden hat und wie groß der Abstand war.“ [11]

Bild 3: Berechnung des Abstands zum Satelliten [11]

Mit den Daten eines einzelnen Satelliten kann jedoch noch keine Position bestimmt werden. Für eine Positionsbestimmung werden die Daten von mindestens drei Satelliten benötigt, um mit deren Hilfe die genaue Position berechnen zu können. Hierbei stellen die Satelliten Punkte dar, von welchen die Position bekannt ist. Legt man hier drei unterschiedlich lange Strecken an, kann mit Hilfe der Triangulation der Punkt berechnet werden, an denen sich die drei Strecken treffen. [11]

Bild 4: Positionsbestimmung mittels drei Satelliten per Triangulation [11]

Für die Bestimmung der unterschiedlichen Laufzeiten der Satellitensignale muss der GPS-Empfänger ebenfalls eine extrem genaue Uhr besitzen. Eine Abweichung der Empfängeruhr von 1 ms würde zu einem Fehler in der Strecke von ca. 300 km führen. Jedoch können in den Empfängern keine Atomuhren verwendet werden. Die Zeitabweichung zwischen Empfängeruhr und GPS-Zeit muss daher individuell ermittelt werden. Hierfür muss ein vierter Satellit empfangen werden. Somit müssen für eine exakte Positionsbestimmung mindestens vier Satelliten empfangen werden: drei Satelliten zur Positionsbestimmung und ein Satellit für die Zeitkorrektur. [11]

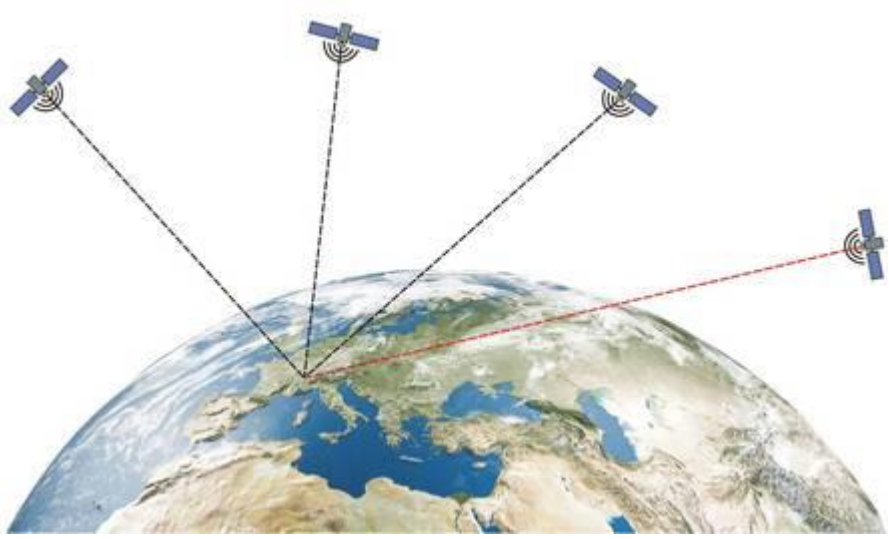


Bild 5: Ermittlung der Zeitkorrektur [11]

Die berechnete Position bezieht sich bei GPS auf das WGS84[8]. Dieses System dient auf der Erde und im erdnahen Weltraum als einheitliche Grundlage für Positionsangaben. Die GPS-Koordinaten werden als Dezimalgrad oder als Grad, Minute und Sekunde angegeben.

Wird einer GPS-Koordinate ein entsprechendes Kartenmaterial hinterlegt, so wird die Position auf einer Karte mit Straßen angezeigt. [11]

In nachfolgender Grafik wird die Position mit den Koordinaten N 53.889545 E 11.444584 (Dezimalgrad WGS84) bzw. N 53° 53‘ 22.362“ E 11° 26‘ 40.5024“ (Grad Minuten Sekunden WGS84) auf einer Karte grafisch dargestellt. Es handelt sich hierbei um die Hochschule Wismar – Fakultät für Ingenierswissenschaften / Bereich Elektrotechnik und Informatik. [13]

[8] WGS84 = World Geodetic System 1984

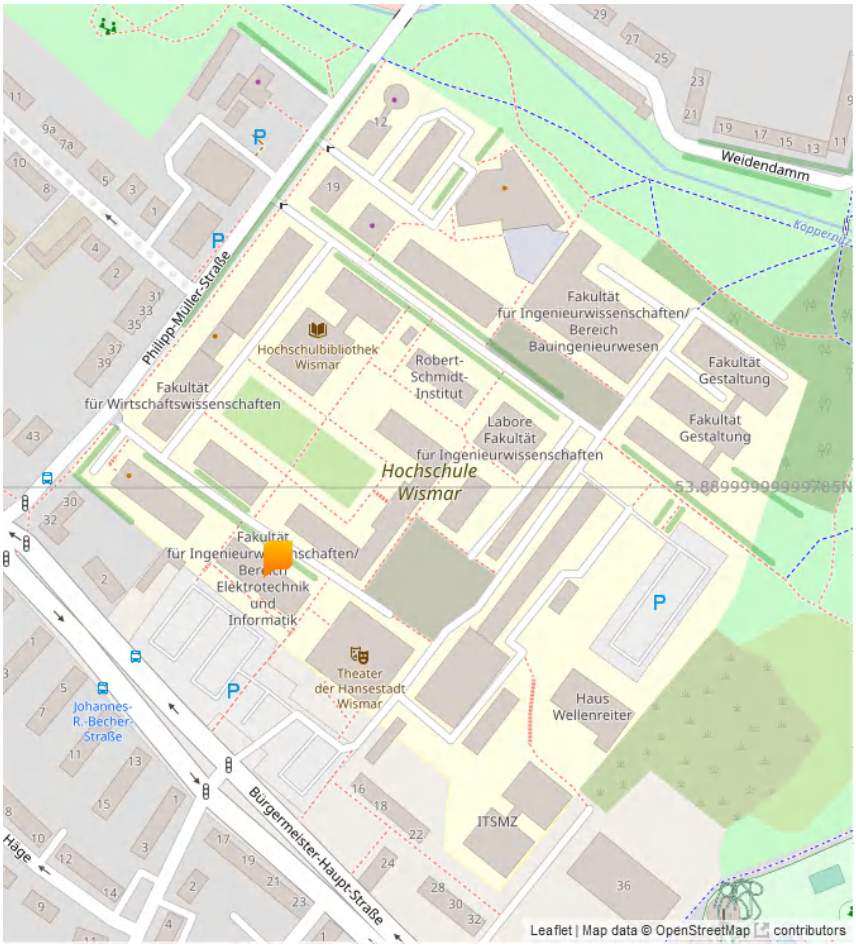


Bild 6: Darstellung der Positionsangabe auf einer Karte [13]

Zur Genauigkeit von GPS lässt sich pauschal sagen, dass die Genauigkeit mit der Anzahl der empfangenen Satelliten zunimmt. Die GPS-Empfänger von Smartphones arbeiten mittlerweile mit bis zu zwölf Satellitensignalen und können neben GPS auch weitere Navigationssatelliten-Systeme empfangen. [14]

Die Genauigkeit bei Positionsangaben bei GPS liegt in der Regel unter 10 Meter, jedoch ist sie von vielen Faktoren abhängig. Technisch bedingt können sich Fehler in der Zeit und der Laufzeit, sowie Satellitenfehler auf die Positionsbestimmung auswirken. Der wichtigste Faktor für die Genauigkeit ist jedoch die freie Sicht zum Satelliten. So können Gebäude, Bäume, der natürliche Geländeverlauf und auch das Wetter das Signal abschatten oder auch reflektieren, wie nachfolgende Abbildung zeigt. [11]

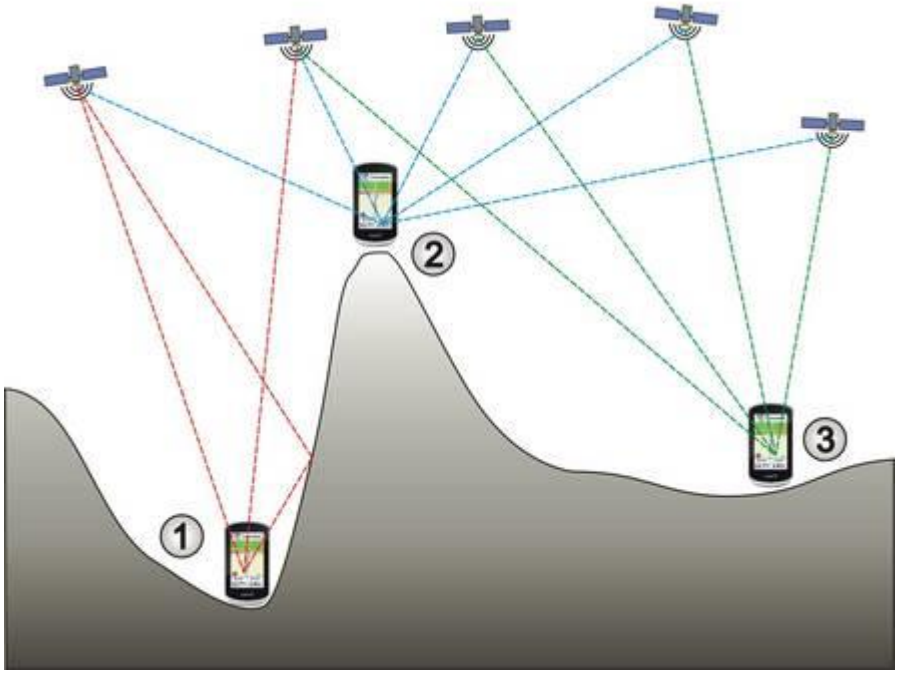


Bild 7: Genauigkeit von GPS [11]

Während das Gerät Nr. 2 auf dem Berg fünf Satelliten empfängt und somit sehr guten Empfang hat, hat das Gerät Nr. 3 bereits mit vier empfangbaren Satelliten bereits nur noch guten Empfang. In beiden Fällen ist eine Positionsbestimmung jedoch möglich. Gerät Nr. 1 empfängt nur zwei Satelliten. Eine Positionsbestimmung ist aufgrund des fehlenden dritten Satelliten nicht möglich. Die Grafik veranschaulicht ebenfalls eine Reflektion des Signals an einem natürlichen Geländeverlauf. Der linke Satellit sendet seine Daten an den Empfänger. Das Signal prallt jedoch an dem Berg ab und wird zu Gerät Nr. 1 reflektiert. [11]

Smartphones nutzen neben GPS noch das sogenannte Assisted-Global Positioning System, kurz A-GPS, um eine bessere Positionsbestimmung durchführen zu können. Neben den Daten aus Navigationssatelliten-Systemen werden beim A-GPS noch Bluetooth, WLAN, mobile Daten und der exakte Abstand zu Mobilfunkmasten in die Positionsbestimmung einbezogen. A-GPS vereint somit die Vorteile von mehreren Systemen. [12]

3 Smartphone-Forensik

Das vorangegangene Kapitel hat eine Einführung in eines der für diese Masterthesis relevanten Themengebiete, die der Geodaten, gegeben. Eine weitere Grundlage bildet das Thema Smartphone-Forensik, welches für die forensische Untersuchung von Smartphones benötigt wird.

Hierzu erfolgt nach einer Definition der Forensik im Kapitel über Datenspeicher eine Übersicht der Gerätespeicher, welche in einem Smartphone verbaut sind. Anschließend werden im Kapitel über Betriebssysteme die beiden Betriebssysteme Android und iOS betrachtet. Im Kapitel zur Datenextraktion wird auf die Vorgehensweise bei der Datenextraktion und die drei unterschiedlichen Arten der Datenextraktion eingegangen.

3.1 Definition und Vorgehensweise

Der Begriff Forensik definiert allgemein „alle Arbeitsgebiete, die strafrechtlich und zivilrechtlich relevante Handlungen identifizieren, ausschließen, analysieren und rekonstruieren“. [15]

Eines dieser Arbeitsgebiete bildet die IT-Forensik. Diese wird im Leitfaden „IT-Forensik“ des Bundesamts für Sicherheit in der Informationstechnologie, kurz BSI, wie folgt definiert: [16]

> *„IT-Forensik ist die streng methodisch vorgenommene Datenanalyse auf Datenträgern und in Computernetzen zur Aufklärung von Vorfällen unter Einbeziehung der Möglichkeiten der strategischen Vorbereitung insbesondere aus der Sicht des Anlagenbetreibers eines IT-Systems.“*

Die IT-Forensik lässt sich in mehrere Teilgebiete untergliedern. Hierzu zählen unter anderem:

- Betriebssystem-Forensik
- Multimedia-Forensik
- Netzwerk-Forensik
- Smartphone-Forensik

Unabhängig vom Teilgebiet ist das Ziel einer forensischen Untersuchung im Kontext der Strafverfolgung die Beantwortung nachfolgender Fragen: [16]

- Was ist geschehen?
- Wo ist es passiert?
- Wann ist es passiert?
- Wie ist es passiert?
- Wer hat es getan?
- Was kann gegen eine Wiederholung getan werden?

Die Untersuchung von Beweisen muss immer so durchgeführt werden, dass Thesen anhand von Spuren untermauert, aber auch widerlegt werden können. [16]

Die Vorgehensweise an eine forensische Untersuchung ist hierbei an Anforderungen geknüpft: [16]

- Akzeptanz: Methoden und Schritte müssen in der Fachwelt beschrieben und akzeptiert sein
- Glaubwürdigkeit: Robustheit und Funktionalität von Methoden
- Wiederholbarkeit: gleiches Ausgangsmaterial muss bei gleicher Anwendung von Hilfsmitteln und Methoden zu demselben Ergebnis führen
- Integrität: Spuren dürfen nicht unbemerkt verändert werden
- Ursache und Auswirkungen: Logisch nachvollziehbare Verbindungen zwischen Ereignissen und Beweisspuren und eventuell auch Personen
- Dokumentation des Ermittlungsprozesses

Die IT-Forensik lässt sich bezüglich des Zeitpunkts der Untersuchung in die Live-Forensik und die Post-mortem-Analyse einordnen. [16]

Bei der Live-Forensik beginnt eine Untersuchung bereits während des Vorfalls, um flüchtige Daten wie beispielsweise den Hauptspeicherinhalt, Informationen über bestehende Netzwerkverbindungen und gestartete Prozesse zu sammeln. [16]

Die Post-mortem-Analyse hingegen beginnt erst nach einem Vorfall und klärt diesen im Nachgang auf. Hierfür werden Datenträgerabbilder, sogenannte Images, erstellt und untersucht. Der Fokus liegt hierbei „auf der Gewinnung und Untersuchung von gelöschten, umbenannten sowie anderweitig versteckten und verschlüsselten Dateien von Massenspeichern.“ [16]

Aufgrund der eben genannten Charakteristika ist die Smartphone-Forensik als Post-mortem Analyse einzustufen. Für die Analyse wird ein Image des Smartphones erstellt, welches dann auf vorhandene bzw. nicht vorhandene Spuren hin untersucht wird.

Um das Ziel der forensischen Untersuchung, also die Beantwortung der definierten Fragen, zu erreichen, hat das BSI in seinem Leitfaden die Vorgehensweise einer forensischen Untersuchung in sechs Abschnitte unterteilt: [16]

- Strategische Vorbereitung
- Operationale Vorbereitung
- Datensammlung
- Untersuchung
- Datenanalyse
- Dokumentation

Die nachfolgenden Ausführungen zu den sechs Abschnitten beruhen auf der Quelle [16].

In der Phase der Strategischen Vorbereitung werden die für eine Analyse geeigneten Werkzeuge identifiziert und bereitgestellt. Die Auswahl der Werkzeuge mit den Kriterien dieser Auswahl muss dokumentiert werden.

Bei der Operationalen Vorbereitung beginnt die eigentliche Untersuchung. Hier wird bei einer ersten Bestandsaufnahme der Rahmen der forensischen Untersuchung festgelegt. Es wird entschieden, welche Daten gesichert werden sollen und wie diese Daten gesichert werden können. Dieser Abschnitt muss ebenfalls dokumentiert werden.

Mit Hilfe der in der Strategischen Vorbereitung ausgewählten Werkzeuge werden bei der Datensammlung die bei der Operationalen Vorbereitung festgelegten Daten gesichert. Dabei müssen integritätssichernde Maßnahmen[9] ergriffen werden. Die Authentizität sollte zusätzlich durch das Vier-Augen-Prinzip gesichert werden. Von dem erzeugten Image wird ein Hashwert berechnet, um eine nachträgliche Veränderung des Images feststellen zu können. Diese wird neben weiteren Aspekten in der prozessbegleitenden Dokumentation vermerkt.

Im Abschnitt der Untersuchung (auch Datenextraktion genannt) werden aus den gesammelten Daten die für die Untersuchung relevant erscheinenden Informationen extrahiert. Ebenfalls in diesem Abschnitt werden Daten gegebenenfalls in andere Formate konvertiert und die erstellten Images in die Analyseumgebung eingebunden. Dieser Arbeitsschritt ist ebenfalls in der prozessbegleitenden Dokumentation zu dokumentieren.

Bei der Datenanalyse werden mehrere Datenquellen zueinander in Verhältnis gesetzt. Hier sei als Beispiel die Korrelation zweier Log-Abschnitte genannt, um einen gemeinsamen Zeitstrahl zu erstellen. Auch in diesem Abschnitt werden die Tätigkeiten dokumentiert.

Im chronologisch letzten Abschnitt der Dokumentation wird auf Basis der bereits dokumentierten Abläufe und Ergebnisse aus dem Verlaufsprotokoll ein Ergebnisprotokoll generiert. Das Ergebnisprotokoll soll die gewonnenen Daten interpretieren und wird dann einem entsprechenden Adressatenkreis dargelegt.

[9] Einsatz eines Writeblockers. Dieser verhindert, dass Befehle, welche Datenveränderungen bewirken können, gefiltert werden.

3.2 Datenspeicher

In der IT-Forensik sind vor allem die Speichermedien der Geräte relevant, da diese die für die Sicherung und Untersuchung wichtigen Daten enthalten. Hierzu zählen unter anderem das Gerät selber, eine eventuell vorhandene externe Speicherkarte und die SIM-Karte. Auf jeder dieser Komponenten können Daten, welche unter Umständen für ein Verfahren wichtig sind, gespeichert sein.

3.2.1 Smartphone

Jedes Smartphone hat einen persistenten und einen nicht-persistenten Speicherbereich.

Persistente Speicher halten die Daten auch bei Abschaltung der Stromzufuhr, wie es der Fall ist, wenn das Smartphone im ausgeschalteten Zustand ist. Auf diesem Speicher befinden sich Systemdaten, Applikationsdateien und Benutzerdaten. [17] In heutigen Smartphones sind, Stand August 2021, Speichergrößen von bis zu 1 Terabyte (TB) möglich. [18]

„Aufgrund der persistenten Eigenschaft und der hohen Speicherkapazität stellt“ dieser Speicher die „wichtigste Komponente innerhalb einer forensischen Untersuchung im IT-Umfeld dar.“ [17]

Der Arbeitsspeicher (engl. Random Access Memory, kurz RAM) ist ein nicht-persistenter Speicher. Bei Abschaltung der Stromzufuhr gehen hier im Gegensatz zum persistenten Speicher sämtliche Daten verloren. Im RAM werden ausgeführte Programme und verwendete Daten zwischengespeichert, sodass diese Daten Rückschlüsse auf zuletzt ausgeführte Aktivitäten ermöglichen und relevante Informationen wie beispielsweise Benutzernamen, Passwörter oder Schlüssel zur Entschlüsselung enthalten. [17] Im August 2021 wurde das erste Smartphone mit 20 GB RAM vorgestellt. [19]

Um einen Verlust von Daten zu vermeiden, welche im RAM gespeichert sind, sollten diese Daten zuerst gesichert werden. Dies ist jedoch natürlich

nur möglich, wenn das Smartphone im eingeschalteten Zustand vorgefunden wurde. [17]

3.2.2 Speicherkarte

Viele Smartphones haben die Möglichkeit, den Speicherplatz mit Hilfe einer externen Speicherkarte zu erweitern. Die sogenannten SD-Karten (Secure Digital Memory Card) gibt es mit unterschiedlichen Speicherkapazitäten und Bauformen. Die Micro-SD-Karte ist die Bauform, welche üblicherweise in Smartphones verwendet wird. SD-Karten gibt es mittlerweile mit Speicherkapazitäten bis zu 1 TB. [20]

Die Speicherkarte stellt eine Erweiterung des im vorherigen Kapitel 3.2.1 beschriebenen persistenten Speichers dar und gehört somit ebenfalls zu der wichtigsten Komponente der forensischen Untersuchung.

3.2.3 SIM-Karte

Die SIM-Karte (englisch für Subscriber Identity Module) ist eine Chipkarte, welche den Nutzer eines mobilen Gerätes im Mobilfunknetz identifiziert. Nur wenn ein Nutzer mit der SIM-Karte im Mobilfunknetz authentifiziert ist, kann dieser auf die angebotenen Dienste des Netzbetreibers zugreifen.

SIM-Karten gibt es in verschiedenen Größen:

- Mini-SIM: 15 x 25 mm
- Micro-SIM: 12 x 15 mm
- Nano-SIM: 8,8 x 12,3 mm

Mittlerweile wird die klassische SIM-Karte immer mehr von der eSIM (embedded SIM) abgelöst, welche fest mit den Geräten verbunden ist und nicht manuell ausgetauscht werden kann. Änderungen der Daten bei einem Tarif- oder Anbieter-Wechsel werden dabei über ein Zugangsprofil vorgenommen. Durch die Nutzung einer eSIM können Geräte mit dem Internet verbunden werden, in welchen beispielsweise keinen Platz für eine herkömmliche SIM-Karte besteht, wie beispielsweise einer Smartwatch. [21]

Die SIM-Karte ist zum Schutz vor einer unberechtigten Nutzung mit einer veränderbaren vier- bis achtstelligen PIN, kurz für Personal Identification Number, geschützt. Sofern der Schutz aktiviert ist, wird diese PIN bei jedem Neustart des Smartphones abgefragt. Wird die PIN drei Mal falsch eingegeben, wird der Zugriff auf die SIM-Karte vorrübergehend gesperrt. Diese Sperrung kann unter Verwendung eines Personal Unblocking Keys (PUK), welcher durch den Mobilfunkprovider vergeben wird, aufgehoben werden. Nach zehnmaliger Falscheingabe des PUK wird die SIM-Karte dauerhaft gesperrt. [17]

Die SIM-Karte hat eine Speichergröße von 16 bis 512 Kilobyte (kB) und enthält neben temporären Daten auch das Telefon- und Notizbuch, einen SMS-Speicher und die zuletzt gewählten Telefonnummern. [17]

3.3 Betriebssysteme

Bei den Smartphone Betriebssystemen (engl. Operating System = OS) haben sich in den vergangenen Jahren die beiden großen Systeme Android und iOS durchgesetzt. Während in Japan und den Vereinigten Staaten von Amerika iOS bevorzugt wird, liegt in Deutschland das Betriebssystem Android deutlich vorne, wie nachfolgende Grafik verdeutlicht. [22]

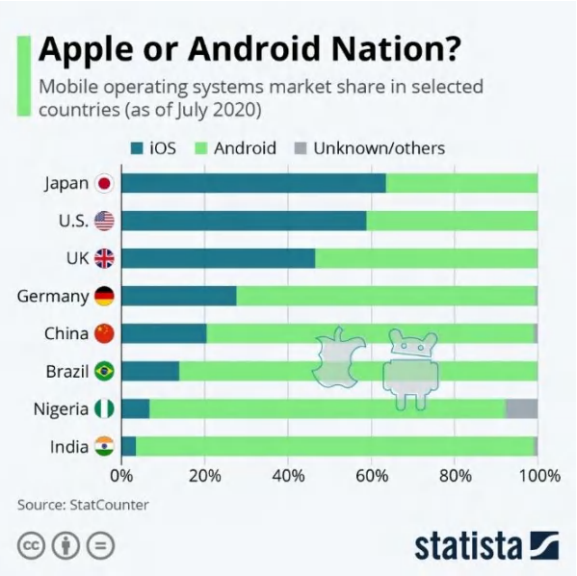


Bild 8: Vergleich iOS – Android [22]

Mit dem Betriebssystem Android bietet Google ein Open Source System, welches auf Offenheit und Anpassbarkeit setzt. Apple hingegen ist mit seinem Betriebssystem auf Sicherheit und Geschlossenheit bedacht.

Tabelle 1: Vergleich Android - iOS [23] [24] [25]

	Android	**iOS**
Entwickler	Open Handset Alliance	Apple Inc.
Veröffentlichung	23. September 2008	29. Juli 2007
OS-Familie	Linux	OS X, Unix
Programmiersprache	C, C++, Java	C, C++, Objective-C
Neuste Version	12 (Snow Cone)	15.1
Anpassbarkeit	Viel, fast alles kann geändert werden	Limitiert, falls kein Jailbreak
Plattform	Open-Source	Geschlossen, jedoch mit Open-Source Komponenten
Verfügbare Sprachen	> 100	40
App Store	Google Play Store	Apple App Store
Anzahl Apps (1. Quartal 2021)	> 3,4 Millionen	> 2,2 Millionen
Updates	Uneinheitlich, hängt vom Gerätehersteller ab; Bsp.: Samsung = drei neue Android Versionen und vier Jahre Sicherheitspatches	Bis zu sechs Updates auf iOS-Generationen

3.4 Datenextraktion

Für die Erstellung eines Smartphone-Images wird häufig der Zugriff über sogenannte Wartungs- und Service-Modi gewählt. Diese sind von den Herstellern für den Zugriff in einem Service-Fall vorgesehen.

Welche Art der Extraktion gewählt wird, hängt von der technischen Machbarkeit, der technischen Ausgangssituation und den vorliegenden Informationen über den Beschuldigten ab. Das nachfolgende Bild stellt eine Übersicht über die drei wichtigsten Datenextraktionsarten dar.

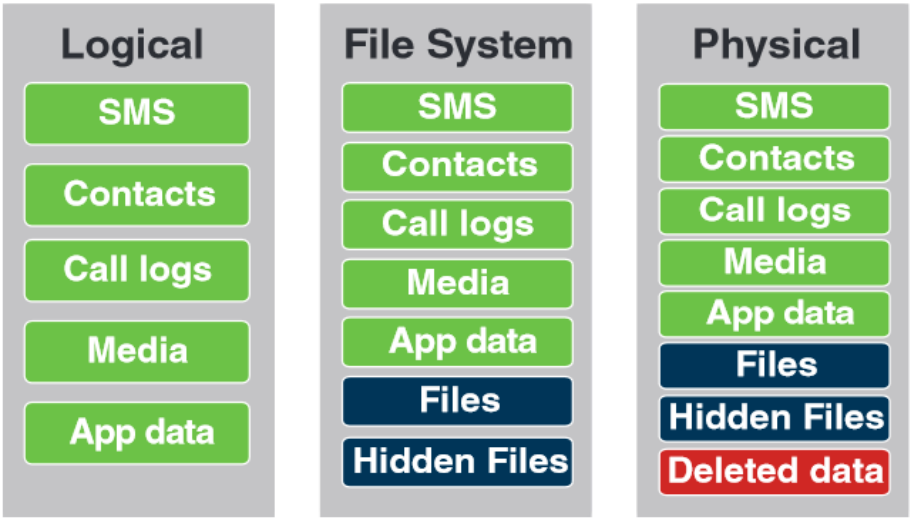


Bild 9: Übersicht Datenextraktionen [26]

In den nachfolgenden Unterkapiteln werden die einzelnen Extraktionsarten vorgestellt, deren Funktionsweise beschrieben und welche Ergebnisse erzielt werden können.

3.4.1 Logische Extraktion

Die Logische Extraktion wird mit Hilfe einer API, Abkürzung für Application Programming Interface, durchgeführt, welche beim Gerätehersteller erhältlich ist. APIs ermöglichen eine Kommunikation der Apps mit dem Betriebssystem. Dieses Verfahren wird ebenfalls für die Datensicherung verwendet, um vorhandene Nutzerdaten wie beispielsweise Anrufe, SMS und weitere Daten über ebendiese Datenschnittstelle sichern zu können. Dabei führt die Forensik-Software schreibgeschützte API-Aufrufe durch, um Daten vom Gerät anzufordern. Das Gerät antwortet auf gültige API-Anfragen und extrahiert die angefragten Inhaltselemente. Nachfolgend wird eine solche Anfrage grafisch dargestellt: [26]

Bild 10: Anfrage einer Logischen Extraktion: Gültige Anfrage [26]

Wird eine ungültige API-Anfrage gesendet, so verweigert das Gerät die Anfrage, wie im Folgenden grafisch dargestellt: [26]

Bild 11: Anfrage einer Logischen Extraktion: Ungültige Anfrage [26]

Bei der Logischen Extraktion handelt es sich um die schnellste und am meisten unterstützte Extraktionsmethode. Die Daten werden in lesbarer Form dargestellt, jedoch ist sie auf den Inhaltsumfang beschränkt, welchen der jeweilige Anbieter der API zur Verfügung stellt. Beispielsweise können keine Bilder gesichert werden, welche mit einer Drittanbieter-App aufgenommen werden, da diese nicht im Standardordner gespeichert werden. [27]

3.4.2 Dateisystem / Erweiterte Logische Extraktion

Der Hauptunterschied zwischen der Logischen Extraktion und der Dateisystem / Erweiterten Logischen Extraktion ist der direkte Zugriff der forensischen Software auf die Dateien im internen Speicher eines Mobilgerätes, anstatt der Kommunikation für jeden Datentypen über die API.

Mit Hilfe dieser Sicherungsmethode kann neben den Sicherungsinhalten der Logischen Extraktion auch die Verzeichnisstruktur gesichert werden. Diese Daten enthalten unter anderem Datenbankdateien, Systemdateien und Protokolle. Die meisten Apps speichern ihre Informationen in Datenbanken.

Löscht ein Benutzer Daten auf seinem Mobilgerät, so wird der entsprechende Eintrag in der Datenbank als gelöscht markiert und ist dadurch für den Benutzer nicht mehr sichtbar. Die Daten in der Datenbank sind jedoch nach wie vor intakt und können so lange wiederhergestellt werden, bis die Daten entweder durch eine routinemäßige Bereinigung oder durch Überschreiben des Datenbankeintrages entfernt werden. Erst dann sind die Daten unwiederbringlich verloren. [27]

Die gesicherten Daten enthalten folglich die Rohdaten. Diese müssen dekodiert werden, um die Daten lesen und analysieren zu können. Verschiedene Hersteller von forensischer Software setzen dies bereits in ihrer Software um, sodass die Daten als Rohdaten - wie sie im Gerätespeicher gespeichert sind - und zusätzlich in einem für Menschen lesbaren Format dargestellt werden. [27]

Das Bild 12 zeigt eine Anfrage bei einer Dateisystem Extraktion. Das Mobilgerät wird angefragt und gibt als Antwort auf diese Anfrage das Dateisystem zur weiteren Verarbeitung zurück.

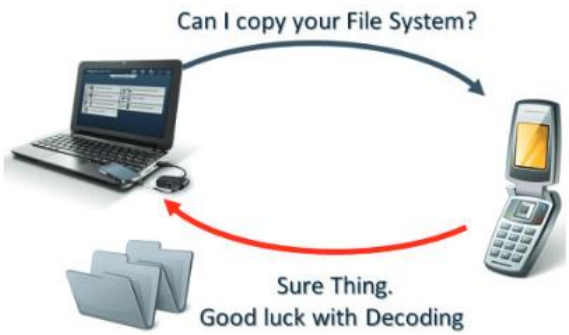


Bild 12: Anfrage einer Dateisystem Extraktion: Dekodierung [26]

3.4.3 Physikalische Extraktion

Die umfangreichste Sicherungsmethode, welche jedoch von den Geräten am wenigsten unterstützt wird, ist die Physikalische Extraktion. Dies ist darin begründet, dass der vollständige Zugriff auf den internen Speicher vom Betriebssystem und den Sicherheitsmaßnahmen der Mobilgerätehersteller abhängt.

Es handelt sich hierbei um eine Kopie der Daten auf Bit-Ebene, so wird ein vollständiges Systemabbild Bit-für-Bit erstellt. Die Voraussetzung für diese Extraktion ist jedoch der direkte Zugang zur Hardware des Systems. Neben den bereits durch die anderen beiden Extraktionsarten bekannten Daten, können bei der Physikalischen Extraktion zusätzlich gelöschte Daten, welche außerhalb von Datenbanken gespeichert sind, wiederhergestellt werden. Hierbei kann es sich beispielsweise um Bilder, Videos und E-Mails handeln. [27]

Zusätzlich werden Daten gesichert, welche das Mobilgerät ohne Benutzeraktion und teilweise auch ohne Benutzerwissen sammelt, wie beispielsweise Wi-Fi Netzwerke, GPS-Standorte, den Webverlauf, Exif-Daten von Bildern und Systemdaten.

Auch hier müssen die Daten wie bei der Dateisystem Extraktion dekodiert werden. [26]

3.5 Datenarten

Das Auslesen von Mobilgeräten ergibt eine Vielzahl an Informationen, die für Ermittlungsverfahren relevant sein können. Je nach Art des Ermittlungsverfahrens können hierbei verschiedene Datenarten interessant sein. Neben im Gerät eingespeicherten Rufnummern und Chatverläufen sind beispielsweise auch Bilder und Videos wichtig oder aber eingegebene Suchverläufe und Standorte.

Für diese Masterthesis sind nicht alle Datenarten auf Smartphones relevant, daher wird in den folgenden Unterkapiteln nur auf die für die Thesis wichtigen Aspekte eingegangen.

3.5.1 Daten von Apps

Der Begriff App wird vom englischen Wort Application abgeleitet und bezeichnet eine Anwendungssoftware für ein Mobilgerät. Eine Anwendungssoftware ist ein zusätzliches Programm, welches jedoch nicht für die Funktion eines Systems selbst relevant ist.

Damit Apps Daten ablegen und diese wieder auslesen können, werden Daten in Datenbanken gespeichert. Auch im sogenannten Cache, dem Zwischenspeicher, legen viele Apps ihre Daten ab, um diese schneller laden zu können. Neben diesen zwischengespeicherten Daten werden auch temporäre Daten dort abgelegt.

Bei diesen Daten handelt es sich unter Umständen um Daten, welche durch Nutzereingaben entstanden sind. Die Daten sind daher für Ermittlungsverfahren äußerst wertvoll.

3.5.2 Standortdaten

Standortdaten gehören eigentlich zu den Daten aus Apps, werden hier jedoch aufgrund der Thematik der Masterthesis separat betrachtet. Die auf dem Mobilgerät gespeicherten Standortdaten können auf verschiedene Art und Weise generiert werden.

Wofür in vergangenen Tagen ein separates Navigationsgerät verwendet wurde, kann in Zeiten des Smartphones die Navigations-App verwendet werden. Die Eingabe der Ziele und auch die Routenführung sind Standortdaten, die mit Hilfe forensischer Software ausgelesen werden können.

Ebenfalls wäre es möglich, dass Eingaben aus Suchen auf dem Gerät gespeichert werden, ohne dass das Gerät zu diesem Zeitpunkt an dem angegebenen Ort war. Dies hat jedoch zur Folge, dass die Entstehung der Standortdaten genau betrachtet werden muss.

Diese Aspekte der Standortdaten sollen mit Hilfe von Testszenarien in den beiden folgenden Kapiteln 4 und 5 definiert, analysiert und interpretiert werden.

3.5.3 Metadaten aus Bildern

Digitale Fotos enthalten weit mehr Daten, als das reine Bild dem Betrachter zeigt. Die sogenannten Metadaten speichern Informationen über das generierte Bild. Ein Standardformat ist das Exchangeable Image File Format, kurz Exif. Entwickelt wurde das Exif-Format durch die japanische Kamera-Industrie und ermöglichte es erstmals, Metadaten in Bilddateien der Formate JPEG (Joint Photographic Experts Group) und TIFF (Tagged Image File Format) hinzuzufügen. [28]

Von fast allen Smartphone-Herstellern werden nachfolgende Exif-Daten unterstützt [28]:

- Datum und Uhrzeit
- Blende, Belichtungszeit, Brennweite, ISO-Wert[10], Blitzinformationen
- Informationen zum Fotografen und zum Urheberrecht
- Vorschaubild (Thumbnail)
- Geo-Informationen und Kamera-Winkel

[10] Der ISO-Wert (kurz für International Organization for Standardization) gibt an, wie lichtempfindlich ein Bildsensor ist. Dieser kann bei digitalen Geräten in den Einstellungen geändert werden und kann dadurch den aktuellen Lichtverhältnissen angepasst werden. [33]

4 Testszenarien

Die nachfolgenden Unterkapitel sollen einen Überblick über den grundsätzlichen Versuchsaufbau, die Definition der Testszenarien, sowie eine Beschreibung der forensischen Software und der zu untersuchenden Apps geben.

4.1 Versuchsaufbau

Die definierten Testszenarien werden auf einem Android-basierten und einem iOS-basierten Smartphone durchgeführt. Bei den Geräten handelt es sich um ein Samsung Galaxy S8 64GB und ein Apple iPhone 8 64GB, welche in folgender Tabelle 2 gegenübergestellt werden.

Tabelle 2: Vergleich Testgeräte [29] [30]

	Samsung Galaxy S8	**Apple iPhone 8**
Modellnummer	SM-G950F	A1905 (MQ6G2ZD/A)
Betriebssystem	Android	iOS
Betriebssystem-Version	9 Sicherheitspatch 1. August 2019	14.4.1
Seriennummer	RF8J904SLDP	C7CWHQ2NJC67
TAC[11]	35904008	35949608
Veröffentlichung	April 2017	September 2017
Navigation	GPS, A-GPS, Galileo, Glonass, BeiDou	GPS, A-GPS, Glonass

Die Auswahl der Smartphone-Modelle erfolgte unter Einbeziehung der Möglichkeiten zur Extraktion der Daten. Um möglichst viele Daten in die

[11] TAC = Type Allocation Code: erste 8 Ziffern der IMEI zur Identifizierung eines Gerätes

Analyse und Interpretation der Testszenarien einbeziehen zu können, wurden daher zwei bereits etwas ältere Smartphone-Modelle ausgewählt, welche zuverlässig einer Datenextraktion (siehe Kapitel 3.4) unterzogen werden können.

Vor der Durchführung der Testszenarien werden die Smartphones jeweils auf Werkseinstellung zurückgesetzt, sodass ein Testszenario immer mit der Ersteinrichtung beginnt. Dies hat den Vorteil, dass keine Daten von vorherigen Testszenarien auf den Smartphones gespeichert sind und das Ergebnis verfälschen könnten.

Die Testszenarien benötigen unterschiedliche Anwendungen, welche für das jeweilige Szenario über den Apple App Store bzw. Google Play Store heruntergeladen werden. Mit den bereits zuvor angelegten Accounts erfolgt eine Anmeldung in der jeweiligen Anwendung.

Die Testszenarien werden gemäß der Definition aus Kapitel 4.2 durchgeführt. Im Anschluss wird das Gerät mit Hilfe der forensischen Software ausgelesen. Das erzeugte Image wird im Rahmen der Evaluation (siehe Kapitel 5) auf Geodaten hin überprüft. Hierbei werden nur die im Kontext zur Fragestellung hin erzeugten Geodaten betrachtet.

Geodaten, welche nicht im Zusammenhang mit der jeweiligen verwendeten App erzeugt wurden, werden - soweit nicht anders angegeben – nicht in die Analyse und Interpretation miteinbezogen.

Eine verallgemeinerte Beschreibung einer als sinnvoll erachteten Vorgehensweise bei der Analyse von Images mit UFED kann der Anlage A entnommen werden.

4.2 Definition der Testszenarien

Die Testszenarien mit einer kurzen Erläuterung werden in nachfolgenden Unterkapiteln beschrieben.

4.2.1 Speicherung von Geodaten

Werden bei einem Smartphone Standortdaten aktiviert, so ist es denkbar, dass das Gerät Standortdaten ohne Zutun des Nutzers speichert. Dieses Testszenario soll zeigen, ob das Gerät in einem solchen Fall Standortdaten speichert, welche dann gegebenenfalls analysiert werden. Hierfür werden die Testgeräte nach der Einrichtung eine Zeit lang ohne aktive Nutzung beiseitegelegt und anschließend für die Analyse ausgelesen.

4.2.2 Genauigkeit von Geodaten: Metadaten von Bildern

Werden Bilder auf dem Smartphone aufgenommen besteht die Möglichkeit diesen die Standortinformationen hinzuzufügen. Hier soll der gespeicherte Standort mit dem tatsächlichen Standort der Aufnahme des Bildes verglichen werden.

4.2.3 Genauigkeit von Geodaten: Google Standortverlauf

Im Google Standortverlauf werden Geodaten mit einer Angabe zur Genauigkeit gespeichert. Welche Bedeutung diese Werte allerdings genau haben ist nicht bekannt. Durch einen Test soll herausgefunden werden, wie sich der Wert der Genauigkeit zur tatsächlich zurückgelegten Strecke verhält.

4.2.4 Navigation

Ein Testgerät wird zur Navigation mit der auf dem Gerät bereits installierten Karten-App verwendet. Hierbei wird eine Route berechnet und diese Strecke zum Zielort zurückgelegt.

Welche Daten sind danach auf dem Gerät vorhanden? Können die Daten einen sicheren Rückschluss ermöglichen, dass eine Navigation tatsächlich stattgefunden hat?

4.2.5 Suche: Google

Dieses Testszenario beschäftigt sich mit der Suchmaschine Google und der Erzeugung von Geodaten aufgrund von Suchergebnissen. Wenn in Google nach einem Ort gesucht und dieser in Google Maps (bei Samsung in der App, bei Apple über die Webseite) angezeigt wird, können diese Standorte auf dem Gerät festgestellt werden?

Zusätzlich wird auf der Karte in Google Maps ein weiterer Ort ausgewählt, sodass Google Maps zu diesem Standort Informationen anzeigt. Können diese Daten festgestellt werden?

4.2.6 Versand von Geodaten: E-Mail

Ein Bild, welches Standortdaten enthält, wird per E-Mail verschickt. Über die App des E-Mail Providers wird die E-Mail geöffnet.

- Variante 1: Anzeige des Bildes als Vorschau
- Variante 2: Herunterladen des Bildes auf das Gerät

Können die Geostandorte auf dem empfangenden Gerät festgestellt werden?

4.2.7 Versand von Geodaten: WhatsApp

Ein Bild, welches Standortdaten enthält, wird per WhatsApp verschickt. Können die Geostandorte auf dem empfangenden Testgerät festgestellt werden?

4.2.8 Versand von Geodaten: Facebook Messenger

Ein Bild, welches Standortdaten enthält, wird per Facebook Messenger verschickt.

- Variante 1: Das Bild wird angesehen
- Variante 2: Das Bild wir heruntergeladen

Können die Geostandorte auf dem Gerät festgestellt werden?

4.2.9 Versand von Geodaten: SnapChat

Ein Snap, welcher mit einem Standort getaggt wurde, wird an einen Chatpartner versendet. Kann der Standort auf dem sendenden Testgerät gesichert werden?

4.2.10 Upload von Geodaten: Facebook

Ein Bild, welches Standortdaten enthält, wird als Statusbeitrag in Facebook hochgeladen. Können die Geostandorte vom Bild in Bezug auf Facebook auf dem Gerät festgestellt werden?

4.2.11 Standortmarkierung: Facebook

Wird ein Status-Beitrag auf Facebook erstellt, kann ein Standort hinzugefügt werden. Dieser Standort kann auf zwei Arten erzeugt werden:

- Variante 1: Manuelle Eingabe des Ortes
- Variante 2: Eingabe mit Hilfe des Ortungsdienstes

Mit Hilfe dieser Varianten soll festgestellt werden, ob und wie die angegebenen Standorte in den ausgelesenen Daten enthalten sind.

4.2.12 Standortfreigabe: Facebook Messenger

Über den Messenger von Facebook kann der aktuelle Standort mit einer weiteren Person geteilt werden.

- Variante 1: Testgerät ist Empfänger des Standortes
- Variante 2: Testgerät ist Sender des Standortes

Die durch die Testszenarien erhaltenen Daten sollen auf die Geodaten überprüft werden. Sind diese auf dem Gerät enthalten und kann zwischen dem Sender und Empfänger unterschieden werden?

4.2.13 Standortfreigabe: WhatsApp

Im Messenger WhatsApp kann der Standort an einen Chatpartner gesendet werden.

- Variante 1: Testgerät ist Empfänger des Standortes
- Variante 2: Testgerät ist Sender des Standortes

Können die Standorte in den ausgelesenen Daten festgestellt werden und ist eine Unterscheidung zwischen dem Sender und Empfänger möglich?

4.2.14 Live-Standortfreigabe: WhatsApp

Im Messenger WhatsApp kann der Standort im Live-Modus für eine Stunde oder andere definierbare Zeiträume mit einem Chatpartner geteilt werden.

- Variante 1: Testgerät ist Empfänger des Standortes
- Variante 2: Testgerät ist Sender des Standortes

Können die Standorte auf den Testgeräten festgestellt werden? Und ist eine Unterscheidung möglich, dass diese Daten bei Variante 1 von einem fremden Gerät erzeugt und gesendet wurden?

4.3 Forensik-Software

Um digitale Geräte und die darauf enthaltenen Daten analysieren zu können, müssen diese mit Hilfe entsprechender Forensik-Software ausgelesen werden. Hier gibt es sowohl kommerzielle, als auch Open-Source Produkte.

Für die vorliegende Masterthesis wurde die Software Cellebrite UFED, kurz für Universal Forensic Extraction Device, des israelischen Herstellers Cellebrite gewählt. Cellebrite verspricht für seine Software eine Einsatzmöglichkeit nicht nur bei Mobilgeräten, sondern auch bei Drohnen, GPS-Geräten und mehr. Muster-, Kennwort- oder PIN-Sperren auf Geräten, sowie die Verschlüsselungen von gängigen Android- und iOS-Geräten können mit Hilfe von UFED umgangen werden. [31]

Nach der Datensammlung mit Hilfe der Software UFED werden die gewonnenen Geodaten zur Visualisierung in einem GIS dargestellt. Die Software QGIS ist eine Open-Source-Software, welche Geodaten anzeigen, bearbeiten und analysieren kann. [32]

Tabelle 3: Verwendete Versionen der Software

Software	Version
UFED	7.48.1.3
QGIS	3.20.2

4.4 Zu untersuchende Apps

Im Rahmen dieser Thesis sollen verschiedene mobile Anwendungen analysiert werden. Die nachfolgenden Unterkapitel geben einen sehr kurzen Überblick über die Anwendungen und die Einsatzgebiete.

4.4.1 Facebook

Bei der Anwendung Facebook handelt es sich um ein soziales Netzwerk, bei welchem private Profile oder Seiten für Firmen und Künstler, sowie für Gruppen mit gemeinsamen Interessen erstellt werden können.

Nachfolgende Tabelle zeigt eine kurze Zusammenfassung der wichtigsten Zahlen von Facebook.

Tabelle 4: Facebook [33] [34]

Anwendung	**Facebook (Eigenschreibweise: facebook)**
Logo	facebook
Kategorie	Soziales Netzwerk & Messenger
Hersteller	Facebook Inc.
Gründungsjahr	2004
Nutzer	Q2/2021: 3,51 Milliarden

4.4.2 WhatsApp

Bei der Anwendung WhatsApp handelt es sich um einen Messenger, bei welchem Nachrichten versendet und empfangen, Videotelefonate sowie Audiotelefonate durchgeführt werden können.

Nachfolgende Tabelle zeigt eine kurze Zusammenfassung der wichtigsten Zahlen von WhatsApp.

Tabelle 5: WhatsApp [35] [36]

Anwendung	**WhatsApp**
Logo	
Kategorie	Messenger
Hersteller	Facebook Inc.
Gründungsjahr	2009
Nutzer	2021: 2 Milliarden

4.4.3 Snapchat

Bei der Anwendung Snapchat handelt es sich um einen Messenger, bei welchem Nachrichten, Bilder und Videos versendet werden können. Eine Besonderheit besteht in der Löschung von Nachrichten. Diese löschen sich, je nach Einstellung des Benutzers, direkt nach dem Lesen bzw. nach 24 Stunden von alleine.

Nachfolgende Tabelle zeigt eine kurze Zusammenfassung der wichtigsten Zahlen von Snapchat.

Tabelle 6: Snapchat [37] [38]

Anwendung	**Snapchat**
Logo	
Kategorie	Messenger
Hersteller	Snap Inc.

Gründungsjahr	2011
Nutzer	Q2/2021: 293 Millionen

4.4.4 Navigation

Bei Google Maps und Apple Maps handelt es sich um Anwendungen für Karten und Navigation. Für die Durchführung der Navigation kann hierbei ausgewählt werden, wie die Strecke zurückgelegt werden soll: per Auto, zu Fuß, mit dem ÖNPV, per Fahrrad oder per Personenbeförderung. Die Routen werden mit Informationen in Echtzeit angereichert, sodass die aktuelle Verkehrslage, aber auch beispielsweise Busfahrpläne angezeigt werden.

Apple Maps beschreibt auf seiner Webseite, dass Stand Oktober 2021, bald zusätzlich Routen für E-Fahrzeuge berechnet werden können. In diese Route werden der aktuelle Ladestand des Akkus und unter anderem auch Höhenunterschiede berücksichtigt, woraus dann automatisch Ladestopps berechnet werden sollen. [39]

Nachfolgende Tabelle zeigt eine kurze Zusammenfassung der wichtigsten Zahlen von Google Maps.

Tabelle 7: Google Maps [40] [41]

Anwendung	**Google Maps**
Logo	
Kategorie	Navigation
Hersteller	Google LLC
Gründungsjahr	Google Maps: 2005
Nutzer	2021: > 1 Milliarde

Nachfolgende Tabelle zeigt eine kurze Zusammenfassung der wichtigsten Zahlen von Apple Maps.

Tabelle 8: Apple Maps [42] [43]

Anwendung	**Apple Maps**
Logo	
Kategorie	Navigation
Hersteller	Apple
Gründungsjahr	2012
Nutzer	Dezember 2020: „hundreds of millions“

4.4.5 GMX

Bei GMX handelt es sich um einen Anbieter von E-Mail-Diensten, welcher in drei Varianten zur Verfügung steht – zwei gebührenpflichtige und ein gebührenfreier Tarif. Bei allen drei Varianten steht dem Nutzer Cloud-Speicher zur Verfügung, welcher gegen einen Aufpreis erweitert werden kann.

Nachfolgende Tabelle zeigt eine kurze Zusammenfassung der wichtigsten Zahlen von GMX.

Tabelle 9: GMX [44] [45] [46]

Anwendung	**GMX**
Logo	GMX
Kategorie	E-Mail
Hersteller	1&1 Mail & Media GmbH
Gründungsjahr	1997
Nutzer	2020: 10,84 Millionen

5 Analyse und Interpretation

Die Ergebnisse sowie deren Interpretation au den im vorangegangenen Kapitel beschriebenen Testszenarien werden in diesem Kapitel dargestellt. Hierfür wurden die beiden Testgeräte für jedes Testszenario und dessen Varianten jeweils auf Werkseinstellungen zurückgesetzt und neu eingerichtet. Die Einrichtung erfolgte, wenn nicht anders in den Unterkapiteln angegeben, ohne die Erlaubnis für den Zugriff auf die Standortfreigabe.

Die Testgeräte wurden mit UFED gesichert. Hierbei wurde das Samsung-Testgerät mittels Physikalischer Extraktion und das Apple-Testgerät mit Hilfe der Erweitert Logischen Extraktion ausgelesen.

5.1 Speicherung von Geodaten

Wie in Kapitel 4.2.1 beschrieben, soll dieses Testszenario automatisch generierte Geodaten analysieren. Diese wurden erzeugt, ohne dass durch den Nutzer Handlungen durchgeführt wurden.

Nach erfolgter Durchführung und Analyse konnte festgestellt werden, dass das Apple-Testgerät, im Gegensatz zum Samsung-Testgerät, Daten gespeichert hat:

Tabelle 10: Speicherung von Geodaten

	Apple	**Samsung**
Geodaten	ja	nein

5.1.1 Analyse Apple iPhone 8

Im Image des Apple-Testgerätes konnten 731 Datensätze mit Standortdaten festgestellt werden. Davon liegen 699 dieser Standorte in Europa[12],

[12] Die grafische Darstellung der Datensätze in Europa als Gesamtübersicht sind der Anlage B1 zu entnehmen.

15 Datensätze liegen an den Geokoordinaten Längengrad 0 und Breitengrad 0. Bei den verbleibenden 17 Standortdaten konnten keine zugehörigen Geokoordinaten festgestellt werden, weshalb diese nicht auf einer Karte dargestellt werden können. Es ergibt sich nachfolgendes grafisches Bild aller Geokoordinaten, welche im Testgerät Apple iPhone 8 festgestellt werden konnten:

Bild 13: Vorhandene Standorte

Die vorhandenen Standorte werden durch UFED in vier Kategorien eingeteilt:

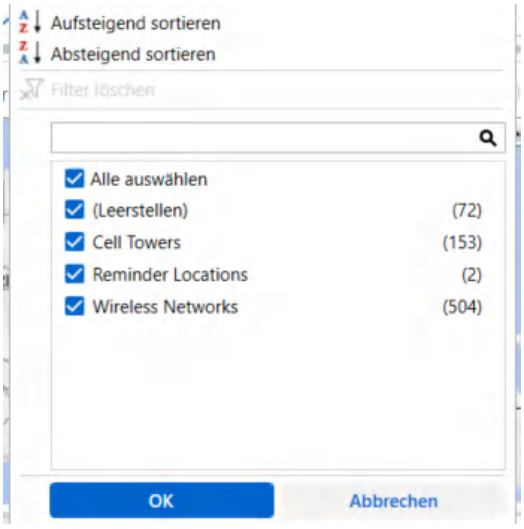


Bild 14: Standort-Kategorien

5.1.1.1 Kategorie „(Leerstellen)“

In der Kategorie „(Leerstellen)“ sind Standorte enthalten, welche durch UFED als Typ „Visited“ und der Quelle „Native Locations“ angegeben werden. Diese Daten liegen in der Datenbank Cache.sqlite-wal unter nachfolgendem Pfad:

`Apple_iPhone 8 (A1905).zip/root/private/var/mobile/Library/Caches/com.apple.routined/Cache.sqlite-wal`

Über die Manpage[13] kann herausgefunden werden, dass sich hinter „routined“ ein benutzerspezifischer Dienst befindet, welcher die historischen Standorte des Benutzers lernt und somit zukünftige Besuche von Standorten vorhersehen kann.

Die hier enthaltenen Standorte liegen alle im Umkreis des tatsächlichen Standortes, welcher in nachfolgendem Bild mit einem roten Kreuz markiert wurde.

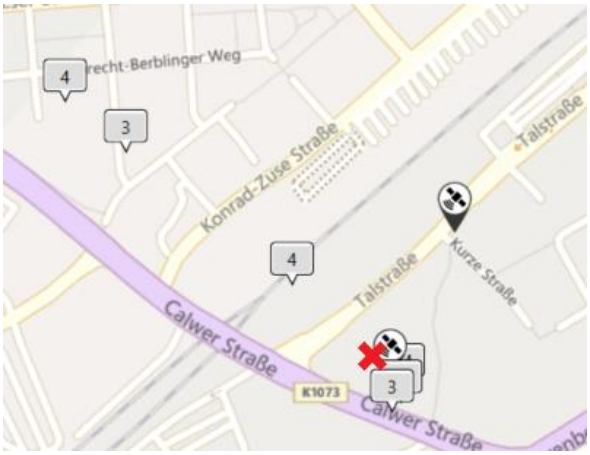


Bild 15: Standorte Kategorie „(Leerstellen)“

Bei der Betrachtung des zugehörigen Genauigkeits-Wertes lässt sich erkennen, dass die Werte teilweise, obwohl sie auf der Karte nebeneinander

[13] Die Manpage ist eine textbasierte Eräuterung bzw. Anleitung eines Befehls, welche über die Kommandozeile aufgerufen werden kann.

liegen, abweichen. So wird eine Geokoordinate mit einer Abweichung von 16 angegeben, eine weitere mit einer Abweichung von 23, obwohl sie nebeneinander liegen. Ob es für diese Werte eine Maßeinheit gibt, kann nicht festgestellt werden. Nimmt man die angegebenen Werte als Wert in Meter, so kann festgestellt werden, dass dies mit dem Abstand zum tatsächlichen Standort nicht übereinstimmt.

5.1.1.2 Kategorie „Cell Towers“

Die Kategorie „Cell Towers“ lässt vermuten, dass Apple hier Standorte von Funkzellmasten speichert. Diese Daten liegen in der Tabelle „LteCellLocation“ der Datenbank Cache_encryptedB.db-wal unter nachfolgendem Pfad:

`Apple_iPhone 8 (A1905).zip/root/private/var/root/Library/Caches/locationd/cache_encryptedB.db-wal`

Hinter “locationd” verbirgt sich ein Dienst, welcher den geografischen Standort beinhaltet und die Autorisierung für Apps verwaltet, welche eine Standortaktualisierung anfordern.

Die hier enthaltenen Standorte liegen nicht nur im Umkreis des tatsächlichen Standortes, wie das nachfolgende Bild zeigt:

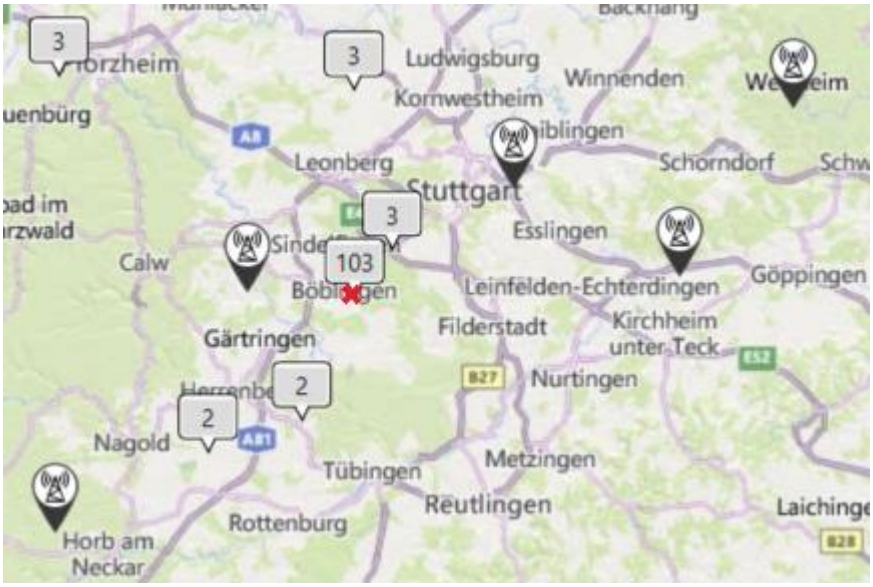


Bild 16: Standorte Kategorie „Cell Towers“

Aus dem Tabellennamen „LteCellLocation“ der Quelldatei wird ersichtlich, dass es sich hierbei um Funkzellen des Mobilfunkstandards LTE (kurz für Long Term Evolution) handeln soll.

Zwischen dem tatsächlichen Standort des Gerätes und dem am weitesten entfernt liegenden CellTower rechts oben bei Welzheim liegen ca. 50 Kilometer Luftlinie. Die Reichweite von Funkzellen wird unter anderem durch geografische Gegebenheiten beeinflusst. So liegen in diesem Fall mehrere größere Städte, ein Höhenunterschied von 40 Meter und mehrere Erhebungen im Gelände zwischen den beiden Orten. Es dürfte sich daher bei den in dem Image enthaltenen Daten um keine zu diesem Zeitpunkt empfangenen Funkzellen handeln.

Die im Image enthaltenen Funkzellen und deren Standorte wurden auf den angegebenen Standort überprüft. Hierbei wurde festgestellt, dass die Geokoordinaten nicht mit Standorten von Funkmasten übereinstimmen. Dies kann mit Hilfe einer sogenannten EMF-Karte (Elektromagnetische Felder), welche durch die BNetzA (Bundesnetzagentur) bereitgestellt wird, abgeglichen werden. Das nachfolgende Bild zeigt einen Ausschnitt aus der EMF-Karte im Bereich Böblingen. Die vorhandenen Funkmasten sind hierbei mit einem blauen Dreieck mit einem darin enthaltenen weißen „i“ gekennzeichnet. In dieses Bild wurden die ungefähren Standorte der ausgelesenen Geodaten von Funkmasten in diesem Bereich mit einem roten „x“ eingezeichnet.

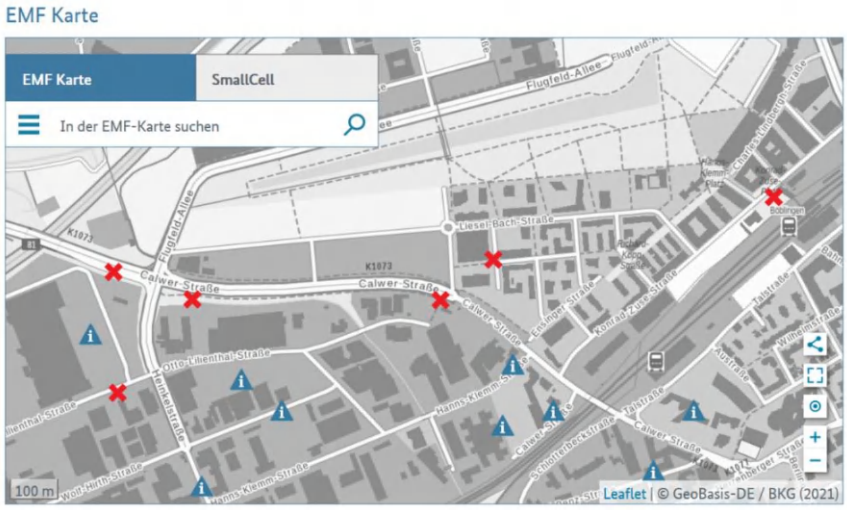


Bild 17: EMF-Karte

5.1.1.3 Kategorie „Reminder Locations“

In der Kategorie „Reminder Locations“ liegen nur zwei Datensätze vor. Hier kann jedoch festgestellt werden, dass diese sehr genau dem tatsächlichen Standort entsprechen.

Diese Daten liegen in der Datenbank consolidated.db-wal in der Tabelle „Fences“ (dt. Zäune) unter nachfolgendem Pfad:

`Apple_iPhone 8 (A1905).zip/root/private/var/root/Library/Caches/locationd/consolidated.db-wal`

Bei dem Datensatz könnte es sich um Geodaten aus der App „Reminder“ handeln, welche auch standortbasierte Alarme auslösen kann.

Bild 18: Standorte Kategorie „Reminder Locations“

5.1.1.4 Kategorie „Wireless Networks“

Die Kategorie „Wireless Networks“ lässt vermuten, dass Apple hier Standorte von WLANs speichert. Diese Daten liegen wie die „CellTowers“ in der Datenbank Cache_encryptedB.db-wal, jedoch in der Tabelle „WifiLocation“, unter nachfolgendem Pfad:

`Apple_iPhone 8 (A1905).zip/root/private/var/root/Library/Caches/locationd/cache_encryptedB.db-wal`

Die hier enthaltenen Standorte liegen im weitläufigeren Umkreis des tatsächlichen Standortes, wie das nachfolgende Bild zeigt:

Bild 19: Standorte Kategorie „Wireless Networks“

Inwieweit die Daten der WLANs korrekt sind, wird im Rahmen dieser Masterthesis aber nicht näher untersucht.

5.1.2 Analyse Samsung Galaxy S8

Auf dem Testgerät Samsung Galaxy S8 konnten keine Geodaten festgestellt werden. Eine Bestimmung des Standortes zum Testzeitpunkt ist daher anhand der Daten des Images nicht möglich.

5.1.3 Interpretation

Mit Hilfe der Daten aus dem Apple-Testgerät kann eine Eingrenzung des Standortes vorgenommen werden. Es kann jedoch nur ein größerer Bereich festgelegt werden, in welchem sich das Gerät zum jeweiligen Zeitpunkt befunden haben dürfte. Generell lässt sich hierbei sagen, je mehr Standorte

vorhanden sind, desto größer ist die Wahrscheinlichkeit, dass sich das Gerät in diesem Bereich befunden hat, wie auch in den Ergebnissen des Kapitels 5.4.1 zu sehen ist.

Besonders wertvoll scheinen in den Daten bei Apple-Geräten die Werte der Kategorie „Reminder Location“ zu sein, da diese einen ziemlich exakten Wert anzeigen, was ebenfalls die Daten der Kategorie „Reminder Locations“ aus Kapitel 5.4.1 zeigen. Diese Vermutung müsste jedoch mit weiteren Tests belegt werden.

5.2 Genauigkeit von Geodaten: Metadaten von Bildern

Die Genauigkeit von Geodaten ist, wie in Kapitel 2.3 beschrieben, abhängig von der Anzahl der Satelliten, welche durch das Mobilgerät empfangen werden können. Mit Hilfe von an verschiedenen Lokationen erzeugten Bildern soll die Genauigkeit von satellitenerzeugten Geodaten evaluiert werden. Dabei wurden verschiedene Lokationen gewählt, um mögliche Hindernisse, welche das Satellitensignal abschirmen könnten, in die Analyse miteinzubeziehen. Diese Lokationen lassen sich in vier Kategorien einteilen:

- im Gelände unter freiem Himmel
- im Wald
- in einem Bürogebäude mit schusssicheren Fenstern
- in einem Wohnhaus im Dachgeschoss

Die in den Bildern als Exif-Daten gespeicherten Geodaten werden mit Hilfe des - für die private Nutzung kostenlosen - Bildbetrachters IrfanView ausgelesen. Dieser verfügt über ein PlugIn zur Darstellung von Exif-Daten. Die Bilder mit allen dazugehörigen Exif-Daten können den Anlagen B.2.2 bis B.2.5 entnommen werden.

Die Geokoordinaten, welche bei der Erstellung des Bildes durch das Smartphone ermittelt wurden, werden den tatsächlichen Standorten zum Zeitpunkt der Bilderstellung gegenübergestellt. Für die Ermittlung der tatsächlichen Standorte wurden diese in der GIS-Software QGIS eingezeichnet und

die dort angegebenen Geokoordinaten abgelesen. Aufgrund Ungenauigkeiten beim Einzeichnen der Standpunkte können die ermittelten Geokoordinaten geringfügig zum tatsächlichen Standort abweichen. Sie werden jedoch dennoch als „tatsächlicher Standort“ für die Analysen herangezogen.

Um die Genauigkeiten der Geokoordinaten in Relation zu den Geokoordinaten in den erzeugten Bildern zu setzen, werden die beiden Standorte gemeinsam in einer Karte dargestellt. Der rote Punkt stellt hierbei die Koordinaten aus den Bildern dar, der grüne Punkt den eigentlichen Standort zum Zeitpunkt des Erstellens des Bildes.

Mit Hilfe einer Formel lässt sich die Entfernung zwischen beiden Geokoordinaten ermitteln, diese wurden in dieser Arbeit auf eine Nachkommastelle gerundet.

Es gibt mehrere Möglichkeiten, die Entfernung zwischen zwei Geokoordinaten zu berechnen, welche unterschiedliche Faktoren in die Berechnung miteinbeziehen.

Aufgrund der geringen Entfernung der beiden Geokoordinaten aus den vorliegenden Versuchen wird in dieser Thesis auf eine einfachere Berechnung zurückgegriffen. Hierfür werden fünf Werte benötigt:

- Längengrad 1 (LG 1) und Längengrad 2 (LG 2)
- Breitengrad 1 (BG 1) und Breitengrad 2 (BG 2)
- Differenz Breitengrad (hier: Abkürzung lat)

$$lat = \frac{(BG\ 1 + BG\ 2)}{2 \cdot 0{,}01745} \tag{5.1}$$

- Hilfsvariable d(LG)

$$d(LG) = 111{,}3 \cdot \cos(lat) \cdot (LG\ 1 - LG\ 2) \tag{5.2}$$

- Hilfsvariable d(BG)

$$d(BG) = 111{,}3 \cdot (BG\ 1 - BG\ 2) \tag{5.3}$$

Die Berechnung der Entfernung beider Geokoordinaten erfolgt dann mit Hilfe der Formel:

$$Entfernung = \sqrt{d(BG) \cdot d(BG) + d(LG) \cdot d(LG)} \tag{5.4}$$

Der daraus errechnete Wert stellt die Entfernung in Kilometer dar. Eine Umrechnung in die Entfernung in Meter erfolgt entsprechend mittels Multiplikation mit 1000.

$$Entfernung\ in\ m = Entfernung\ in\ km \cdot 1000 \tag{5.5}$$

Die Berechnungen der Entfernungen wurden mit Hilfe der Formeln in Microsoft Excel durchgeführt. In den nachfolgenden Kapiteln wird jeweils nur der errechnete Wert dargestellt. Die Berechnung dieses Wertes kann der Anlage B.2.1 entnommen werden. Hier werden neben den tatsächlichen Geokoordinaten auch die Geokoordinaten des Bildes, sowie die erforderlichen Hilfsvariablen und die eigentliche Berechnung der Entfernung und deren Umrechnung in Meter aufgeführt.

5.2.1 Bildstandort „Freier Himmel“

Um die Genauigkeit von Bildern unter freiem Himmel zu testen, wurden zwei Bilder, einmal im Stadtrandbereich und einmal in freiem Gelände in einem Gartengrundstück, aufgenommen.

Aufgrund der Kenntnisse über die Probleme bei Positionsbestimmungen, ist es zu erwarten, dass es keine großen Abweichungen zwischen den Geokoordinaten des Bildes und des tatsächlichen Standortes gibt.

Tabelle 11: Bildstandort "Freier Himmel"

Bildtitel	Bild	Geokoordinaten
Sonnenblume	 Bild 20: Sonnenblume	**Wert aus Bild** Längengrad: 8.90xxxxxx Breitengrad: 48.77xxxxxx **Tatsächlicher Wert** Längengrad: 8.90xxxxxx Breitengrad: 48.77xxxxxx
Blume	 Bild 21: Blume	**Wert aus Bild** Längengrad: 8.92xxxxxxx Breitengrad: 48.75xxxxxx **Tatsächlicher Wert** Längengrad: 8.92xxxxxx Breitengrad: 48.75xxxxxx

Tabelle 12: Bildstandort "Freier Himmel" - Entfernung

Bildtitel	Standortdaten vs. tatsächlicher Standort	Entfernung
Sonnenblume	 Bild 22: Differenz Sonnenblume	2,6 Meter

Bildtitel	Standortdaten vs. tatsächlicher Standort	Entfernung
Blume	 Bild 23: Differenz Blume	4,9 Meter

Bei dem Bild „Sonnenblume“ handelt es sich um ein Bild, welches am Ortsrand des Ortes Renningen-Malmsheim erstellt wurde. Der Geländeverlauf des Standortes ist eben. Zum Zeitpunkt der Erstellung des Bildes war es sonnig.

Das Bild „Blume“ wurde in einem Gartengrundstück deutlich außerhalb des Ortes Renningen aufgenommen. Es sind leichte Höhenunterschiede vorhanden, sodass der Geländeverlauf nicht eben ist. An diesem Tag war die Temperatur kühler als im vorherigen Bild „Sonnenblume“, jedoch war es ebenfalls sonnig.

Die Betrachtung dieser Werte zeigt wie erwartet, dass Geokoordinaten, welche bei einer geringen Abschattung (siehe Kapitel 2.3) entstanden sind, sehr genau sind. Bei beiden Bildern beträgt die Entfernung zum tatsächlichen Standpunkt weniger als 5 Meter. Somit wären diese Daten von sehr hoher Aussagekraft.

5.2.2 Bildstandort „Wald“

Um die Genauigkeit von Bildern, welche in einem Wald erstellt wurden zu testen, wurden zwei Bilder an verschiedenen Stellen in einem im Wald liegenden Tierpark aufgenommen.

Bäume und unebene Geländeverläufe sorgen für Abschattungen. Es ist daher zu erwarten, dass diese zu größeren Ungenauigkeiten der Geokoordinaten führen.

Tabelle 13: Bildstandort "Wald"

Bildtitel	Bild	Geokoordinaten
Reh	 Bild 24: Reh	**Wert aus Bild** Längengrad: 8.906975 Breitengrad: 48.772806 **Tatsächlicher Wert** Längengrad: 8.90694034 Breitengrad: 48.77281167
Bär	 Bild 25: Bär	**Wert aus Bild** Längengrad: 8.922853 Breitengrad: 48.750644 **Tatsächlicher Wert** Längengrad: 8.9228866 Breitengrad: 48.7507057

Tabelle 14: Bildstandort "Wald" - Entfernung

Bildtitel	Standortdaten vs. tatsächlicher Standort	Entfernung
Reh	 Bild 26: Differenz Reh	811,7 Meter
Bär	 Bild 27: Differenz Bär	14,9 Meter

Bei dem Bild „Reh“ handelt es sich um ein Bild, welches in einem Gehege erstellt wurde, das sich im Wald befindet und von dicht stehenden großen Bäumen umgeben ist. Der Geländeverlauf des Standortes ist uneben, es sind Höhenunterschiede vorhanden. Zum Zeitpunkt der Erstellung des Bildes war es sonnig mit einigen Wolken.

Das Bild „Bär“ wurde am Bärengehege aufgenommen, welches, obwohl das Gehege ebenfalls in den Wald integriert ist, an einer Lichtung liegt. Der Geländeverlauf zeichnet sich durch leichte Höhenunterschiede aus. Dieses

Bild wurde am selben Tag wie das Bild „Reh“ aufgenommen, das Wetter ist daher identisch.

Die Betrachtung dieser Werte zeigt wie erwartet, dass Abschattungen bei der Bestimmung der Geokoordinaten per Satellit eine große Rolle spielen. Das Reh-Gehege, in welchem viele Bäume stehen, hat keine freie Sicht auf den Himmel, dies ist jedoch beim Bild „Bär“ der Fall. Bei beiden Bildern ist die Entfernung zum tatsächlichen Standort größer als bei den vorherigen Bildern. Bei dem Bild „Reh“ ist die Differenz mit über 800 Meter deutlich größer, als bei dem Bild „Bär“, welches eine Differenz von knapp 15 Metern aufweist. Dies kann auf die Abschattung durch die Bäume und auch auf die Abschattung durch die vorhandenen Wolken zurückgeführt werden.

In Ermittlungsverfahren müssen diese Daten besonders betrachtet und vorsichtig verwendet werden. Verwendet man das Bild „Reh“ ohne das Bild selbst zu betrachten, so könnte man die Hypothese bilden, dass sich das Gerät zu diesem Zeitpunkt auf der Straße befand. Erst mit der Betrachtung des Bildes wird hier deutlich, dass der Standort nicht dem tatsächlichen Standort entsprechen kann.

5.2.3 Bildstandort „Bürogebäude“

Um die Genauigkeit von Bildern, welche in einem Bürogebäude erstellt wurden zu testen, wurden zwei Bilder in unterschiedlichen Positionen im Gebäude aufgenommen.

Neben Bäumen und dem Gelände können auch Gebäude Signale abschirmen. Es ist daher auch hier eine größere Abweichung vom tatsächlichen Standort zu erwarten.

Tabelle 15: Bildstandort "Bürogebäude"

Bildtitel	Bild	Geokoordinaten
Cola-Flasche	 Bild 28: Cola-Flasche	**Wert aus Bild** Längengrad: 9,00xxxxxx Breitengrad: 48,68xxxxxx **Tatsächlicher Wert** Längengrad: 9,00xxxxxx Breitengrad: 48,68xxxxxx
Büro	 Bild 29: Büro	**Wert aus Bild** Längengrad: 8,99xxxxxx Breitengrad: 48,68xxxxxx **Tatsächlicher Wert** Längengrad: 9,00xxxxxx Breitengrad: 48,68xxxxxx

Tabelle 16: Bildstandort "Bürogebäude" - Entfernung

Bildtitel	Standortdaten vs. tatsächlicher Standort	Entfernung
Cola-Flasche	 Bild 30: Differenz Cola-Flasche	64,8 Meter
Büro	 Bild 31: Differenz Büro	573,0 Meter

Die beiden Bilder wurden in einem Bürogebäude mit schusssicheren Fenstern aufgenommen. Das eine Büro (Bild „Cola-Flasche“) ist in Richtung einer größeren Freifläche gelegen, das andere Bild wurde auf dem Flur stehend in Richtung eines Büros aufgenommen, bei dem vor den Fenstern Bäume und in etwas weiterer Entfernung weitere und höhere Bürogebäude stehen. Zum Zeitpunkt der Erstellung der Bilder war es bewölkt.

Auch hier zeigt sich, dass Abschattungen die Genauigkeit der Standortdaten beeinflussen. Wie auch im Mobilfunknetz, wo die schusssicheren Fenster zu Beeinträchtigungen in der Sprachqualität führen, dürften sie auch die Genauigkeit des Standortes negativ beeinträchtigen.

Die Bäume, die direkt vor dem Büro stehen, welches auf dem Bild „Büro“ zu sehen ist, dürften ebenfalls zu einer zusätzlichen Abschattung und somit einer schlechteren Genauigkeit führen.

Wenn man die Genauigkeiten beider Bilder miteinander vergleicht, so fällt auf, dass die Genauigkeit bei dem Bild mit freier Fläche vor dem Bürogebäude höher ist. Es zeigt sich somit, dass Bäume das Satellitensignal stark abschatten.

Auch in diesem Versuch zeigt es sich, wie wichtig es ist, nicht nur die Standorte separiert zu betrachten. Wie in dem vorherigen Bild „Reh“ könnte auch hier der Eindruck entstehen, dass sich der Standort zum Zeitpunkt der Bildaufnahme beide Male auf der Straße befand.

5.2.4 Bildstandort „Haus“

Um die Genauigkeit von Bildern, welche in einem Wohnhaus erstellt wurden zu testen, wurden zwei Bilder in einem Wohnhaus im Dachgeschoss aufgenommen.

Aufgrund der Lage der Wohnung könnten die Werte durch eine geringere Abschattung des Gebäudes recht genau sein.

Tabelle 17: Bildstandort "Haus"

Bildtitel	Bild	Geokoordinaten
Torte	 Bild 32: Torte	**Wert aus Bild** Längengrad: 8,90xxxxxx Breitengrad: 48,77xxxxxx **Tatsächlicher Wert** Längengrad: 8,90xxxxxx Breitengrad: 48,77xxxxxx
Nachtisch	 Bild 33: Nachtisch	**Wert aus Bild** Längengrad: 8,90xxxxxx Breitengrad: 48,77xxxxxx **Tatsächlicher Wert** Längengrad: 8,90xxxxxx Breitengrad: 48,77xxxxxx

Tabelle 18: Bildstandort "Haus" - Entfernung

Bildtitel	Standortdaten vs. tatsächlicher Standort	Differenz
Torte	 Bild 34: Differenz Torte	395,4 Meter
Nachtisch	 Bild 35: Differenz Nachtisch	0,3 Meter

Beide Bilder wurden in der Küche einer Dachgeschosswohnung aufgenommen, welche um eine Dachgaube mit Fenstern erweitert wurde. Der Standort des Bildes „Torte“ befindet sich hierbei eher in Richtung des Gebäudeinneren, während das Bild „Nachtisch“ näher an den Fenstern der Küche erstellt wurde. Diese beiden Positionen befinden sich in einem Meter Abstand zueinander. Die Aufnahmen wurden zu unterschiedlichen Tageszeiten erstellt. Während das Bild „Torte“ am Abend eines eher wolkigen Tages mit Sonne und Regenschauern erstellt wurde, wurde das Bild „Nachtisch“ an einem sonnigen Nachmittag erstellt. Zwischen dem Haus und einer weiteren Bebauung befinden sich ein Garten und eine Straße mit Parkplätzen am Seitenstreifen.

Die Genauigkeit dieser Standortdaten überrascht. Während das Bild „Nachtisch“ eine fast 100%-ige Übereinstimmung aufweist, ist beim Bild „Torte“ eine Differenz von knapp 400 Meter vorhanden. Aufgrund der annähernd selben Position bei der Erstellung des Bildes bedeutet dies, dass sich bereits ein geringer Unterschied der Position stark auf die Abschattung auswirken kann. Zusätzlich wirken sich ganz offenbar auch die Wetterverhältnisse auf die Qualität des Satellitensignals aus. Für die Bewertung der Genauigkeit von Geodaten müssen daher auch die Wetterverhältnisse in die Interpretation miteinbezogen werden.

5.2.5 Interpretation

Die Analyse der Geodaten, welche in Exif-Daten von Bildern gespeichert werden zeigt, dass diese Daten nicht ungeprüft für Ermittlungsverfahren übernommen werden dürfen. Für eine generelle erste Einschätzung sind diese Daten sehr gut geeignet und können zeigen, ob sich ein potentieller Täter möglicherweise in der Nähe eines Tatortes aufgehalten hat.

Wichtig hierbei ist, dass die Bilder selbst betrachtet werden und mit Hilfe des Motivs auf dem Bild eruiert wird, ob der Standort korrekt sein kann. Dies ergibt eine erste Einschätzung, ob die Standorte einer genaueren Betrachtung unterzogen werden müssen. Sollte dies der Fall sein, ist als nächstes der Geländeverlauf zu betrachten. So können Hinweise auf Erhebungen im Gelände bedeuten, dass der Standort ungenau sein könnte.

Auch wenn diese Feststellungen in der Folge nicht zu einem exakten Standort führen, kann dadurch erreicht werden, dass eine Einschätzung bezüglich der Genauigkeit der extrahierten Standorte abgegeben werden kann.

Generell lässt sich sagen, dass bereits ein geringer Standortwechsel, der Geländeverlauf und das Wetter zu einer Veränderung der Abschattung führen können, was somit die Genauigkeit der Geodaten beeinflusst.

5.3 Genauigkeit von Geodaten: Google Standortverlauf

Bei der Einrichtung des Samsung-Testgerätes bzw. bei der Verwendung von Android-Geräten allgemein, wird ein Google-Account hinterlegt. In diesem kann manuell der Standortverlauf aktiviert werden. Dieser wurde für den Testaccount aktiviert.

Für dieses Testszenario (siehe Kapitel 4.2.3) wurde die nachfolgend grafisch dargestellte Strecke zu Fuß zurückgelegt. Das rote „x“ markiert den Start- bzw. Zielpunkt. An der gelb markierten Stelle wurde eine Navigation mit dem Zielpunkt „71034 Böblingen, Talstraße 50“ gestartet. Hierbei handelt es sich um die Postanschrift des Start- bzw. Zielpunkts der abgelaufenen Strecke.

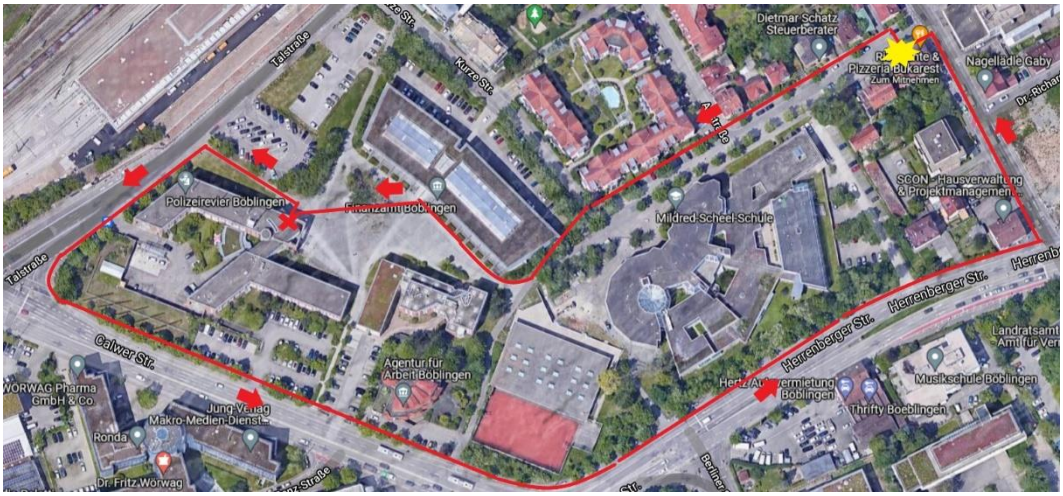


Bild 36: Route

Damit der Standort und die Uhrzeit nachvollzogen werden können, wurde ab dem Zeitpunkt des Starts der Navigation ein Video aufgenommen, welches die zurückgelegte Strecke und die Zeit mit Hilfe der im Internet verfügbaren Atomuhr[14] dokumentiert. Diese Daten und die Daten aus dem Google

[14] Die Atomuhr wurde verwendet, weil diese die Zeit mit Sekunden anzeigt. Diese waren für den Test erforderlich. Es wurde die Atomuhr der Webseite https://www.uhrzeit.org/atomuhr.php verwendet.

Standortverlauf sollen für eine Aussage bezüglich der Genauigkeit herangezogen werden.

Um die Daten von Google zu erhalten, müssen diese über den Google-Account angefordert werden. Hier kann ausgewählt werden, welche Daten exportiert werden sollen. Bei der Auswahl des Standortsverlauf erhält man die Datei „Standortverlauf.json“ und den Ordner „Semantic Location History“ mit der im vorliegenden Fall darin enthalten Datei „2021_OCTOBER.json“. Die .json Dateien können mit Hilfe eines Texteditors angezeigt werden und weisen vom Aufbau eine Ähnlichkeit zu XML-Dateien auf. Zur besseren Lesbarkeit wurden die Daten in Microsoft Excel in Tabellenform aufbereitet, sowie die Zeitstempel in lesbares Datum und Uhrzeitformat konvertiert[15]. Die Werte von Längen- und Breitengrad werden durch Google ohne „.“ (Punkt) dargestellt, in der Tabelle wurde dieser an der jeweiligen Stelle händisch eingefügt.

Ein Datensatz der Datei „Standortverlauf.json“ enthält neben den Angaben zum Zeitstempel und den Geokoordinaten auch eine Wahrscheinlichkeitsangabe bezogen auf welche Art von Bewegung es sich gehandelt hat. Google unterscheidet unter anderem zwischen „STILL“, „IN_VEHICLE“ und „WALKING“. Wie auch bei den Geodaten aus dem Smartphone bezieht Google in die Standortlokalisierung verschiedene Faktoren mit ein. Neben dem „GPS“ sind auch „CELL“ und „WIFI“ in den Daten enthalten. Für die Bewertung von Standortdaten ist der Wert „Accuracy“ (dt. Genauigkeit) von großer Bedeutung. Mit Hilfe dieses Wertes sollen die im Standortverlauf enthaltenen Geodaten mit dem tatsächlichen Wert verglichen und auf deren Richtigkeit geprüft werden.

Die enthaltenen Geokoordinaten aus dem Standortverlauf wurden als .csv-Datei gespeichert und in QGIS eingelesen. Es wurde ein zeitlicher Filter

[15] Der Zeitstempel liegt ursprünglich als UNIX-Timestamp vor.
Formel zur Umrechnung in Microsoft Excel: UNIX-Timestamp/1000/86400+25569

gesetzt, sodass nur die Daten des Testszenarios angezeigt werden. Dadurch ergibt sich folgende grafische Ansicht[16]:

Bild 37: Standortverlauf.json

Es fällt auf, dass Google erst dann vermehrt Standorte speichert, nachdem die Navigation gestartet wurde. Ebenfalls sind erst ab diesem Zeitpunkt Datensätze mit der Quelle „GPS“ enthalten.

Für die Analyse wurden stichprobenartig für fünf Zeitstempel die Geokoordinaten aus Google des Typs „GPS“ mit den tatsächlichen Geokoordinaten abgeglichen und die Distanz anhand der in Kapitel 5.2 beschriebenen Formel errechnet[17]. Der Wert wurde kaufmännisch auf den vollen Meter gerundet.

[16] Die Grafik ist in der Anlage B.3.1 zur besseren Lesbarkeit auf einer kompletten Seite dargestellt
[17] Siehe Anlage B.3.2

Tabelle 19: Genauigkeit Standortverlauf.json

Zeitstempel	Koordinaten Google	Koordinaten tatsächlich	Genauigkeit lt. Google	Distanz (in m)
15.10.2021 13:07:51	48.68538480 9.00555770	48.68542617 9.00553394	8	5
15.10.2021 13:08:52	48.68516130 9.00487740	48.68513798 9.00480907	7	6
15.10.2021 13:09:23	48.68501240 9.00450540	48.68500296 9.00446709	7	3
15.10.2021 13:11:56	48.68438660 9.00296830	48.68438861 9.00298144	7	1
15.10.2021 13:12:12	48.68446830 9.00284690	48.68449264 9.00282118	4	3

Wie die Tabelle zeigt, dürfte es sich bei der Genauigkeit, welche durch Google angegeben wird, um Werte in Meter handeln. Vergleicht man diese mit der tatsächlichen Abweichung, kann gesagt werden, dass diese Werte sehr nah beieinander liegen. Für Ermittlungsverfahren sind diese Daten von großer Bedeutung. Selbst wenn die Genauigkeit geringer ist, also der Wert größer, so kann doch ein Bereich festgelegt werden, in welchem sich das Gerät befunden haben muss. Je geringer dieser Wert, desto aussagekräftiger ist der Standort jedoch für den Ermittler.

5.4 Navigation

Für die Analyse der Geodaten, welche möglicherweise bei einer Navigation erzeugt werden, wurde jeweils nach einem Zielort auf dem entsprechenden Gerät gesucht, die Navigation gestartet und die Strecke zurückgelegt. In den nachfolgenden Unterkapiteln sollen die Daten hinsichtlich der in Kapitel 4.2.4 beschriebenen Fragestellung, ob Geodaten gespeichert werden und ob die Navigation auf dem Testgerät nachvollzogen werden kann, analysiert werden.

Nach erfolgter Durchführung und Analyse konnte festgestellt werden, dass das Apple-Testgerät, im Gegensatz zum Samsung-Testgerät, Daten gespeichert hat:

Tabelle 20: Navigation

	Apple	Samsung
Geodaten	ja	nein

5.4.1 Analyse Apple iPhone 8

Für das Testszenario wurde eine Navigation mit der auf dem Gerät vorinstallierten App Maps ausgehend von „Urbanstraße 20, 70182 Stuttgart“ nach „Talstraße 50, 71034 Böblingen“ gestartet.

Es konnten 4249 Geodaten auf dem Testgerät Apple iPhone 8 festgestellt werden. Diese stellen sich grafisch wie folgt dar:

Bild 38: Standorte Navigation Apple

Die hier dargestellten Daten enthalten, wie in Kapitel 5.1.1 beschrieben, Daten der Kategorien CellTower, Wireless Networks, Reminder Locations. Neu hinzugekommen sind Daten erzeugt durch das GPS.

Zuerst werden die Daten im Gesamten betrachtet, bevor eine Analyse der Daten aus der Kategorie „Apple Maps“ erfolgt.

Wie dem Bild 38 entnommen werden kann, ist bei den Daten eine Bewegung feststellbar. Da zwischen den Städten Stuttgart und Böblingen die meisten Geodaten vorhanden sind, kann mit Hilfe der Zeitstempel bereits hier die Aussage getroffen werden, dass sich das Gerät von Stuttgart in Richtung Böblingen bewegt haben muss. Betrachtet man die Häufigkeiten im Bereich Stuttgart, kann festgestellt werden, dass sich die meisten Datensätze im Bereich der Olgastraße in Stuttgart befinden:

Bild 39: Aggregierte Standorte: höchster Wert

Bei der weiteren Analyse kann der Verlauf der Fahrt anhand den Standortdaten nachvollzogen werden, wie der nachfolgende Ausschnitt aus UFED zeigt.

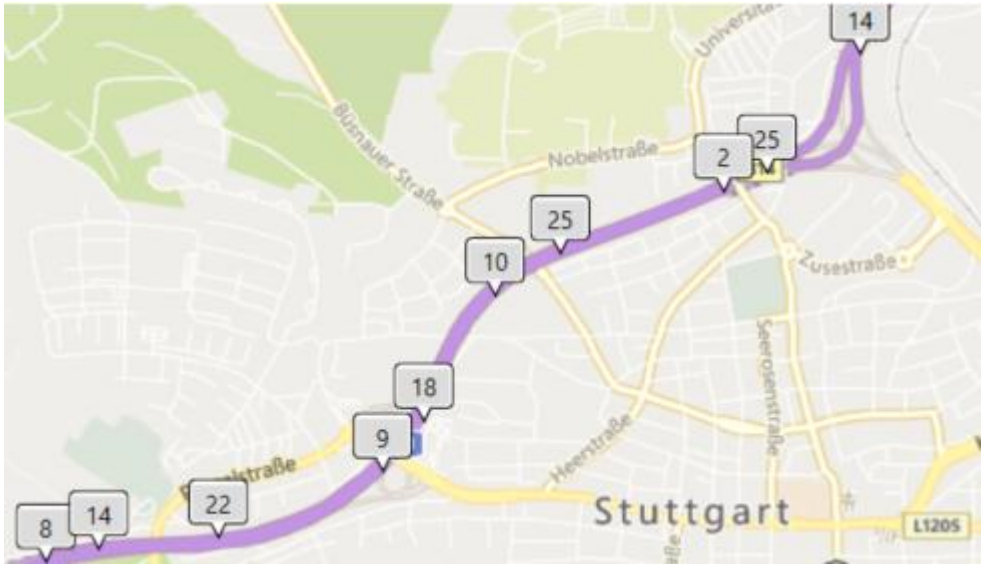


Bild 40: Routenverlauf

Betrachtet man die Daten in Böblingen, so fällt eine Häufung von Daten im Bereich der Calwer Straße auf:

Bild 41: Datenhäufung Böblingen

Die Fahrt von Stuttgart nach Böblingen kann den Geodaten aus dem Testgerät entnommen werden und ist somit für Ermittlungsverfahren von hoher Aussagekraft.

Im vorliegenden Image gibt es drei Datensätze, die als Quelle „Apple Maps“ enthalten. Es handelt sich hierbei um zwei Datensätze in Böblingen und einen in Stuttgart. Die Datensätze liegen in folgender Quelldatei:

`Apple_iPhone 8 (A1905).zip/root/private/var/mobile/Containers/Shared/AppGroup/6576898F-7DBB-4CC9-9077-EDCD9C507990/Maps/MapsSync_0.0.1-wal`

Tabelle 21: Quelle Apple Maps

Zeitstempel	Geokoordinaten	Name	Adresse
06.10.2021 09:21:05	48.776933 9.187598		
06.10.2021 09:21:20	48.684666 9.000900	Talstraße 50	Talstraße, Böblingen, 71034, Baden-Württemberg, Deutschland
06.10.2021 09:21:21	48.684666 9.000900		

Aufgrund des Testaufbaus können die vorliegenden Daten wie folgt interpretiert werden. Der erste Datensatz wurde geschrieben, als der aktuelle Standort ermittelt wurde. Bei der Eingabe des Zieles wurde der zweite Datensatz mit den Spalten „Name“ und „Adresse“ geschrieben. Die Navigation zu diesem Punkt wurde gestartet, hierbei wurde der dritte Datensatz geschrieben.

Wenn man über die Suche in UFED nach dem Begriff „maps“ sucht, so werden Suchergebnisse in verschiedenen Kategorien angezeigt. Die Kategorie „Reisen“ enthält einen Eintrag, welcher die bereits bekannten Daten aus Apple Maps enthält. Dieser Eintrag wird im nachfolgenden Bild 42 dargestellt.

Bild 42: Screenshot der Kategorie "Reisen"

5.4.2 Analyse Samsung Galaxy S8

Auf dem Testgerät Samsung Galaxy S8 konnten keine Geodaten festgestellt werden. Zusätzlich zu den durch UFED aufbereiteten Daten wurden die Datenbanken von Google Maps direkt betrachtet. Diese waren größtenteils leer bzw. enthielten lediglich undefinierbare und nicht zuordenbare Zeichenketten.

Bei der Betrachtung der durch UFED ausgelesenen Bildern konnten elf Bilder festgestellt werden, welche Bezug zum Zielort der Navigation haben. Es handelt sich hierbei um ein Bild, bei welchem es sich um einen Snapshot aus der Google Maps-App handelt und 10 Bilder, welche das Gebäude von außen und innen zeigen. Diese Bilder werden in der App angezeigt, wenn man nach dem Zielort sucht. Die Bilder mit den zugehörigen Pfaden aus dem Image können der Anlage B.4 entnommen werden.

5.4.3 Interpretation

Mit Hilfe der gewonnenen Daten aus dem Testgerät von Apple lässt sich feststellen, dass diese für die Standortbestimmung eine sehr große Bedeutung haben. Auch wenn durch Apple Maps selber keine Daten während der eigentlichen Navigation geschrieben werden, kann dies durch die durch Apple generell generierten Standortdaten ausgeglichen werden. Betrachtet man die Daten von Apple Maps separat, so kann keine Aussage getroffen werden, ob nur die Navigation eingegeben und gestartet oder die Navigation tatsächlich durchgeführt wurde.

Beim Testgerät von Samsung hingegen werden keinerlei Geodaten gespeichert, was eine nachträgliche Standortbestimmung anhand dieser unmöglich macht. Die im Gerät enthaltenen Bilder können jedoch ein Hinweis darauf sein, nach was der Nutzer des Gerätes in Google Maps gesucht hat.

5.5 Suche: Google

Schnell mal eine Stadt oder eine Örtlichkeit googeln und sich Informationen über diese anzeigen lassen – in der heutigen Zeit dank Smartphone kein Problem mehr. Wenn diese Informationen mit Geokoordinaten hinterlegt auf dem Smartphone abgespeichert werden, könnte es sein, dass dies zu falschen Rückschlüssen von Ermittlungsbehörden führt. Daher soll mit Hilfe dieses Testszenarios das Verhalten von Smartphones bei Suchen über Google und Suchen in Google Maps analysiert werden. Hierfür wurde über den Browser die Webseite www.google.de aufgerufen und der Suchbegriff „renningen“ eingegeben. Bei dem Apple Testgerät wurde das Ergebnis in Google Maps über den Browser aufgerufen, bei Samsung über die Google Maps App. Zusätzlich wurde im Anschluss in Google Maps nach „Polizeirevier Böblingen“ gesucht.

Nach erfolgter Durchführung und Analyse konnte festgestellt werden, dass das Apple-Testgerät, im Gegensatz zum Samsung-Testgerät, Daten gespeichert hat.

Tabelle 22: Suche: Google

	Apple	Samsung
Geodaten	ja	nein

5.5.1 Analyse Apple iPhone 8

Bei dem Apple-Testgerät konnten 12 Gerätestandorte festgestellt werden. Anders als bei den bisherigen Testszenarien wurden die enthalten Geokoordinaten nicht auf einer Karte grafisch dargestellt. Betrachtet man den Ursprung der Daten, stellt man fest, dass die Geokoordinaten aus Webadressen extrahiert werden. Aus dem Webverlauf geht hervor, dass zuerst die Webseite Google aufgerufen wurde, und im weiteren Verlauf nach „renningen“ gesucht wurde. Ebenfalls kann anhand der Webadressen festgestellt werden, dass das Ergebnis „renningen“ in Google Maps geöffnet wurde. Im weiteren Web-Verlauf ist auch die Suche nach „Polizeirevier Böblingen“ enthalten. Als Quelle für diese Daten ist der Browser Safari angegeben. Der Kategorie der „Gesuchten Elemente“ sind diese Daten ebenfalls zu entnehmen.

Die durch UFED extrahierten Bilder wurden ebenfalls auf mögliche Hinweise zu Standorten betrachtet. Hierbei konnte festgestellt werden, dass Bilder von Böblingen, Renningen, sowie den Nachbarorten Weil der Stadt, Rutesheim und Magstadt enthalten sind. Eine Auswahl der Bilder finden sich im Anhang B.5.1.

5.5.2 Analyse Samsung Galaxy S8

Im Gegensatz zum Apple-Testgerät liegen im Testgerät von Samsung keine Daten in der Kategorie „Gerätestandorte“ vor. Auch in der Kategorie „Web-Verlauf“ sind keine Daten in Bezug auf das durchgeführte Testszenario enthalten. Lediglich in der Kategorie „Gesuchte Elemente“ konnte ein Eintrag festgestellt werden der aufzeigt, dass über die App von Google nach dem Suchbegriff „renningen“ gesucht wurde.

Da keine weiteren Daten festgestellt werden konnten, wurde über die Suche in UFED manuell nach „renningen“ und „Polizeirevier Böblingen“ gesucht. Für „renningen“ wurde das oben erwähnte Ergebnis gefunden, der Begriff „Polizeirevier Böblingen“ ergab keinen Treffer. Ebenfalls erfolgte eine manuelle Überprüfung der Datenbank von Google Maps, um auszuschließen, dass durch UFED Geodaten nicht aufbereitet wurden. Hier sind ebenfalls keine Daten enthalten.

Auch bei diesem Testgerät wurden die Bilder betrachtet. Es konnten wie bei dem Apple-Testgerät Bilder von Böblingen, Renningen, Weil der Stadt, Rutesheim und Magstadt festgestellt werden. Eine Auswahl der Bilder finden sich im Anhang B.5.2.

5.5.3 Interpretation

Die gewonnen Erkenntnisse aus den Daten der Testgeräte zeigen, dass die eingegebenen Orte nicht in die grafische Analyse der Geräteorte in UFED einfließen. Diese sind entweder gar nicht vorhanden, oder aber sie werden im Falle des Apple-Testgerätes nur in Tabellenform ausgegeben.

Anhand der Bilder, welche auf beiden Testgeräten gespeichert wurden, können mit Ortskenntnissen zwar die Orte erkannt werden, aber es kann zum einen nicht gesagt werden, nach welchem Ort gesucht wurde, zum andern ist es nicht möglich, aus diesen Bildern den Aufenthaltsort des Nutzers zum Zeitpunkt der Suche festzustellen.

Anhand der ausgewerteten Daten lässt sich sagen, dass bei diesem Testszenario keine Gefahr für eine Fehlinterpretation von Daten besteht, da diese nicht existieren bzw. von UFED für eine grafische Auswertung nicht angezeigt werden.

5.6 Versand von Geodaten: E-Mail

Wenn ein Smartphone im Rahmen eines Ermittlungsverfahrens gesichert wird und die Standortdaten in die Ermittlungsarbeit einfließen, muss bewie-

sen werden, dass die auf dem Smartphone enthaltenen Geodaten tatsächlich zu diesem Smartphone gehören. In einem Gerichtsverfahren könnte es ansonsten zu der Frage kommen, ob die Geodaten auch über einen Datentransfer auf das Smartphone gelangt sein können.

Eine Möglichkeit wäre hierbei der Empfang des Bildes per E-Mail. Um dies zu untersuchen wurden zwei Testszenarien erstellt. Für beide Testszenarien wird auf dem Testgerät die App des E-Mail-Providers GMX eingerichtet. An die E-Mail-Adresse GeoDatenWings@gmx.de wird eine E-Mail mit einem Bild, welches Standortdaten enthält, gesendet. Bei Variante 1 des Testszenarios wird die Mail geöffnet und das Bild anschließend heruntergeladen. Bei der Variante 2 wird die Mail geöffnet und das Bild lediglich in der Bildvorschau angezeigt. Diese Variante beinhaltet jedoch nicht das Herunterladen des Bildes.

Nachfolgende Tabelle zeigt die Ergebnisse der Testszenarien:

Tabelle 23: Versand von Geodaten: E-Mail

Testvariante	Apple	Samsung
Variante 1	nein	ja
Variante 2	ja	ja

In den folgenden beiden Unterkapiteln werden die Ergebnisse für jedes Testgerät separat dargestellt.

5.6.1 Analyse Apple iPhone 8

Das Testszenario der Variante 2 wurde zuerst durchgeführt und wird daher zuerst beschrieben.

Bei Variante 2 konnte das Bild mit den Geodaten in dem Image festgestellt werden. Als Metadaten konnten neben den Geokoordinaten auch Angaben zu dem Bild an sich festgestellt werden.

Metadata

Kamerahersteller:	Xiaomi
Kameramodell:	Mi 9T Pro
Erfassungszeit:	22.07.2021 10:17:06
Pixelauflösung:	4000x3000
Auflösung:	72x72 (Einheit: Zoll)
Ausrichtung:	Horizontal (normal)
Lat/Lon:	49.033384 / 9.053364

Karte

Position:	(49.033384, 9.053364)

Bild 43: Exif-Daten

Bei Testvariante 1 ist ebenfalls ein Geodatum in der Kategorie „Geräteorte“ enthalten. Betrachtet man dieses, fällt auf, dass es sich hierbei um das Bild aus Testvariante 2 handelt, obwohl das Gerät nach dem Test auf Werkseinstellung zurückgesetzt wurde. Dies liegt an den Einstellungen von Apple, dass Bilder automatisch mit dem Apple-Account synchronisiert werden.

Das Ergebnis verwundert. Es wäre zu erwarten, dass in beiden Varianten die Bilder auf dem Gerät mit Geodaten vorliegen, jedoch kann dieses nicht aus dem Image entnommen werden.

Die nachfolgende Tabelle zeigt den Pfad aus dem Image, welcher das Bild mit den Geodaten enthält[18].

Tabelle 24: Pfadangaben Apple

Testvariante	Pfad
Variante 1	-
Variante 2	Apple_iPhone 8 (A1905).zip/root/private/var/mobile/Containers/Data/Application/FAADEB89-1A14-4581-B41D-BE49F363D1B5/Library/Caches/attachments/6859905a5112ae96b89603a33e13b440ead13926.jpg

[18] Siehe Anlage B.6.1

In beiden Images konnten die Bilder in mehrfacher Ausfertigung aufgefunden werden. Hier handelt es sich unter anderem um das Bild als Thumbnail, also dem kleinen Vorschaubild.

5.6.2 Analyse Samsung Galaxy S8

Sowohl bei Testvariante 1 als auch bei Testvariante 2 konnten die Geodaten in den Images festgestellt werden. Das festgestellte Bild weist dieselben Metadaten auf, wie bei dem Testszenario mit dem Apple Testgerät (siehe Bild 43).

Die nachfolgende Tabelle zeigt die Pfade aus den Images, welche das Bild mit den Geodaten enthalten[19].

Tabelle 25: Pfadangaben Samsung

Testvariante	Pfad
Variante 1	USERDATA (ExtX)/Root/media/0/Download/IMG_20210722_101704-2.jpg
Variante 2	data/Root/data/de.gmx.mobile.android.mail/cache/attachment_1388464220267967493.temp

Die beiden Varianten können an den Pfadangeben erkannt werden. Während bei Variante 1 das Bild im Download-Ordner und mit dem für Android typischen Namen gespeichert wurde, so liegt das Bild bei Variante 2 in einem Cache-Verzeichnis.

5.6.3 Interpretation

Die Analyse der Daten zeigt, dass Geodaten, welche in den Metadaten von Bildern eingebettet sind und per E-Mail verschickt wurden, auch auf dem empfangenden Smartphone enthalten sind. Dies bedeutet, dass hierbei Standorte entstehen, an welchem sich das Gerät jedoch nicht befunden hat.

[19] Siehe Anlage B.6.2

Für die Analyse und Interpretation von Geodaten ist es daher wichtig, dass hierauf ein besonderes Augenmerk gelegt wird.

Hinweise zur Überprüfung der Bilder können sich aus folgenden Informationen ergeben:

- Pfad des Speicherortes (z.B.: Download-Ordner)
- Dateiname (bei Android oftmals IMG_Datum_Uhrzeit)
- Exif-Daten: Kamerahersteller, Kameramodell, Auflösung

Schwierigkeiten sind hierbei zu erwarten, wenn ein baugleiches Gerät verwendet wird und die Daten beispielsweise durch Synchronisation auf verschiedenen Geräten geteilt werden.

5.7 Versand von Geodaten: WhatsApp

In der heutigen Zeit werden Nachrichten schnell und unkompliziert per Messenger verschickt. Diese können Text, aber auch Bilder und Videos enthalten. Neben dem Versand von Bildern per E-Mail soll daher auch, wie in Kapitel 4.2.7 beschrieben, der Versand per WhatsApp analysiert werden.

Nach erfolgter Durchführung und Analyse konnte festgestellt werden, dass beide Testgeräte keinerlei Daten gespeichert haben:

Tabelle 26: Versand von Geodaten: WhatsApp

	Apple	**Samsung**
Geodaten	nein	nein

5.7.1 Analyse Apple iPhone 8

Auf dem Apple-Testgerät konnte das Testbild in mehrfacher Ausfertigung festgestellt werden[20]. Die in dem Ursprungsbild enthaltenen Geodaten, sowie weitere Metadaten konnten nicht mehr festgestellt werden.

5.7.2 Analyse Samsung Galaxy S8

Auch auf dem Samsung Galaxy S8 können analog zu dem Apple-Testgerät nur die Bilder ohne Metadaten festgestellt werden[21].

5.7.3 Interpretation

Da durch WhatsApp beim Versand die Metadaten entfernt werden, ist es nicht möglich, Rückschlüsse über den Entstehungsort des Bildes zu erlangen.

5.8 Versand von Geodaten: Facebook Messenger

Neben dem Versand von Nachrichten über den Messenger WhatsApp kann bei einem bestehenden Facebook-Account auch dessen Messenger verwendet werden. Der Facebook Messenger ermöglicht dem Nutzer Bilder anzusehen und diese auch herunterzuladen.

Aus diesem Grund wurden zwei Varianten des Tests durchgeführt. Variante 1 beinhaltet lediglich das Öffnen und Ansehen des Bildes, welches von einem weiteren Facebook Account verschickt wurde. Bei Variante 2 wird das Bild zusätzlich heruntergeladen.

Nach erfolgter Durchführung und Analyse konnte festgestellt werden, dass beide Testgeräte keine Geodaten gespeichert haben.

[20] Siehe Anlage B.7.1
[21] Siehe Anlage B.7.2

Tabelle 27: Versand von Geodaten: Facebook Messenger

Testvariante	Apple	Samsung
Variante 1	nein	nein
Variante 2	nein	nein

5.8.1 Analyse Apple iPhone 8

Auf dem Testgerät Apple iPhone 8 konnte in beiden Varianten das Testbild ohne Geodaten festgestellt werden. Die Bilder liegen unter nachfolgenden Pfaden[22]:

Tabelle 28: Pfadangaben Apple

Testvariante	Pfad
Variante 1	Apple_iPhone 8 (A1905).zip/root/private/var/mobile/Containers/Shared/AppGroup/0BE94256-0B0D-4604-B01E-F65369AE708F/Library/Caches/lightspeed-imageCache/0186ecd127cce43c0e2af037bdff5e75
Variante 2	Apple_iPhone 8 (A1905).zip/root/private/var/mobile/Containers/Shared/AppGroup/0BE94256-0B0D-4604-B01E-F65369AE708F/Library/Caches/lightspeed-imageCache/0186ecd127cce43c0e2af037bdff5e75 (entspricht Pfad aus Variante 1)
	Apple_iPhone 8 (A1905).zip/root/private/var/mobile/Media/PhotoData/Thumbnails/V2/DCIM/100APPLE/IMG_0001.JPG/5003.JPG
	Apple_iPhone 8 (A1905).zip/root/private/var/mobile/Containers/Shared/AppGroup/0BE94256-0B0D-4604-B01E-F65369AE708F/Library/Caches/lightspeed-imageCache/69fc4e7e15a12cb416414cf48e0d70d1
	Apple_iPhone 8 (A1905).zip/root/private/var/mobile/Media/PhotoData/Thumbnails/3310.ithmb/thumb_1.bmp

[22] Siehe B.8.1

5.8.2 Analyse Samsung Galaxy S8

Auf dem Testgerät Samsung Galaxy S8 konnte in beiden Varianten das Testbild ohne Geodaten festgestellt werden. Die Bilder liegen unter nachfolgenden Pfaden:

Tabelle 29: Pfadangaben Samsung

Testvariante	Pfad
Variante 1	data/Root/data/com.facebook.orca/cache/image/9XQdIiDCtULRF-gK-PiP7VmhHOM
	data/Root/data/com.facebook.orca/cache/image/pQRtmzvU4gdX3QH1ExSbiDjz5_Y
Variante 2	data/Root/data/com.facebook.orca/cache/image/cwVNtboqP_rcT_CRbRMMOlP1rrI
	data/Root/media/0/Pictures/Messenger/received_4536112579786760.jpeg

5.8.3 Interpretation

Bei beiden Varianten auf beiden Testgeräten konnten keine Geodaten festgestellt werden – diese wurden durch den Facebook Messenger entfernt. Es ist daher nicht möglich Rückschlüsse über den Entstehungsort des Bildes zu erlangen.

5.9 Versand von Geodaten: Snapchat

Bei Snapchat können einem sogenannten Snap (ein zuvor erstelltes Bild) Text und Smileys, aber auch ein Standort hinzugefügt werden, bevor es an den Chatpartner versendet wird.

Alle Nachrichten löschen sich automatisch nach einer bestimmten Zeit (sofort nach dem Ansehen oder 24 Stunden später). Für Ermittlungen ist es daher interessant, ob Daten von Snapchat auf dem ausgelesenen Gerät festgestellt werden können.

Nach erfolgter Durchführung und Analyse konnte festgestellt werden, dass beide Testgeräte keine Daten gespeichert haben:

Tabelle 30: Versand von Geodaten: Snapchat

	Apple	**Samsung**
Snapchat	nein	nein

5.9.1 Analyse Apple iPhone 8

UFED hat die Konversation in Snapchat feststellen können, jedoch ohne nähere Informationen zu den beiden Chat-Teilnehmern[23]. In den extrahierten Bildern konnte das in Snapchat erstellte Bild nicht aufgefunden werden.

5.9.2 Analyse Samsung Galaxy S8

Bei dem Samsung Gerät konnte UFED zwei Kommunikationen feststellen, was darauf zurückzuführen ist, dass die Nachrichten-Löschung erst nach den eingestellten 24 Stunden erfolgt. Weiter konnten dem Image die beiden Namen der Chat-Teilnehmer „Geo Daten“ und „Lena Z“ entnommen werden[24]. Eine Zuordnung, dass es sich bei „Geo Daten“ um den Eigentümer handelt, wurde von UFED korrekt vorgenommen. Auch hier sind jedoch weder das versandte Bild noch Geodaten feststellbar.

5.9.3 Interpretation

Erwartungsgemäß konnten keine Daten zu dem Snap bzw. dessen enthaltenen Geodaten aufgefunden werden, was mit der Philosophie von Snapchat zusammenhängen dürfte. Hier sind also keine Daten für Ermittlungsfahren zu erwarten.

[23] Siehe Anlage B.9.1
[24] Siehe Anlage B.9.2

5.10 Upload von Geodaten: Facebook

In Facebook können neben textbasierten Statusbeiträgen auch Beiträge mit Bildern hochgeladen werden. Dieses Testszenario soll zeigen, ob ein Bild hinsichtlich der in Kapitel 4.2.10 gestellten Fragestellung mit Geodaten in im Kontext zu Facebook erkennbar ist.

Tabelle 31: Upload von Geodaten: Facebook

	Apple	**Samsung**
Upload Bild	ja	ja
Geodaten Bild	nein	ja

5.10.1 Analyse Apple iPhone 8

Aus dem Apple-Testgerät konnten nur „alte“ Beiträge von Facebook extrahiert werden. Der Beitrag, in welchem das Bild hochgeladen wurde, ist nicht in diesen Daten enthalten.

Das erzeugte Bild mitsamt seinen Geodaten kann zwar festgestellt werden, jedoch ohne einen erkennbaren Bezug zu Facebook.

Über die Kategorie „Bilder“ kann es in UFED - jedoch ohne Geodaten - unter folgendem Pfad festgestellt werden[25]:

`Apple_iPhone 8 (A1905).zip/root/private/var/mobile/Containers/Data/Application/8754D65F-8F08-4F5E-8C69-CE3E6194AC30/Library/Caches/com.facebook.Facebook.MosaicIGImageDiskCache/FBImageDownloader-cb6f72ec15e6d159da7008a40e96a291.jpg`

Der im Bild angegebene Zeitstempel der Erstellung der Bilder stimmt mit dem Zeitstempel der Erstellung des Beitrags in Facebook überein.

[25] Siehe Anlage B.10.1

5.10.2 Analyse Samsung Galaxy S8

Wie schon bei dem Apple-Testgerät kann der Facebook Beitrag selbst auch hier nicht in den Daten festgestellt werden.

Jedoch ist das Bild im Kontext zu Facebook und mit Geodaten in den Daten enthalten[26]:

`data/Root/data/com.facebook.katana/app_uploads/6e5ac268-65ea-49c2-aa7b-cc0bc634c18a/d0fa26e9-917b05bfdd76e8ce.tmp`

Auch hier stimmt die Zeitangabe der Erstellung des Bildes mit der Zeitangabe der Erstellung des Facebook-Posts überein.

5.10.3 Interpretation

Auch ohne das Vorhandensein des Originalbildes wäre es bei Samsung möglich, das Bild mitsamt den Geokoordinaten auf dem Gerät festzustellen und es einem Facebook-Upload zuzuordnen. Dies ist bei Apple so nicht möglich. Das Bild ist vorhanden, jedoch zeigt die Pfadangabe mit „[…]FBImageDownloader", dass es sich hierbei angeblich um einen Download der angegebenen Datei handelt. Somit kann bei Apple nicht festgestellt werden, dass ein Upload des Bildes über dieses Gerät getätigt wurde.

5.11 Standortmarkierung: Facebook

Neben dem Upload von Bildern können auch Status-Beiträge erstellt werden, welche Angaben zu Standorten haben.

Dieser Standort kann auf zwei verschiedene Arten erstellt werden – manuell und per Ortung. Diese beiden Arten stellen jeweils eine Testvariante dar. Zusätzlich wurde ein Beitrag erstellt, in welchem ein Standort eingegeben wurde, der nicht dem tatsächlichen Standort entspricht.

[26] Siehe Anlage B.10.2

In allen drei Fällen war der tatsächliche Standort das Bürogebäude an der Adresse Talstraße 50 in 71034 Böblingen. Bei der manuellen Auswahl des Standortes kann dieser mit Hilfe der Adresse oder durch Eingabe einer Firma o.ä. eingegeben werden. Im Testszenario wurde „Polizei Böblingen“ in das Suchfeld eingegeben und der Eintrag „Böblingen Polizei“, welcher die Adresse des tatsächlichen Standortes hinterlegt hat, ausgewählt.

Bei der Auswahl des Standortes per Ortung musste vor einer Auswahl die Standortbestimmung aktiviert werden. Als mögliche Standorte werden hier Örtlichkeiten mit Entfernungsangabe angegeben. Aus dieser Liste wurde der Eintrag mit der geringsten Entfernung, hier die McDonalds-Filiale in der Herrenberger Straße in Böblingen, ausgewählt.

Ein letztes Testszenario beinhaltet die manuelle Auswahl eines bewusst falschen Standortes. Hierfür wurde in der Suche im Apple-Gerät nach „Polizei Leonberg“ gesucht und der Eintrag mit der hinterlegten Adresse „Gerhart-Hauptmann-Straße 8, 71229 Leonberg“ ausgewählt. Für das Samsung-Gerät wurde nach „Polizei Ludwigsburg“ gesucht und der Eintrag mit der hinterlegten Adresse „Friedrich-Ebert-Straße 30, 71638 Ludwigsburg“ ausgewählt.

Die Testgeräte wurden ausgelesen und es konnten Standortdaten in den Smartphones festgestellt werden, wie nachfolgende Tabelle verdeutlicht.

Tabelle 32: Upload von Geodaten: Facebook

Testvariante	Standort	Apple	Samsung
Variante 1	Tatsächlicher Standort	nein	nein
	Angegebener Standort	ja	ja
Variante 2	Tatsächlicher Standort	nein	nein
	Angegebener Standort	ja	ja

Testvariante	Standort	Apple	Samsung
Variante 3	Tatsächlicher Standort	nein	nein
	Angegebener Standort	ja	ja

Es konnte bei Testvariante 2 und 3 festgestellt werden, dass der Beitrag, welcher in Testvariante 1 erstellt, jedoch in Facebook nicht gelöscht wurde, ebenfalls in den Daten der Images enthalten ist. Facebook speichert demnach bei einer Neuinstallation bereits vorhandene Daten. Aus den ausgelesenen Daten kann nicht evaluiert werden, ob das überprüfte Gerät zur Erstellung des oder der fraglichen Beiträge genutzt wurde, oder ob die Daten bereits bestehender Beiträge nach der Verknüpfung dieses Gerätes mit dem Facebook-Account von dort nachgeladen wurden.

Die Betrachtung der vorhandenen Datensätze erfolgte mangels der erläuterten Trennbarkeit der Daten jeweils gesammelt.

5.11.1 Analyse Apple iPhone 8

Im Apple-Testgerät konnten die in Facebook angegebenen Standorte im Image festgestellt werden, wie nachfolgendes Bild veranschaulicht. Die tatsächlichen Standorte liegen aber nicht vor.

Bild 44: Standortmarkierung: Facebook - Apple

Die Standorte sind in der nachfolgenden aufgeführten Datenbank gespeichert:

`Apple_iPhone 8 (A1905).zip/root/private/var/mobile/Containers/Data/Application/8754D65F-8F08-4F5E-8C69-CE3E6194AC30/Library/Caches/graphStoreDB/GraphStore_100070915526652.sqlite3-wal`

Die drei Standorte liegen jedoch ohne Datums- und Uhrzeitangabe vor, wohingegen die Facebook-Beiträge mit dem Text und dem Erstellungszeitpunkt in dieser Datenbank festgestellt werden können[27]. Eine Verknüpfung dieser Daten müsste daher nach einer Überprüfung der Inhalte manuell erfolgen.

5.11.2 Analyse Samsung Galaxy S8

Im Samsung-Testgerät konnten die in Facebook angegebenen Standorte im Image festgestellt werden, wie nachfolgendes Bild veranschaulicht. Die tatsächlichen Standorte liegen wiederum nicht vor.

Bild 45: Standortmarkierung: Facebook - Samsung

[27] Siehe Anlage B.11.1

Die Standorte sind in der nachfolgend aufgeführten Datenbank gespeichert:

`data/Root/data/com.facebook.katana/cache/graph_store_cache/100070915526652/GraphStore.sqlite3-wal`

Die drei Standorte liegen jedoch ohne Datums- und Uhrzeitangabe vor, wohingegen die Facebook-Beiträge mit dem Text und dem Erstellungszeitpunkt in dieser Datenbank festgestellt werden können[28]. Eine Verknüpfung dieser Daten müsste daher nach einer Überprüfung der Inhalte manuell erfolgen.

5.11.3 Interpretation

Facebook speichert die erstellten Beiträge in einer Datenbank auf dem Gerät. Hier sind neben dem geschriebenen Text auch die Örtlichkeiten, sowie die ausgewählten Adressen als Geokoordinaten hinterlegt. Es konnten keine weiteren Geodaten abseits dieser festgestellt werden.

Bei diesen Geodaten kann es sich demnach um Standortdaten handeln, an welchen sich das Gerät nicht befunden hat. Für die Ermittlungsführung müssen diese Daten folglich mit Vorsicht betrachtet werden. Diese Daten können, müssen aber nicht, korrekt sein.

5.12 Standortfreigabe: Facebook Messenger

Im Facebook Messenger kann der Standort an einen Freund gesendet werden. Die beiden in Kapitel 4.2.12 beschriebenen Varianten wurden unmittelbar nacheinander durchgeführt.

Die Testgeräte wurden ausgelesen und es konnten Standortdaten in den Smartphones festgestellt werden, wie nachfolgende Tabelle verdeutlicht.

[28] Siehe Anlage B.11.2

Tabelle 33: Standortfreigabe: Facebook Messenger

Testvariante	Apple	Samsung
Empfänger	ja	ja
Sender	ja	ja

5.12.1 Analyse Apple iPhone 8

Im Apple-Testgerät konnten acht Standorte in der UFED-Kategorie Geräteorte festgestellt werden[29]. Vier der Standorte sind vom zuvor durchgeführten Test, bei dem Standorte an das bzw. vom Samsung-Testgerät übermittelt wurden. Bei den verbleibenden vier Standorten handelt es sich um die beiden mit dem Apple-Testgerät im Facebook Messenger gesendeten bzw. empfangenen Standorte - jeweils zwei der Datensätze gehören immer zusammen.

Auffällig ist hierbei, dass jeweils ein Datensatz sowohl die Adresse als auch die Geokoordinaten enthält. Der zweite Datensatz enthält nur die Geokoordinaten. Bei beiden Einträgen liegen die Geokoordinaten in einem falschen Format vor (siehe hierzu Kapitel 5.12.3).

Die Daten mit den Geokoordinaten sind in der nachfolgend aufgeführten Datenbank gespeichert:

`Apple_iPhone 8 (A1905).zip/root/private/var/mobile/Containers/Shared/AppGroup/0BE94256-0B0D-4604-B01E-F65369AE708F/lightspeed-100070915526652.db-wal`

In der Datenbank kann dem Eintrag ein Link zu Google Maps mit dem ausgewählten Standort entnommen werden.

[29] Siehe Anlage B.12.1.

5.12.2 Analyse Samsung Galaxy S8

Im Samsung-Testgerät konnten vier Geräteorte festgestellt werden[30]. Hierbei handelt es sich um die beiden im Facebook Messenger gesendeten bzw. empfangenen Standorte - jeweils zwei der Datensätze gehören immer zusammen.

Hier enthält jeweils ein Datensatz lediglich die Adresse, während der zweite Datensatz die Geokoordinaten im falschen Format enthält (siehe Kapitel 5.12.3).

Die Daten mit den Geokoordinaten sind in der nachfolgend aufgeführten Datenbank gespeichert:

`data/Root/data/com.facebook.orca/databases/threads_db2`

In der Datenbank kann dem Eintrag ein Link zu Google Maps mit dem ausgewählten Standort entnommen werden.

5.12.3 Interpretation

Bezüglich der falsch notierten Geokoordinaten konnte festgestellt werden, dass es sich hierbei offensichtlich um ein Problem von UFED handelt.

Werden die Geokoordinaten in den unter Kapitel 5.12.1 und 5.12.2 aufgeführten Datenbanken überprüft, so liegen diese dort in der korrekten Schreibweise gemäß WGS84 vor.

In nachfolgender Tabelle werden beispielhaft die Geokoordinaten des Standortes „Polizei Leonberg“ aus Kapitel 5.12.1 dargestellt.

[30] Siehe Anlage B.12.2

Tabelle 34: Beispiel der fehlerhaften Geokoordinaten

	Geokoordinaten
Koordinaten aus UFED	(4879848000.000000, 901066000.000000)
Koordinaten aus Datenbank	(48.79848, 9.01066)

Hinsichtlich der Aussagekraft ändert sich jedoch diesbezüglich nichts. Durch die Möglichkeit, den Standort manuell auswählen zu können, können diese Daten nicht ungeprüft übernommen werden. Sie sind eher als Indiz zu bewerten.

Die Fragestellung aus Kapitel 4.2.12, inwieweit sich feststellen lässt, ob der Standort gesendet oder empfangen wurden, lässt sich eindeutig mit ja beantworten. Einerseits kann durch die Verknüpfung mit den zugehörigen Chats eine Zuordnung getroffen werden, andererseits über die Datenbank. In der Tabelle „messages“ sind der Name sowie die User-ID des sendenden Facebook-Accounts hinterlegt, sodass diese Information mit dem auf dem Gerät verknüpften Facebook-Account verglichen werden kann.

5.13 Standortfreigabe: WhatsApp

Im Messenger WhatsApp kann der Standort an einen Kontakt gesendet werden. Aufgrund der Einstellungen muss bei beiden Testgeräten zuerst die Erlaubnis zur Nutzung des Standortes erteilt werden.

Hierfür zeigt WhatsApp den Standort auf einer Google Maps Karte an. Neben der Option „Aktuellen Standort senden“ können auch Orte in der Nähe ausgewählt werden. Die Option „Aktuellen Standort senden“ zeigt direkt an, wie genau der Standort ist.

Tabelle 35: Standortfreigabe: WhatsApp

	Apple	Samsung
Sender	ja	ja
Empfänger	ja	ja

5.13.1 Analyse Apple iPhone 8

Bei der Durchführung des Testszenarios mit dem Apple-Testgerät als Sender der Nachricht konnte festgestellt werden, dass die Genauigkeit des Standortes innerhalb kurzer Zeit zunahm.

So wurde beim Versenden eines ersten Standortes beim iPhone eine Genauigkeit von 1475 Metern angezeigt, beim Versenden eines zweiten Standortes eine Genauigkeit von 16 Metern. Zwischen diesen beiden Vorgängen lagen lediglich wenige Minuten. Zudem fand keine Ortsveränderung statt.

Ein Grund hierfür ist nicht bekannt, jedoch ist zu vermuten, dass mit der Zeit mehr Informationen in die Standortbestimmung einfließen (bspw. A-GPS, siehe Kapitel 2.3) bzw. gegebenenfalls mehr Satelliten empfangen werden.

Die beiden Standorte konnten in den Daten festgestellt werden[31]. Hierbei konnten auch in der Datenbank direkt keine Rückschlüsse auf die in der App angezeigten Genauigkeit gezogen werden.

Bei der Durchführung des Testszenarios mit dem Apple-Testgerät als Empfänger der Nachricht kann der Geostandort ebenfalls in den Daten festgestellt werden. Wie auch bei der Sender-Variante kann hier keine Genauigkeit aus den Daten herausgelesen werden.

[31] Siehe Anlage B.13.1.

Die Daten sämtlicher Geokoordinaten des Apple-Testgerätes sind in der nachfolgend aufgeführten Datenbank gespeichert:

`Apple_iPhone 8 (A1905).zip/root/private/var/mobile/Containers/Shared/AppGroup/FBBA1361-1AB4-469D-B6CB-A1396336F0A2/ChatStorage.sqlite`

5.13.2 Analyse Samsung Galaxy S8

Bei der Durchführung des Testszenarios mit dem Samsung-Testgerät als Sender der Nachricht konnte festgestellt werden, dass in der Kategorie „Geräteorte“ von UFED zwei Datensätze vorhanden sind. Beide sind der Anwendung WhatsApp zuzuordnen. Bei einem der beiden Datensätze handelt es sich um den als Nachricht gesendeten Standort. Beim zweiten Datensatz, welcher chronologisch nach dem eigentlichen Datensatz geschrieben wurde, handelt es sich um einen Datensatz ohne Geokoordinaten.

Wie bei dem Apple-Testgerät konnten auch in der Datenbank des Samsung-Testgerätes keine Rückschlüsse auf die in der App angegebene Genauigkeit gezogen werden.

Der durch das Samsung-Testgerät empfangene Standort konnte ebenfalls in den Daten festgestellt werden. Wie auch bei der Sender-Variante kann hier keine Genauigkeit aus den Daten herausgelesen werden.

Die Daten mit den Geokoordinaten sind in der nachfolgend aufgeführten Datenbank gespeichert[32]:

`data/Root/data/com.whatsapp/databases/msgstore.db-wal`

[32] Siehe Anlage B.13.2.

5.13.3 Interpretation

Bei beiden Testgeräten konnten Geodaten von beiden Testvarianten in den Images festgestellt werden. Für die Analyse der Daten bedeutet dies, dass nicht nur die Geodaten, sondern ebenfalls die zugehörigen Chats betrachtet werden müssen, damit die Daten nicht falsch interpretiert werden.

Bei den Daten des Apple-Testgerätes als Empfänger des Standortes konnte festgestellt werden, dass UFED die Daten als „Extern“ angibt. In den Daten aus der WhatsApp-Datenbank „ChatStorage.sqlite“ konnte die Spalte „ZISFROMME“ festgestellt werden, welche UFED verwendet, um den Datensatz als „Extern“ zu kennzeichnen. Hier steht der Wert „0“ für eine eingehende, der Wert „1“ für eine ausgehende Nachricht.

Für Android-Geräte konnte mit Hilfe der Quelle [47] in der Datenbank „msgstore.db“, Tabelle „messages“ die Spalte „key_from_me“ als potentieller Identifier ausgemacht werden. Diese gibt an, ob es sich um eine ein- bzw. ausgehende Nachricht handelt. In den beiden erstellten Images dieses Testszenarios konnte dies nicht nachvollzogen werden, da die Werte vom System noch nicht von der „sql-wal“- in die „sql“-Datenbank transferiert wurden.

Generell können die Daten, wenn ausgeschlossen werden kann, dass diese empfangen wurden, im Rahmen eines Ermittlungsverfahrens verwendet werden. Da die Genauigkeit der Daten, welche WhatsApp beim Sender angibt, nicht gespeichert werden, können jedoch diese Werte jedoch nicht in die Interpretation mit einfließen. Wie generell bei Geodaten muss also beachtet werden, dass der tatsächliche Standort abweichen kann.

5.14 Live-Standortfreigabe: WhatsApp

Neben der im vorherigen Kapitel beschriebenen Standortfreigabe kann der Live-Standort für 15 Minuten, 1 Stunde oder 8 Stunden mit einem Gesprächspartner geteilt werden. Für das Testszenario mit den Varianten

wurde die Standardeinstellung von einer Stunde gewählt. Nach Durchführung des Tests wurde die Freigabe vor Ablauf der Stunde abgebrochen.

Um das Testszenario mit den in Kapitel 4.2.14 beschriebenen Testvarianten durchzuführen, wurden jeweils beide Testgeräte für die Tests verwendet. Im Testaufbau 1 wurde das Samsung-Testgerät als Sender- und das Apple-Testgerät als Empfänger des Livestandortes verwendet. Im Testaufbau 2 erfolgte die Durchführung dann umgekehrt.

Nach erfolgter Durchführung und Analyse konnte festgestellt werden, dass beide Testgeräte Daten gespeichert haben, jedoch nicht den Routenverlauf:

Tabelle 36: Live-Standortfreigabe: WhatsApp

	Apple	**Samsung**
Sender	ja	ja
Sender - Routenverlauf	nein	nein
Empfänger	ja	ja
Empfänger - Routenverlauf	nein	nein

5.14.1 Analyse Apple iPhone 8

Bei der Durchführung des Testszenarios mit dem Apple-Testgerät als Sender des Live-Standortes konnte festgestellt werden, dass in den UFED-Daten nur ein Geodatensatz der Anwendung WhatsApp zugeordnet werden kann. Es handelt sich hierbei um den Standort zum Zeitpunkt des Startes des Live-Standorts.

Neben den Standortdaten aus WhatsApp konnten im Apple-Testgerät weitere Geostandorte festgestellt werden, welche nicht der App WhatsApp zugeordnet sind. Hierbei handelt es sich um automatisch erzeugte Geodaten, welche bereits in Kapitel 5.1.1 erläutert wurden. Diese stehen demnach

nicht im Zusammenhang mit dem durchgeführten Test und können auch nicht manuell zugeordnet werden.

In den Daten des Images des Apple-Testgerätes als Empfänger des Live-Standortes konnte ein Datensatz mit Geokoordinaten festgestellt werden. Diese Koordinaten entsprechen den Koordinaten des Standortes des sendenden Gerätes zum Startzeitpunkt des Live-Standortes.

Auffällig ist hierbei, dass dieser Datensatz, im Gegensatz zu dem Datensatz des Apple-Testgerätes als Sender und den beiden Datensätzen des Samsung-Testgerätes, einen Endzeitpunkt hat.

Die Daten mit den Geokoordinaten sind bei beiden Varianten in der nachfolgend aufgeführten Datenbank gespeichert[33]:

`Apple_iPhone 8 (A1905).zip/root/private/var/mobile/Containers/Shared/AppGroup/FBBA1361-1AB4-469D-B6CB-A1396336F0A2/ChatStorage.sqlite-wal`

5.14.2 Analyse Samsung Galaxy S8

Bei der Durchführung des Testszenarios mit dem Samsung-Testgerät als Sender des Live-Standortes konnte festgestellt werden, dass in den UFED-Daten nur ein Geodatensatz enthalten ist. Es handelt sich hierbei um den Standort zum Zeitpunkt des Startes des Live-Standorts.

In den Daten des Images des Samsung-Testgerätes als Empfänger des Live-Standortes konnte ein Datensatz mit Geokoordinaten festgestellt werden. Diese Koordinaten entsprechen den Koordinaten des Standortes des sendenden Gerätes zum Startzeitpunkt des Live-Standortes.

Die Ergebnisse entsprechen also denen aus dem Apple-Testgerät.

[33] Siehe Anlage B.14.1

Die Daten mit den Geokoordinaten sind bei beiden Varianten in der nachfolgend aufgeführten Datenbank gespeichert[34]:

`data/Root/data/com.whatsapp/databases/msgstore.db-wal`

5.14.3 Interpretation

In den Daten konnte die Route des sendenden Gerätes weder im Apple- noch im Samsung-Testgerät festgestellt werden. Hier wurde durch WhatsApp lediglich der Startpunkt in der Datenbank gespeichert. Dementsprechend konnten in den empfangenden Geräten ebenfalls nur die Geokoordinaten des Startes festgestellt werden.

In der Datenbank des Apple- und des Samsung-Testgerätes konnten keine Hinweise gefunden werden, dass es sich bei den Datensätzen um Live-Standortfreigaben handelt.

Die bei der Freigabe des Live-Standortes automatisch erzeugte Chatnachricht wurde zwar jeweils in den Images festgestellt, aber auch aus ihr ließ sich nicht ableiten, dass es sich um einen Live-Standort handelte.

[34] Siehe Anlage B.14.2

6 Fazit und Ausblick

Geodaten - ein Wundermittel bei modernen Ermittlungsverfahren?

In Ermittlungsverfahren können Geodaten nur dann sinnvoll einfließen, wenn die in Kapitel 1.2 aufgeworfenen Fragen beantwortet werden können. Was passiert, wenn Geodaten in Form von Metadaten versendet werden? Können diese auf dem Empfängergerät festgestellt werden? Wie verhält es sich auf den Testgeräten, wenn Standorte per Messenger verschickt oder Standorte in Social-Media-Plattformen getaggt wurden? Und wie genau sind Geodaten auf Smartphones generell? Kann anhand derer mit großer Sicherheit gesagt werden, wo jemand sich aufgehalten hat? Könnten diese Daten demnach für eine falsche Interpretation sorgen und einen potentiellen Tatverdächtigen fälschlicherweise be- bzw. entlasten? Fragen die im Rahmen dieser Masterthesis beantwortet werden können.

Mit Hilfe der durchgeführten Testszenarien konnte festgestellt werden, dass die in Bildern in Form von Exif-Informationen enthaltenen Geodaten meistens nicht auf dem Empfängergerät gespeichert werden. Eine Ausnahme hiervon bildet dabei die Übertragung der Bilder als Anhang zu einer E-Mail - hier konnten alle Metadaten auf dem Empfängergerät festgestellt werden.

Diesbezüglich besteht daher kaum eine Gefahr für Fehlinterpretationen. In den meisten Fällen sind keine Geodaten vorhanden und bei der Versendung als E-Mail-Anhang ist die Herkunft des Geodatums einfach und sicher nachweisbar.

Das Versenden von Geokoordinaten kann jedoch auch bewusst in Form von Standortfreigaben durchgeführt werden. So kann auf der Social-Media-Plattform Facebook der Standort in einem Beitrag getaggt werden, oder der Standort kann über die Messenger-Dienste Facebook Messenger oder WhatsApp an einen Kontakt versendet werden.

Dabei kann in einem Facebook-Beitrag jedoch nicht nur der tatsächliche, sondern auch ein fiktiver Standort angegeben werden. Bei einer Untersuchung des Testgerätes konnte festgestellt werden, dass nur der angegebene Standort, nicht aber der tatsächliche Standort, in den Daten gespeichert ist. Wenn also in einem Facebook-Beitrag ein fiktiver Standort angegeben wird, an welchem sich die Person zu diesem Zeitpunkt nicht befunden hat, kann dies zu falschen Rückschlüssen führen.

Über den zu Facebook gehörenden Messenger Facebook Messenger konnten die als Standort freigegebenen Geodaten sowohl auf dem sendenden, als auch auf dem empfangenden Testgerät festgestellt werden. Eine Zuordnung der Daten ist in UFED unter Zuhilfenahme des Chatverlaufes einfach und sicher möglich. Auch hier können fiktive Standorte übermittelt werden, sodass dieser Umstand in die Bewertung der Daten einfließen muss.

Über den Messenger WhatsApp können sowohl ein einmaliger Standort, als auch die Standorte für einen gewissen Zeitraum übermittelt werden. Hierbei könnte man davon ausgehen, dass viele Datensätze mit Geokoordinaten vorliegen. In den Testszenarien konnte jedoch festgestellt werden, dass lediglich ein Geodatum zum Start-Zeitpunkt festgehalten wird. Somit ist für alle Tests mit der Standortfreigabe bei WhatsApp jeweils nur ein Datensatz vorhanden, welcher sowohl auf dem Empfänger-, als auch auf dem Sender-Testgerät festgestellt werden konnte. Beim Vergleich der Datenbanken konnte kein Unterschied zwischen der Standortfreigabe und der Live-Standortfreigabe festgestellt werden. Für die Analyse und Interpretation der Daten lässt sich somit nicht sagen, um welche Art von Freigabe es sich gehandelt hat. Eine Unterscheidung zwischen Sender und Empfänger scheint aber sicher möglich.

Hinsichtlich der generellen Genauigkeit von Geodaten konnte festgestellt werden, dass die Abschattung (siehe Kapitel 2.3) eine große Rolle spielt und dass bereits geringfügige Ortsveränderungen zu einer großen Abweichung des Standortes führen können.

Im Rahmen dieser Masterthesis wurden neben der generellen Genauigkeit von Geodaten auch die Genauigkeit der Geodaten im Google Standortverlauf betrachtet. Die durch Google angegebenen Werte waren bei der Überprüfung von fünf Testdaten als ungenauer angegeben, als sie tatsächlich waren. Hierbei handelt es sich jedoch nur um Abweichungen von wenigen Metern, sodass diese Daten in einem Ermittlungsverfahren sehr wertvoll sein können.

Die Genauigkeit der in den Bildern gespeicherten Geokoordinaten sind von vielen Faktoren abhängig und sind dadurch oftmals nicht exakt. Für die Interpretation bedeutet dies, dass weitere Faktoren wie beispielsweise das Wetter zum Aufnahmezeitpunkt und der Geländeverlauf mit einbezogen werden müssen. Hierzu ist selbstverständlich auch eine detaillierte Überprüfung des Bildes an sich erforderlich.

Generell kann die am Anfang des Fazits gestellte Frage mit „ja“ beantwortet werden. Ja, Geodaten können ein Wundermittel sein. Aber nur wenn diese im Detail betrachtet und analysiert werden. Je wichtiger die Daten im Ermittlungsverfahren sind, desto wichtiger ist eine in die Tiefe gehende Analyse.

Die im Rahmen dieser Masterthesis durchgeführten Testszenarien ergaben einen kleinen Einblick in die große Welt der auf Smartphones erzeugten Geodaten. Aufgrund der Vielfältigkeit an Smartphone-Modellen und Software-Versionen sind die hier erlangten Ergebnisse nicht sicher 1:1 übertragbar. Hierfür müssen diese Tests auf weiteren Geräten und auch mit anderen Software-Versionen durchgeführt werden. Die Durchführung der Testszenarien mit verschiedener Forensik-Software bietet sich ebenfalls an, um eventuelle Unterschiede feststellen zu können.

Die hier betrachteten Apps sind nur eine Auswahl für die jeweilige Kategorie. So gehören neben WhatsApp und Facebook Messenger unter anderem auch Threema, Telegram und Signal zu den häufig verwendeten Messengern.

Bei der Durchführung der Testszenarien konnte festgestellt werden, dass auf dem Apple-Testgerät deutlich mehr Geodaten gespeichert wurden, als auf dem Samsung-Testgerät (siehe Kapitel 5.1.1). Hier stellt sich die Frage, wie lang diese Daten dauerhaft in der internen Apple-Datenbank gespeichert werden, oder ob es sich hierbei um eine Art Ringspeicher handelt. Werden die ältesten Daten überschrieben, sobald die Datenbank eine gewisse Größe erreicht hat ist, oder werden die Daten nach einer gewissen Zeit automatisch entfernt?

Der Hersteller Apple bietet die Möglichkeit verschiedene Geräte miteinander zu synchronisieren. Hierbei werden unter anderem auch Bilder synchronisiert. Wie wirkt sich diese Synchronisation auf die Geodaten von Bildern und auch auf die enthaltenen Geodaten generell aus?

Bei der Durchführung des Testszenarios der Standortmarkierung bei Facebook (siehe Kapitel 5.11) konnte eine in der vorliegenden Thesis nicht betrachtete Fragestellung identifiziert werden, welche ebenfalls interessant erscheint: Können Standortdaten in einem Image festgestellt werden, wenn bei einem Nutzer ein Beitrag von Freunden in seiner Timeline erscheint, in welchem ein Standort markiert wurde? Und wenn ja, geht aus diesen Daten hervor, dass die Geodaten von einem anderen Facebook-Nutzer stammen?

Abschließend kann festgehalten werden, dass es sich bei dem hier betrachteten Thema um nicht nur ein interessantes, sondern auch für die polizeiliche Ermittlungsarbeit wichtiges Thema handelt.

Aufgrund der vielfältigen Kombinationen aus Smartphone-Modellen und Betriebssystemen bzw. Versionen einerseits, sowie unterschiedlichen Apps andererseits gilt es mit der stetigen Entwicklung in diesem Bereich Stand zu halten und die hier überprüften Fragestellungen gegebenenfalls erneut zu prüfen.

7 Literaturverzeichnis

[1] inside-intermedia Digital GmbH, „Zeitreise: So wurde aus dem Handy ein Smartphone," 08. November 2020. [Online]. Verfügbar unter: https://www.inside-digital.de/ratgeber/zeitreise-so-wurde-aus-dem-handy-ein-smartphone. [Zugriff am 02. Juni 2021].

[2] GSMArena.com, „Apple iPhone 3G," [Online]. Verfügbar unter: https://www.gsmarena.com/apple_iphone_3g-2424.php. [Zugriff am 03. Juni 2021].

[3] Statista GmbH: F. Tenzer, „Anteil der privaten Haushalte in Deutschland mit einem Mobiltelefon von 2000 bis 2020," 10. November 2020. [Online]. Verfügbar unter: https://de.statista.com/statistik/daten/studie/198642/umfrage/anteil-der-haushalte-in-deutschland-mit-einem-mobiltelefon-seit-2000/#statisticContainer. [Zugriff am 03. Juni 2021].

[4] Statistika GmbH: F. Tenzer, „Statistiken zur Smartphone-Nutzung in Deutschland," 07. April 2021. [Online]. Verfügbar unter: https://de.statista.com/themen/6137/smartphone-nutzung-in-deutschland/. [Zugriff am 07. August 2021].

[5] Statistika GmbH: Statista Research Department, „Bevölkerung - Einwohnerzahl von Deutschland von 1990 bis 2020," 21. Juni 2021. [Online]. Verfügbar unter: https://de.statista.com/statistik/daten/studie/2861/umfrage/entwicklung-der-gesamtbevoelkerung-deutschlands/. [Zugriff am 07. August 2021].

[6] A. Dhein, „Absicherung der analytischen Interpretation von Geolokalisierungsdaten in der Mobilfunkforensik," Universität Koblenz-Landau, https://kola.opus.hbz-nrw.de/opus45-kola/frontdoor/deliver/index/docId/2005/file/diss_adhein_pub_bib.pdf, 2018.

[7] T. Lakes, „Geodaten," Springer VS, Wiesbaden, 2019. [Online]. Verfügbar unter: https://doi.org/10.1007/978-3-658-21308-4_99. [Zugriff am 22. Mai 2021].

[8] L. f. G. u. L. Baden-Württemberg, „Geoportal Baden-Württemberg," [Online]. Verfügbar unter: https://www.geoportal-bw.de/glossar_g. [Zugriff am 22. Mai 2021].

[9] Huber Kartographie GmbH, „Kartographie," Huber Kartographie GmbH, [Online]. Verfügbar unter: http://kartographie.de/p4/g19/geoinformation. [Zugriff am 22. Mai 2021].

[10] G. Retscher und M. Kistenich, „Vergleich von Systemen zur Positionsbestimmung und Navigation in Gebäuden," *zfv – Zeitschrift für Geodäsie, Geoinformation und Landmanagement,* 1 2006.

[11] Conrad Electronic SE, „GPS » Global Positioning System, Satellitennavigation erklärt," [Online]. Verfügbar unter: https://www.conrad.de/de/ratgeber/technik-einfach-erklaert/gps.html. [Zugriff am 30. Mai 2021].

[12] inside-intermedia Digital GmbH, „GPS-Alternativen: Diese Vorteile bieten Glonass, Galileo, Beidou & Co.," 07. August 2021. [Online]. Verfügbar unter: https://www.inside-digital.de/ratgeber/gps-alternativen-glonass-galileo-beidou. [Zugriff am 20. August 2021].

[13] L. Bauer, „Koordinaten Umrechner,“ [Online]. Verfügbar unter: https://www.koordinaten-umrechner.de/decimal/53.889545,11.444584?karte=OpenStreetMap&zoom=17. [Zugriff am 30. Mai 2021].

[14] inside-intermedia Digital GmbH, „Wie funktioniert GPS? Alles Wissenswerte zum Ortungssystem,“ 21. November 2020. [Online]. Verfügbar unter: https://www.inside-digital.de/ratgeber/gps-erklaert-alles-wissenwerte-zum-ortungssystem. [Zugriff am 30. Mai 2021].

[15] D. Labudde und M. Spranger, Forensik in der digitalen Welt, Berlin: Springer-Verlag GmbH, 2017.

[16] Bundesamt für Sicherheit in der Informationstechnik, „Leitfaden „IT-Forensik“,“ Bonn, 2011.

[17] D. Muth, „Leitfaden zur forensischen Untersuchung von Android Smartphones,“ 2013. [Online]. Verfügbar unter: https://dasec.h-da.de/wp-content/uploads/2013/08/muth-denise-masterarbeit-ss131.pdf.

[18] A. Mühlroth, „Wie viel Speicher braucht ein Smartphone wirklich?,“ Techbook, 02. Juni 2021. [Online]. Verfügbar unter: https://www.techbook.de/mobile/smartphones/wieviel-speicher-smartphone. [Zugriff am 28. August 2021].

[19] Nydus AG, „Android-Smartphone mit 20GB RAM - das erste Mobilgerät ist da,“ 19. August 2021. [Online]. Verfügbar unter: https://nydus.org/news/124742.html. [Zugriff am 28. August 2021].

[20] M. Mierke, „SD-Karte als interner Speicher - so geht's unter Android,“ Heise, 23. August 2021. [Online]. Verfügbar unter: https://www.heise.de/tipps-tricks/SD-Karte-als-interner-Speicher-

so-geht-s-unter-Android-4458642.html. [Zugriff am 29. August 2021].

[21] Telekom Deutschland GmbH, „SIM-Karten-Formate: Alles rund um Mini, Micro und Nano," [Online]. Verfügbar unter: https://www.telekom.de/unterwegs/sim-karten-formate. [Zugriff am 29. August 2021].

[22] Statista, „Apple or Android Nation? Operating System Popularity Across Countries," 26. August 2020. [Online]. Verfügbar unter: https://www.statista.com/chart/22702/andoid-ios-market-share-selected-countries/. [Zugriff am 30. August 2021].

[23] Diffen, „Android vs. iOS," [Online]. Verfügbar unter: https://www.diffen.com/difference/Android_vs_iOS. [Zugriff am 30. August 2021].

[24] Statista, „Anzahl der verfügbaren Apps in den Top App-Stores im 1. Quartal 2021," Mai 2021. [Online]. Verfügbar unter: https://de.statista.com/statistik/daten/studie/208599/umfrage/anzahl-der-apps-in-den-top-app-stores/. [Zugriff am 30. August 2021].

[25] Nexpit, „So lange gibt's Android-Updates bei Samsung, Xiaomi & Co.!," 2021. [Online]. Verfügbar unter: https://www.nextpit.de/wie-lange-android-updates. [Zugriff am 30. August 2021].

[26] Cellebrite, „What Happens When You Press that Button?," [Online]. Verfügbar unter: https://pdf4pro.com/view/what-happens-when-you-press-that-button-43f87f.html. [Zugriff am 27. Juni 2021].

[27] Special Counsel, „3 Methods of Mobile Device Extractions and the Data Each Contains," 03. März 2016. [Online]. Verfügbar unter: https://blog.specialcounsel.com/ediscovery/three-types-of-mobile-

device-extractions-and-what-each-contains/. [Zugriff am 27. Juni 2021].

[28] C. Hesseling, „Ich sehe was, was du nicht siehst: Metadaten in Fotos," 05. November 2015. [Online]. Verfügbar unter: https://irights.info/artikel/metadaten-fotos-anbringen-loeschen-bearbeiten/26353. [Zugriff am 03. Juli 2021].

[29] Samsung, „Specifications," [Online]. Verfügbar unter: https://www.samsung.com/global/galaxy/galaxy-s8/specs/. [Zugriff am 18. September 2021].

[30] DeviceSpecifications, „Apple iPhone 8 - Technische Daten und Spezifikationen," [Online]. Verfügbar unter: https://www.devicespecifications.com/de/model/d85c45ac. [Zugriff am 18. September 2021].

[31] Cellebrite, „Cellebrite UFED," Cellebrite, [Online]. Verfügbar unter: https://www.cellebrite.com/de/cellebrite-ufed-de/. [Zugriff am 03. September 2021].

[32] QGIS Development Team, „QGIS - Das führende Open-Source-Desktop-GIS," [Online]. Verfügbar unter: https://www.qgis.org/de/site/about/index.html. [Zugriff am 02. September 2021].

[33] Statista, „Cumulative number of monthly Facebook product users as of 2nd quarter 2021," Juli 2021. [Online]. Verfügbar unter: https://www.statista.com/statistics/947869/facebook-product-mau/. [Zugriff am 09. Oktober 2021].

[34] Facebook, [Online]. Verfügbar unter: https://static.xx.fbcdn.net/rsrc.php/y8/r/dF5SId3UHWd.svg. [Zugriff am 09. Oktober 2021].

[35] WhatsApp, „Über WhatsApp," [Online]. Verfügbar unter: https://www.whatsapp.com/about. [Zugriff am 09. Oktober 2021].

[36] WhatsApp, [Online]. Verfügbar unter: https://static.whatsapp.net/rsrc.php/ym/r/36B424nhiL4.svg. [Zugriff am 09. Oktober 2021].

[37] Snap Inc., „Snap Inc. Announces Second Quarter 2021 Financial Results," [Online]. Verfügbar unter: https://s25.q4cdn.com/442043304/files/doc_financials/2021/q2/Q2%E2%80%9921-Earnings-Release-Final_7.22.21.pdf. [Zugriff am 09. Oktober 2021].

[38] Logos-World, „Snapchat Logo," 14. August 2021. [Online]. Verfügbar unter: https://logos-world.net/snapchat-logo/. [Zugriff am 09. Oktober 2021].

[39] Apple, „Mach dich auf den besten Weg.," [Online]. Verfügbar unter: https://www.apple.com/de/maps/. [Zugriff am 09. Oktober 2021].

[40] Techbook, „Das ist die Geschichte hinter Google Maps," 06. Februar 2020. [Online]. Verfügbar unter: https://www.techbook.de/apps/google-maps-geschichte. [Zugriff am 09. Oktober 2021].

[41] Computerbild, „Google: Nutzerzahlen des Internetriesen im Überblick," 29. April 2021. [Online]. Verfügbar unter: https://tipps.computerbild.de/internet/suchmaschinen/google-nutzerzahlen-765589.html. [Zugriff am 09. Oktober 2021].

[42] AppleInsider, „Apple Maps," [Online]. Verfügbar unter: https://appleinsider.com/inside/apple-maps. [Zugriff am 10. Oktober 2021].

[43] Apple, „Apple delivers all-new Apple Maps across Canada," [Online]. Verfügbar unter: https://www.apple.com/ca/newsroom/2020/12/apple-delivers-all-new-apple-maps-across-canada/. [Zugriff am 10. Oktober 2021].

[44] GMX, „Geschichte," [Online]. Verfügbar unter: https://web.archive.org/web/20120527143642/http://www.gmx.net/presse/geschichte.html. [Zugriff am 10. Oktober 2021].

[45] GMX, „Neuer Rekordwert: Portale WEB.DE und GMX werden immer stärker genutzt," [Online]. Verfügbar unter: https://newsroom.gmx.net/2020/07/08/neuer-rekordwert-portale-web-de-und-gmx-werden-immer-staerker-genutzt/. [Zugriff am 10. Oktober 2021].

[46] GMX, „Impressum," [Online]. Verfügbar unter: https://www.gmx.net/impressum/. [Zugriff am 10. Oktober 2021].

[47] I. Mikhailov, „WhatsApp in Plain Sight: Where and How You Can Collect Forensic Artifacts," 07. November 2019. [Online]. Verfügbar unter: https://blog.group-ib.com/whatsapp_forensic_artifacts. [Zugriff am 28. Oktober 2021].

[48] Meinberg, [Online]. Verfügbar unter: https://www.meinberg.de/images/news/xsatellite-systems.jpg.pagespeed.ic.3KpEvdP0Pt.jpg.

[49] ifolor, „ISO im Detail erklärt – Lichtempfindlichkeit von Kameras," [Online]. Verfügbar unter: https://www.ifolor.ch/inspirationen/iso-im-

detail-erklart-lichtempfindlichkeit-von-kameras. [Zugriff am 26. Oktober 2021].

[50] GTK Electronics GmbH, „Kapazitive Touchscreens für Displays," [Online]. Verfügbar unter: https://www.gtkgmbh.de/produkte/displays/display-massgeschneidert-und-zubehoer/kapazitive-touchscreens. [Zugriff am 11. September 2021].

8 Bilderverzeichnis

9 Tabellenverzeichnis

10 Anlagen

11 Verzeichnis der Abkürzungen

A-GPS ..... *Assisted-Global Positioning System*
API ..... *Application Programming Interface*
App ..... *Applikation*
BNetzA ..... *Bundesnetzagentur*
BSI ..... *Bundesamt für Sicherheit in der Informationstechnologie*
EMF ..... *Elektromagnetische Felder*
Exif ..... *Exchangeable Image File Format*
GIS ..... *Geoinformationssytem*
GLONASS ..... *Global Navigation Satellite System*
GPS ..... *Global Positioning System*
ISO ..... International Organization for Standardization
JPEG ..... *Joint Photographic Experts Group*
KB ..... *Kilobyte*
LTE ..... *Long Term Evolution*
ÖNPV ..... *Öffentlicher Personennahverkehr*
OS ..... *Operating System*
PIN ..... *Personal Identification Number*
PUK ..... *Personal Unblocking Key*
RAM ..... *Random Access Memory*
SD-Karten ..... *Secure Digital Memory Card*
SIM ..... *Subscriber Identity Module*
TAC ..... *Type Allocation Code*
TB ..... *Terabyte*
TIFF ..... *Tagged Image File Format*
UFED ..... *Universal Forensic Extraction Device*
WLAN ..... *Wireless Local Area Network*

12 Selbstständigkeitserklärung

Hiermit erkläre ich, dass ich die hier vorliegende Arbeit selbstständig, ohne unerlaubte fremde Hilfe und nur unter Verwendung der in der Arbeit aufgeführten Hilfsmittel angefertigt habe.

Renningen, 06.11.2021

13 Thesen

1. Pauschale Aussagen zur Genauigkeit eines bestimmen GPS-Empfängers sind nicht möglich
2. Der Geländeverlauf und das Wetter beeinflussen die Abschattung des GPS-Signals und beeinflussen somit die Genauigkeit von Geokoordinaten
3. Bereits ein geringfügiger Standortwechsel kann daher zu einer starken Abweichung führen
4. Durch die Feststellung von Geodaten auf einem Smartphone kann nicht automatisch darauf geschlossen werden, dass diese auch auf diesem Gerät erzeugt wurden und das Smartphone sich zu dieser Zeit an diesem Ort befand
5. Das Verhalten hängt nicht nur vom Betriebssystem, sondern auch von den verwendeten Apps und der jeweiligen Version ab, sodass Aussagen grundsätzlich nur für eine bestimmte Version gelten können
6. Exif-Daten von Fotos sind nach dem Versenden über die getesteten Messenger nicht mehr vorhanden
7. Die Verwendung eines Smartphones zur Navigation erzeugt kaum Spuren auf dem Gerät
8. Aus den Einträgen in den WhatsApp-Datenbanken kann nicht zwischen der Einmalfreigabe und der Live-Standortfreigabe unterschieden werden
9. In kritischen Fällen müssen die Feststellungen über Tests mit einem baugleichen Smartphone und identischen Software-Versionen überprüft werden
10. Geodaten müssen grundsätzlich genau hinterfragt und überprüft werden

A Vorgehensweise bei der Testdurchführung

Der nachfolgend aufgeführte verallgemeinerte Ablauf hat sich m Rahmen dieser Masterthesis für die Durchführung von Testszenarien samt anschließender Analyse der gewonnen Daten mittels UFED bewährt.

1. Festlegung eines Testszenarios
2. Testgerät: Rücksetzen auf Werkseinstellung und Neueinrichtung
3. Durchführung des Testszenarios
4. Erstellung des Images durch UFED
5. Analyse der Daten in UFED
    a. Betrachtung der vorgegebenen Kategorien durch UFED
        i. Geräteorte
        ii. Bei Messenger: Chats
        iii. Bei Social Media: Soziale Netzwerke
    b. Betrachtung der Datenbanken
    c. Suche nach Anwendungsname im Suchfenster

B Analyse der Testszenarien

Nach Durchführung der Testszenarien ergibt sich nachfolgende Übersicht der Ergebnisse:

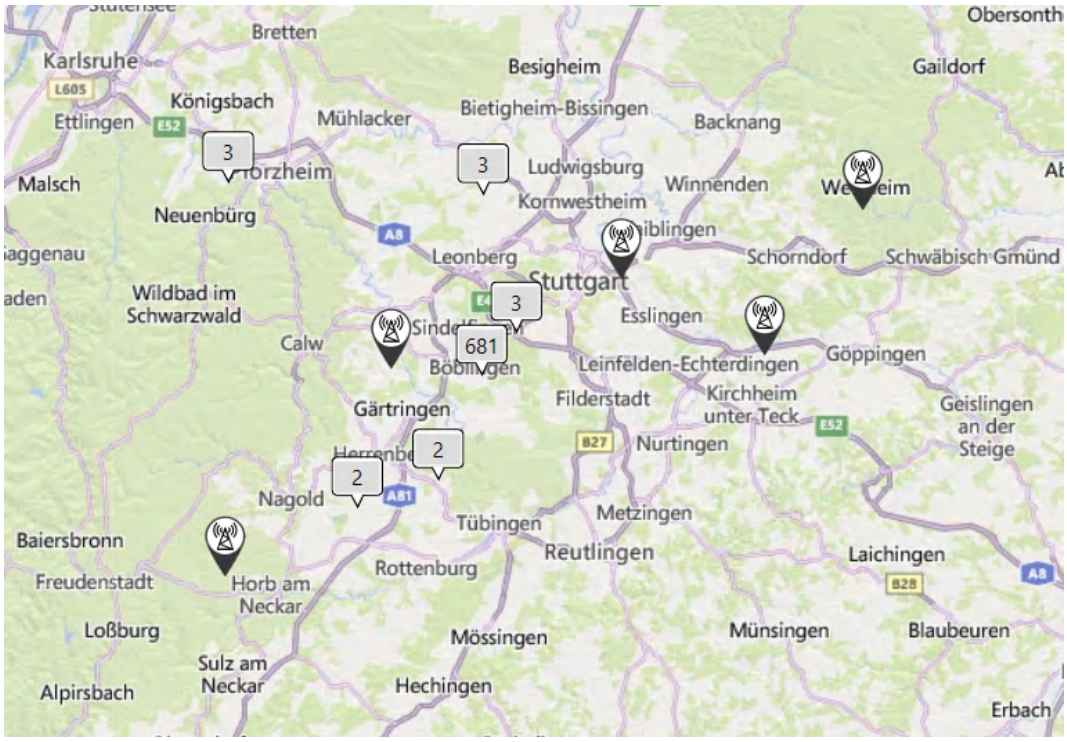
Testszenario	Variante	Apple	Samsung
Speicherung von Geodaten	-	ja	nein
Navigation	-	ja	nein
Suche: Google	-	ja	nein
Versand von Geodaten: E-Mail	Bilddownload	nein	ja
	Bildvorschau	ja	ja
Versand von Geodaten: WhatsApp	-	nein	nein
Versand von Geodaten: Facebook Messenger	Bildvorschau	nein	nein
	Bilddownload	nein	nein
Versand von Geodaten: Snapchat	-	nein	nein
Upload von Geodaten: Facebook	-	nein	ja
Standortmarkierung: Facebook	Manuelle Auswahl	ja	ja
	Auswahl per Ortung	ja	ja
	Falscher Standort	ja	ja
Standortfreigabe: Facebook Messenger	Empfänger	ja	ja
	Sender	ja	ja

Testszenario	Variante	Apple	Samsung
Standortfreigabe: WhatsApp	Empfänger	ja	ja
	Sender	ja	ja
Live-Standortfreigabe: WhatsApp	Sender	ja	ja
	Sender - Routenverlauf	nein	nein
	Empfänger	ja	ja
	Empfänger - Routenverlauf	nein	nein

In den folgenden Unterkapiteln finden sich weitere Informationen zu den in der Masterthesis durchgeführten und beschriebenen Testszenarien.

B.1 Testszenario 1 – Speicherung von Geodaten

Die auf der groben Übersicht angezeigten Datensätze der durch das Apple-Testgerät gespeicherten Daten in Europa liegen bei genauerer Betrachtung allesamt in Deutschland. Diese werden in nachfolgender Grafik dargestellt. Hierbei werden die angegebenen Kategorien der Datensätze nicht berücksichtig.



B.2 Testszenario 2 – Genauigkeit von Geodaten: Metadaten v. Bildern

B.2.1 Berechnungen der Genauigkeiten

Mit Hilfe der in der Masterthesis vorgestellten Formel lassen sich Entfernungen zwischen zwei Geokoordinaten berechnen.

Hierfür werden die tatsächlichen Geokoordinaten zum Zeitpunkt der Erstellung des Bildes benötigt:

Name Bild	Längengrad (tatsächlich)	Breitengrad (tatsächlich)
Sonnenblume	8,90	48,77
Blume	8,92	48,75
Reh	9,04	49,02
Bär	9,04	49,02
Cola-Flasche	9,00	48,68
Büro	9,00	48,68
Torte	8,90	48,77
Nachtisch	8,90	48,77

Zudem werden die Geokoordinaten der in den Bildern enthaltenen Exif-Daten in die Berechnung miteinbezogen:

Name Bild	Längengrad (Bild)	Breitengrad (Bild)
Sonnenblume	8,90	48,77
Blume	8,92	48,75
Reh	9,05	49,03
Bär	9,04	49,02
Cola-Flasche	9,00	48,68
Büro	8,99	48,68
Torte	8,90	48,77
Nachtisch	8,90	48,77

Anhand dieser Daten werden drei Hilfsvariablen dx, dy und lat berechnet:

Name Bild	Hilfsvariable dx	Hilfsvariable dy	lat
Sonnenblume	0,002	-0,000	0,851
Blume	0,00	0,00	0,85
Reh	-0,59	-0,55	0,85
Bär	0,01	-0,00	0,85
Cola-Flasche	0,00	0,06	0,84
Büro	0,51	-0,24	0,84
Torte	0,38	0,08	0,85
Nachtisch	-0,00	-0,00	0,85

Mit diesen Werten kann die Entfernung zwischen den beiden Geokoordinaten berechnet werden:

Name Bild	Entfernung in KM	Entfernung in M
Sonnenblume	0,00261998	2,619979913
Blume	0,00494643	4,94643275
Reh	0,81174958	811,74957784
Bär	0,01490496	14,90496274
Cola-Flasche	0,06476963	64,76962847
Büro	0,57299501	572,99500741
Torte	0,39536650	395,36649942
Nachtisch	0,00026221	0,26220941

Die Werte der Berechnung der Entfernung in Metern sind mit Rundung auf eine Nachkommastelle in die Masterthesis übernommen worden.

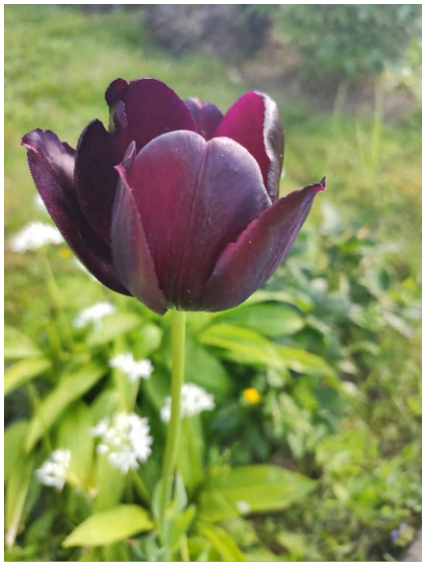
B.2.2 Bildstandort „Freier“ Himmel

Bild Sonnenblume

IMG_20210809_163458.jpg - EXIF Info

EXIF Tag	Value
Filename	IMG_20210809_163458.jpg
ImageWidth	262144000
Model	Mi 9T Pro
ImageLength	196608000
Orientation	Top left
DateTime	2021:08:09 16:34:59
YCbCrPositioning	Centered
ExifOffset	211
ResolutionUnit	Inch
XResolution	72
YResolution	72
Make	Xiaomi
ISOSpeedRatings	112
ExposureProgram	Normal program
FNumber	1.75
ExposureTime	1/4685 seconds
SensingMethod	Not defined
SubsecTimeDigitized	102279
SubsecTimeOriginal	102279
SubsecTime	102279
FocalLength	4.77 mm
Flash	Flash not fired, compulsory flash mode
LightSource	D65
MeteringMode	Center weighted average
SceneCaptureType	Standard
InteroperabilityOffset	2910
FocalLengthIn35mmFilm	26 mm
MaxApertureValue	F 1.75
DateTimeDigitized	2021:08:09 16:34:59
ExposureBiasValue	0.00
ExifImageHeight	3000
White Balance	Auto
DateTimeOriginal	2021:08:09 16:34:59
BrightnessValue	6.55
ExifImageWidth	4000
ExposureMode	Auto
ApertureValue	F 1.75
ComponentsConfiguration	YCbCr
ColorSpace	sRGB
SceneType	A directly photographed image
ShutterSpeedValue	1/4682 seconds
ExifVersion	0220
FlashPixVersion	0100
GPS information:	
GPSLatitudeRef	N
GPSLatitude	48 [redacted]
GPSLongitudeRef	E
GPSLongitude	8 [redacted]
GPSAltitudeRef	Above Sea Level
GPSAltitude	440.20 m
GPSTimeStamp	14 34 54
GPSDateStamp	2021:08:09

Bild Blume



IMG_20210529_185918.jpg - EXIF Info

EXIF Tag	Value
Filename	IMG_20210529_185918.jpg
ImageWidth	262144000
Model	Mi 9T Pro
ImageLength	196608000
Orientation	Right top
DateTime	2021:05:29 18:59:19
YCbCrPositioning	Centered
ExifOffset	211
ResolutionUnit	Inch
XResolution	72
YResolution	72
Make	Xiaomi
ISOSpeedRatings	126
ExposureProgram	Normal program
FNumber	1.75
ExposureTime	1/100 seconds
SensingMethod	Not defined
SubsecTimeDigitized	649352
SubsecTimeOriginal	649352
SubsecTime	649352
FocalLength	4.77 mm
Flash	Flash not fired, auto mode
LightSource	D65
MeteringMode	Center weighted average
SceneCaptureType	Standard
InteroperabilityOffset	2910
FocalLengthIn35mmFilm	26 mm
MaxApertureValue	F 1.75
DateTimeDigitized	2021:05:29 18:59:19
ExposureBiasValue	0.00
ExifImageHeight	3000
White Balance	Auto
DateTimeOriginal	2021:05:29 18:59:19
BrightnessValue	1.98
ExifImageWidth	4000
ExposureMode	Auto
ApertureValue	F 1.75
ComponentsConfiguration	YCbCr
ColorSpace	sRGB
SceneType	A directly photographed image
ShutterSpeedValue	1/100 seconds
ExifVersion	0220
FlashPixVersion	0100
GPS information:	
GPSLatitudeRef	N
GPSLatitude	48 [redacted]
GPSLongitudeRef	E
GPSLongitude	8 [redacted]
GPSAltitudeRef	Above Sea Level
GPSAltitude	515.36 m
GPSTimeStamp	16 59 14
GPSDateStamp	2021:05:29

B.2.3 Bildstandort Wald

Bild Reh

IMG_20210722_101704.jpg - EXIF Info

EXIF Tag	Value
Filename	IMG_20210722_101704.jpg
ImageWidth	262144000
Model	Mi 9T Pro
ImageLength	196608000
Orientation	Top left
DateTime	2021:07:22 10:17:06
YCbCrPositioning	Centered
ExifOffset	211
ResolutionUnit	Inch
XResolution	72
YResolution	72
Make	Xiaomi
ISOSpeedRatings	202
ExposureProgram	Normal program
FNumber	1.75
ExposureTime	1/100 seconds
SensingMethod	Not defined
SubsecTimeDigitized	874509
SubsecTimeOriginal	874509
SubsecTime	874509
FocalLength	4.77 mm
Flash	Flash not fired, compulsory flash mode
LightSource	D65
MeteringMode	Center weighted average
SceneCaptureType	Standard
InteroperabilityOffset	2910
FocalLengthIn35mmFilm	26 mm
MaxApertureValue	F 1.75
DateTimeDigitized	2021:07:22 10:17:06
ExposureBiasValue	0.00
ExifImageHeight	3000
White Balance	Auto
DateTimeOriginal	2021:07:22 10:17:06
BrightnessValue	2.37
ExifImageWidth	4000
ExposureMode	Auto
ApertureValue	F 1.75
ComponentsConfiguration	YCbCr
ColorSpace	sRGB
SceneType	A directly photographed image
ShutterSpeedValue	1/100 seconds
ExifVersion	0220
FlashPixVersion	0100
GPS information:	
GPSLatitudeRef	N
GPSLatitude	49 2 0.186 (49.033385)
GPSLongitudeRef	E
GPSLongitude	9 3 12.1139 (9.053365)
GPSAltitudeRef	Above Sea Level
GPSAltitude	0.00 m
GPSTimeStamp	8 17 2
GPSDateStamp	2021:07:22

Bild Bär

IMG_20210722_112821.jpg - EXIF Info

EXIF Tag	Value
Filename	IMG_20210722_112821.jpg
ImageWidth	213909504
Model	Mi 9T Pro
ImageLength	160432128
Orientation	Top left
DateTime	2021:07:22 11:28:23
YCbCrPositioning	Centered
ExifOffset	211
ResolutionUnit	Inch
XResolution	72
YResolution	72
Make	Xiaomi
ISOSpeedRatings	100
ExposureProgram	Normal program
FNumber	2.40
ExposureTime	1/111 seconds
SensingMethod	Not defined
SubsecTimeDigitized	304835
SubsecTimeOriginal	304835
SubsecTime	304835
FocalLength	5.54 mm
Flash	Flash not fired, compulsory flash mo
LightSource	D65
MeteringMode	Center weighted average
SceneCaptureType	Standard
InteroperabilityOffset	2910
FocalLengthIn35mmFilm	52 mm
MaxApertureValue	F 2.39
DateTimeDigitized	2021:07:22 11:28:23
ExposureBiasValue	0.00
ExifImageHeight	2448
White Balance	Auto
DateTimeOriginal	2021:07:22 11:28:23
BrightnessValue	4.09
ExifImageWidth	3264
ExposureMode	Auto
ApertureValue	F 2.39
ComponentsConfiguration	YCbCr
ColorSpace	sRGB
SceneType	A directly photographed image
ShutterSpeedValue	1/111 seconds
ExifVersion	0220
FlashPixVersion	0100
GPS information:	
GPSLatitudeRef	N
GPSLatitude	49 1 34.6548 (49.026293)
GPSLongitudeRef	E
GPSLongitude	9 2 33.424702 (9.042618)
GPSAltitudeRef	Above Sea Level
GPSAltitude	380.04 m
GPSTimeStamp	9 28 21
GPSDateStamp	2021:07:22

B.2.4 Bildstandort Bürogebäude

Bild Cola-Flasche

IMG_20210406_085851.jpg - EXIF Info

EXIF Tag	Value
Filename	IMG_20210406_085851.jpg
ImageWidth	262144000
Model	Mi 9T Pro
ImageLength	196608000
Orientation	Right top
DateTime	2021:04:06 08:58:52
YCbCrPositioning	Centered
ExifOffset	211
ResolutionUnit	Inch
XResolution	72
YResolution	72
Make	Xiaomi
ISOSpeedRatings	656
ExposureProgram	Normal program
FNumber	1.75
ExposureTime	1/33 seconds
SensingMethod	Not defined
SubsecTimeDigitized	065662
SubsecTimeOriginal	065662
SubsecTime	065662
FocalLength	4.77 mm
Flash	Flash not fired, compulsory flash mode
LightSource	D65
MeteringMode	Center weighted average
SceneCaptureType	Standard
InteroperabilityOffset	2910
FocalLengthIn35mmFilm	26 mm
MaxApertureValue	F 1.75
DateTimeDigitized	2021:04:06 08:58:52
ExposureBiasValue	0.00
ExifImageHeight	3000
White Balance	Auto
DateTimeOriginal	2021:04:06 08:58:52
BrightnessValue	-0.92
ExifImageWidth	4000
ExposureMode	Auto
ApertureValue	F 1.75
ComponentsConfiguration	YCbCr
ColorSpace	sRGB
SceneType	A directly photographed image
ShutterSpeedValue	1/33 seconds
ExifVersion	0220
FlashPixVersion	0100
GPS information:	
GPSLatitudeRef	N
GPSLatitude	48 [redacted]
GPSLongitudeRef	E
GPSLongitude	9 [redacted]
GPSAltitudeRef	Above Sea Level
GPSAltitude	493.40 m
GPSTimeStamp	6 58 29
GPSDateStamp	2021:04:06

Bild Büro

IMG_20210817_164220.jpg - EXIF Info

EXIF Tag	Value
Filename	IMG_20210817_164220.jpg
ImageWidth	262144000
Model	Mi 9T Pro
ImageLength	196608000
Orientation	Right top
DateTime	2021:08:17 16:42:22
YCbCrPositioning	Centered
ExifOffset	211
ResolutionUnit	Inch
XResolution	72
YResolution	72
Make	Xiaomi
ISOSpeedRatings	161
ExposureProgram	Normal program
FNumber	1.75
ExposureTime	1/33 seconds
SensingMethod	Not defined
SubsecTimeDigitized	541388
SubsecTimeOriginal	541388
SubsecTime	541388
FocalLength	4.77 mm
Flash	Flash not fired, compulsory flash mode
LightSource	D65
MeteringMode	Center weighted average
SceneCaptureType	Standard
InteroperabilityOffset	2910
FocalLengthIn35mmFilm	26 mm
MaxApertureValue	F 1.75
DateTimeDigitized	2021:08:17 16:42:22
ExposureBiasValue	0.00
ExifImageHeight	3000
White Balance	Auto
DateTimeOriginal	2021:08:17 16:42:22
BrightnessValue	0.08
ExifImageWidth	4000
ExposureMode	Auto
ApertureValue	F 1.75
ComponentsConfiguration	YCbCr
ColorSpace	sRGB
SceneType	A directly photographed image
ShutterSpeedValue	1/33 seconds
ExifVersion	0220
FlashPixVersion	0100
GPS information:	
GPSLatitudeRef	N
GPSLatitude	48 [redacted]
GPSLongitudeRef	E
GPSLongitude	8 [redacted]
GPSAltitudeRef	Above Sea Level
GPSAltitude	0.00 m
GPSTimeStamp	14 42 13
GPSDateStamp	2021:08:17

B.2.5 Bildstandort Haus

Bild Torte

IMG_20210704_220829.jpg - EXIF Info

EXIF Tag	Value
Filename	IMG_20210704_220829.jpg
ImageWidth	262144000
Model	Mi 9T Pro
ImageLength	196608000
Orientation	Right top
DateTime	2021:07:04 22:08:31
YCbCrPositioning	Centered
ExifOffset	211
ResolutionUnit	Inch
XResolution	72
YResolution	72
Make	Xiaomi
ISOSpeedRatings	467
ExposureProgram	Normal program
FNumber	1.75
ExposureTime	1/33 seconds
SensingMethod	Not defined
SubsecTimeDigitized	767176
SubsecTimeOriginal	767176
SubsecTime	767176
FocalLength	4.77 mm
Flash	Flash not fired, compulsory flash mode
LightSource	D65
MeteringMode	Center weighted average
SceneCaptureType	Standard
InteroperabilityOffset	2927
FocalLengthIn35mmFilm	45 mm
MaxApertureValue	F 1.75
DateTimeDigitized	2021:07:04 22:08:31
ExposureBiasValue	0.00
ExifImageHeight	3000
White Balance	Auto
DateTimeOriginal	2021:07:04 22:08:31
BrightnessValue	-0.55
ExifImageWidth	4000
ExposureMode	Auto
ApertureValue	F 1.75
ComponentsConfiguration	YCbCr
ColorSpace	sRGB
SceneType	A directly photographed image
ShutterSpeedValue	1/33 seconds
ExifVersion	0220
FlashPixVersion	0100
GPS information:	
GPSLatitudeRef	N
GPSLatitude	48[redacted]
GPSLongitudeRef	E
GPSLongitude	8[redacted]
GPSAltitudeRef	Above Sea Level
GPSAltitude	0.00 m
GPSTimeStamp	20 8 16
GPSDateStamp	2021:07:04

Bild Nachtisch

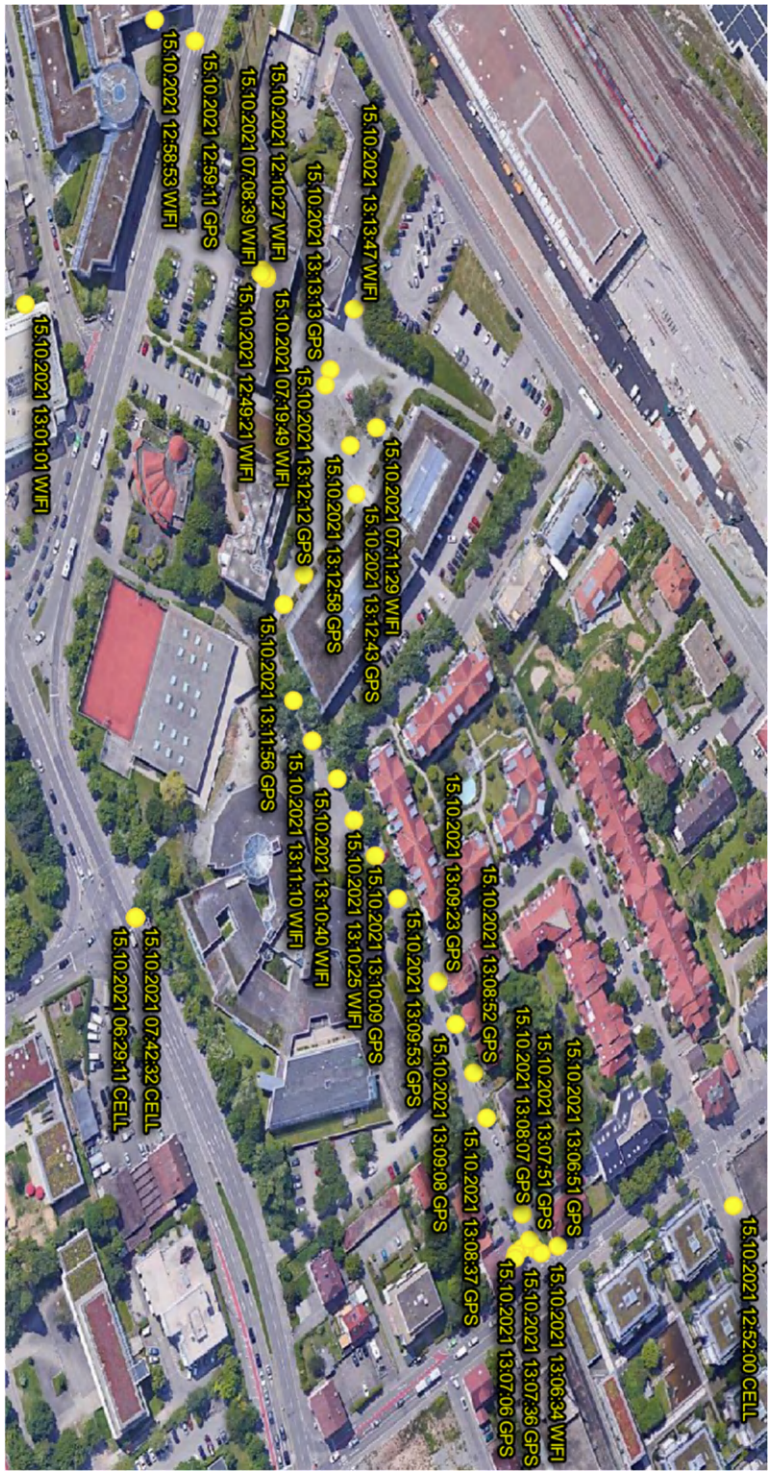
IMG_20210905_144921.jpg - EXIF Info

EXIF Tag	Value
Filename	IMG_20210905_144921.jpg
ImageWidth	262144000
Model	Mi 9T Pro
ImageLength	196608000
Orientation	Right top
DateTime	2021:09:05 14:49:23
YCbCrPositioning	Centered
ExifOffset	211
ResolutionUnit	Inch
XResolution	72
YResolution	72
Make	Xiaomi
ISOSpeedRatings	1130
ExposureProgram	Normal program
FNumber	1.75
ExposureTime	1/30 seconds
SensingMethod	Not defined
SubsecTimeDigitized	284095
SubsecTimeOriginal	284095
SubsecTime	284095
FocalLength	4.77 mm
Flash	Flash not fired, compulsory flash mode
LightSource	D65
MeteringMode	Center weighted average
SceneCaptureType	Standard
InteroperabilityOffset	2927
FocalLengthIn35mmFilm	42 mm
MaxApertureValue	F 1.75
DateTimeDigitized	2021:09:05 14:49:23
ExposureBiasValue	0.00
ExifImageHeight	3000
White Balance	Auto
DateTimeOriginal	2021:09:05 14:49:23
BrightnessValue	-2.02
ExifImageWidth	4000
ExposureMode	Auto
ApertureValue	F 1.75
ComponentsConfiguration	YCbCr
ColorSpace	sRGB
SceneType	A directly photographed image
ShutterSpeedValue	1/30 seconds
ExifVersion	0220
FlashPixVersion	0100
GPS information:	
GPSLatitudeRef	N
GPSLatitude	48 [redacted]
GPSLongitudeRef	E
GPSLongitude	8 [redacted]
GPSAltitudeRef	Above Sea Level
GPSAltitude	473.24 m
GPSTimeStamp	12 49 22
GPSDateStamp	2021:09:05

B.3 Testszenario 3 – Genauigkeit Geodaten: Google Standortverlauf

Zur Ermittlung der Genauigkeit des Google Standortverlauf wurde eine zuvor definierte Strecke zurückgelegt.

B.3.1 Darstellung der Route



B.3.2 Berechnung der Genauigkeit

Längengrad (tatsächlich)	Breitengrad (tatsächlich)	Längengrad (Google)	Breitengrad (Google)
9,00553394	48,68542617	9,00555770	48,68538480
9,00480907	48,68513798	9,00487740	48,68516130
9,00446709	48,68500296	9,00450540	48,68501240
9,00298144	48,68438861	9,00296830	48,68438660
9,00282118	48,68449264	9,00284690	48,68446830

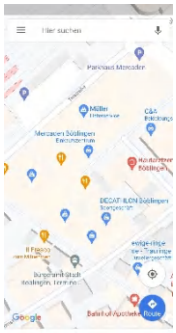
Hilfsvariable dx	Hilfsvariable dy	lat	Entfernung in KM	Entfernung in M
-0,00174654	0,00460472	0,84956033	0,00492482	4,92481802
-0,00502179	-0,00259552	0,84955586	0,00565289	5,65288592
-0,00281579	-0,00105121	0,84955338	0,00300561	3,00561210
0,00096576	0,00022341	0,84954256	0,00099126	0,99126243
-0,00189037	0,00270930	0,84954418	0,00330361	3,30360908

B.4 Testszenario 4 – Navigation

Auf dem Samsung Testgerät konnten nachfolgende Bilder, welche mit dem Zielort der Navigation in Zusammenhang stehen, aufgefunden werden:





B.5 Testszenario 5 – Suche: Google

Dieses Testszenario beschäftigt sich mit der Fragestellung, ob nach Suchanfragen von Orten oder Gebäuden in Google diese als Standorte in den Testgeräten festgestellt werden können.

B.5.1 Apple iPhone 8

Auf dem Apple-Testgerät konnten Bilder, welche mit dem Ort der Google-Suche in Zusammenhang stehen, aufgefunden werden. Aufgrund der Vielzahl an Bildern wurde eine Auswahl erstellt:




B.5.2 Samsung Galaxy S8

Auf dem Samsung-Testgerät konnten Bilder, welche mit dem Ort der Google-Suche in Zusammenhang stehen, aufgefunden werden. Aufgrund der Vielzahl an Bildern wurde eine Auswahl erstellt:







B.6 Testszenario 6 – Versand von Geodaten: E-Mail

Bei diesem Testszenario wurde das Bild „Reh“ aus dem Testszenario 5.2.2 versendet:

Auf beiden Testgeräten konnten die Geodaten mit den in den Unterkapitel beschriebenen Informationen festgestellt werden.

B.6.1 Apple iPhone 8

Dieses Bild konnte mit den nachfolgenden Informationen auf dem Apple-Testgerät gefunden werden:

Variante Bildvorschau	Variante Bilddownload
 Name: 6859905a5112ae96b89603a33e13b440ead13926.jpg Typ: Bilder Größe (Bytes): 8921704 Pfad: Apple_iPhone 8 (A1905).zip/root/private/var/mobile/Containers/Data/Application/FAADEB89-1A14-4581-B41D-BE49F363D1B5/Library/Caches/attachments/6859905a5112ae96b89603a33e13b440ead13926.jpg Erstellt: 23.08.2021 11:50:38(UTC+0) Zugegriffen: 23.08.2021 11:50:38(UTC+0) Geändert: 23.08.2021 11:50:53(UTC+0) Bearbeitet: 23.08.2021 11:50:53(UTC+0) Gelöschte: Extraktion: Dateisystem MD5: 9140fce50c93cd1e4734f9d16dc1a0ec Quelldatei: 6859905a5112ae96b89603a33e13b440ead13926.jpg **Metadata** Kamerahersteller: Xiaomi Kameramodell: Mi 9T Pro Erfassungszeit: 22.07.2021 10:17:06 Pixelauflösung: 4000x3000 Auflösung: 72x72 (Einheit: Zoll) Ausrichtung: Horizontal (normal) Lat/Lon: 49.033384 / 9.053364 **Karte** Position: (49.033384, 9.053364) Adresse: Kartenadresse: 	-

B.6.2 Samsung Galaxy S8

Dieses Bild konnte mit den nachfolgenden Informationen auf dem Samsung-Testgerät gefunden werden:

Variante Bildvorschau	Variante Bilddownload
	

B.7 Testszenario 7 – Versand von Geodaten: WhatsApp

Auf beiden Testgeräten konnten nach Versenden eines Bildes mit Geoinformationen per WhatsApp keine Geodaten festgestellt werden. Die Bilder konnten jedoch auf den Testgeräten teilweise in mehrfacher Fertigung vorgefunden werden.

Bei diesem Testszenario wurde das Bild „Reh“ aus dem Testszenario 5.2.2 verschickt:

B.7.1 Apple iPhone 8

Dieses Bild konnte mit den nachfolgenden Informationen auf dem Apple-Testgerät gefunden werden:

Name:	2BDB7D97-B944-4871-9378-0ACF8E90265C.jpg
Typ:	Bilder
Größe (Bytes):	79941
Pfad:	Apple_iPhone 8 (A1905).zip/root/private/var/mobile/Containers/Data/Application/A11A7CE3-D670-4642-9CE2-CC46364657E4/Library/Caches/ChatMedia/491771970626@s.whatsapp.net/2BDB7D97-B944-4871-9378-0ACF8E90265C.jpg
Erstellt:	23.09.2021 12:57:24(UTC+0)
Zugegriffen:	23.09.2021 12:57:24(UTC+0)
Geändert:	23.09.2021 12:57:24(UTC+0)
Bearbeitet:	23.09.2021 12:57:24(UTC+0)
Gelöschte:	
Extraktion:	Dateisystem
MD5:	50714824e6ac95f159e6892da6a6c1cd
Quelldatei:	2BDB7D97-B944-4871-9378-0ACF8E90265C.jpg

Metadata

Pixelauflösung:	619x464
Ausrichtung:	Horizontal (normal)

Name:	IMG_0001.JPG
Typ:	Bilder
Größe (Bytes):	769242
Pfad:	iPhone von Geo/mobile/Media/DCIM/100APPLE/IMG_0001.JPG
Erstellt:	23.09.2021 12:57:24(UTC+0)
Zugegriffen:	23.09.2021 12:57:24(UTC+0)
Geändert:	23.09.2021 12:57:24(UTC+0)
Bearbeitet:	
Gelöschte:	
Extraktion:	Erweitert logisch
MD5:	e441b577ea93273189e74f08bd589291
Quelldatei:	IMG_0001.JPG

B.7.2 Samsung Galaxy S8

Dieses Bild konnte mit den nachfolgenden Informationen auf dem Samsung-Testgerät gefunden werden:

Name:	IMG-20210923-WA0000.jpg
Typ:	Bilder
Größe (Bytes):	565
Pfad:	data/Root/data/com.whatsapp/databases/msgstore.db/IMG-20210923-WA0000.jpg
Erstellt:	
Zugegriffen:	
Geändert:	
Bearbeitet:	
Gelöschte:	
Extraktion:	Physisch
MD5:	e753ba9fe8c705426266fef0c55d7713
Quelldatei:	msgstore.db : 0x65D8C

Name:	IMG-20210923-WA0000.jpg
Typ:	Bilder
Größe (Bytes):	769242
Pfad:	data/Root/media/0/WhatsApp/Media/WhatsApp Images/IMG-20210923-WA0000.jpg
Erstellt:	23.09.2021 07:28:42(UTC+0)
Zugegriffen:	23.09.2021 07:28:42(UTC+0)
Geändert:	23.09.2021 07:28:44(UTC+0)
Bearbeitet:	
Gelöschte:	
Extraktion:	Physisch
MD5:	e441b577ea93273189e74f08bd589291
Quelldatei:	IMG-20210923-WA0000.jpg

Name:	.thumbdata4--1967290299_embedded_1.jpg
Typ:	Bilder
Größe (Bytes):	3019
Pfad:	data/Root/media/0/DCIM/.thumbnails/.thumbdata4--1967290299/.thumbdata4--1967290299_embedded_1.jpg
Erstellt:	
Zugegriffen:	
Geändert:	
Bearbeitet:	
Gelöschte:	
Extraktion:	Physisch
MD5:	3882470b4916441ca3ed05ea74bff775
Quelldatei:	.thumbdata4--1967290299 : 0x35B6D

Name:	6662770209425284840.0
Typ:	Bilder
Größe (Bytes):	115247
Pfad:	data/Root/media/0/Android/data/com.sec.android.gallery3d/cache/0/6662770209425284840.0
Erstellt:	23.09.2021 07:29:43(UTC+0)
Zugegriffen:	23.09.2021 07:29:43(UTC+0)
Geändert:	23.09.2021 07:29:43(UTC+0)
Bearbeitet:	
Gelöschte:	
Extraktion:	Physisch
MD5:	22626c760fe25c234f7b4e0f706d9fd8
Quelldatei:	6662770209425284840.0

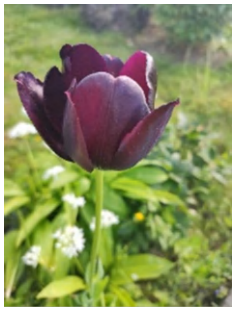
Name:	1632381908119.jpg
Typ:	Bilder
Größe (Bytes):	20149
Pfad:	data/Root/media/0/DCIM/.thumbnails/1632381908119.jpg
Erstellt:	23.09.2021 07:25:08(UTC+0)
Zugegriffen:	23.09.2021 07:25:08(UTC+0)
Geändert:	23.09.2021 07:25:08(UTC+0)
Bearbeitet:	
Gelöschte:	
Extraktion:	Physisch
MD5:	745f131d0e9129ccacbd1bec4cbfce17
Quelldatei:	1632381908119.jpg

B.8 Testszenario 8 – Versand von Geodaten: Facebook Messenger

Auf beiden Testgeräten konnten keine Geodaten festgestellt werden, nachdem ein Bild mit Geokoordinaten per Facebook Messenger verschickt wurde. Die Bilder konnten jedoch auf den Testgeräten teilweise in mehrfacher Ausfertigung vorgefunden werden.

B.8.1 Apple iPhone 8

Bei dem Testszenario wurde das Bild „Blume“ aus dem Testszenario 5.2.1 versendet:



Dieses Bild konnte mit den nachfolgenden Informationen auf dem Apple-Testgerät gefunden werden:

Variante 1

Name:	0186ecd127cce43c0e2af037bdff5e75
Typ:	Bilder
Größe (Bytes):	50312
Pfad:	Apple_iPhone 8 (A1905).zip/root/private/var/mobile/Containers/Shared/AppGroup/0BE94256-0B0D-4604-B01E-F65369AE708F/Library/Caches/lightspeed-imageCache/0186ecd127cce43c0e2af037bdff5e75
Erstellt:	05.10.2021 08:26:07(UTC+2)
Zugegriffen:	05.10.2021 08:26:07(UTC+2)
Geändert:	05.10.2021 08:26:07(UTC+2)
Bearbeitet:	05.10.2021 08:26:07(UTC+2)
Gelöschte:	
Extraktion:	Dateisystem
MD5:	e22315cb7ee318e7ebd0a99af01ed3f8
Quelldatei:	0186ecd127cce43c0e2af037bdff5e75

Variante 2

Name:	0186ecd127cce43c0e2af037bdff5e75
Typ:	Bilder
Größe (Bytes):	50312
Pfad:	Apple_iPhone 8 (A1905).zip/root/private/var/mobile/Containers/Shared/AppGroup/0BE94256-0B0D-4604-B01E-F65369AE708F/Library/Caches/lightspeed-imageCache/0186ecd127cce43c0e2af037bdff5e75
Erstellt:	05.10.2021 06:26:07(UTC+0)
Zugegriffen:	05.10.2021 06:26:07(UTC+0)
Geändert:	05.10.2021 06:26:07(UTC+0)
Bearbeitet:	05.10.2021 06:26:07(UTC+0)
Gelöschte:	
Extraktion:	Dateisystem
MD5:	e22315cb7ee318e7ebd0a99af01ed3f8
Quelldatei:	0186ecd127cce43c0e2af037bdff5e75

Name:	5003.JPG
Typ:	Bilder
Größe (Bytes):	35873
Pfad:	Apple_iPhone 8 (A1905).zip/root/private/var/mobile/Media/PhotoData/Thumbnails/V2/DCIM/100APPLE/IMG_0001.JPG/5003.JPG
Erstellt:	05.10.2021 09:35:37(UTC+0)
Zugegriffen:	05.10.2021 09:35:37(UTC+0)
Geändert:	05.10.2021 09:35:37(UTC+0)
Bearbeitet:	05.10.2021 09:35:37(UTC+0)
Gelöschte:	
Extraktion:	Dateisystem
MD5:	7c80d5833c4a500ea64f53660c6ae3d3
Quelldatei:	5003.JPG

Name:	69fc4e7e15a12cb416414cf48e0d70d1
Typ:	Bilder
Größe (Bytes):	27758
Pfad:	Apple_iPhone 8 (A1905).zip/root/private/var/mobile/Containers/Shared/AppGroup/0BE94256-0B0D-4604-B01E-F65369AE708F/Library/Caches/lightspeed-imageCache/69fc4e7e15a12cb416414cf48e0d70d1
Erstellt:	05.10.2021 06:25:30(UTC+0)
Zugegriffen:	05.10.2021 06:25:30(UTC+0)
Geändert:	05.10.2021 06:25:30(UTC+0)
Bearbeitet:	05.10.2021 06:25:30(UTC+0)
Gelöschte:	
Extraktion:	Dateisystem
MD5:	fa6f5682c661cabc1d9fe6853b823ab7
Quelldatei:	69fc4e7e15a12cb416414cf48e0d70d1

Name:	thumb_1.bmp
Typ:	Bilder
Größe (Bytes):	11466
Pfad:	Apple_iPhone 8 (A1905).zip/root/private/var/mobile/Media/PhotoData/Thumbnails/3310.ithmb/thumb_1.bmp
Erstellt:	
Zugegriffen:	
Geändert:	
Bearbeitet:	
Gelöschte:	
Extraktion:	Dateisystem
MD5:	7b4f1bcf352157df74b97b3cf608f3b6
Quelldatei:	3310.ithmb

B.8.2 Samsung Galaxy S8

Bei diesem Testszenario wurde das Bild „Sonnenblume“ aus dem Testszenario 5.2.1 verschickt:

Dieses Bild konnte mit den nachfolgenden Informationen auf dem Samsung-Testgerät gefunden werden:

Variante 1

Name:	9XQdliDCtULRF-gK-PiP7VmhHOM
Typ:	Bilder
Größe (Bytes):	67018
Pfad:	data/Root/data/com.facebook.orca/cache/image/9XQdliDCtULRF-gK-PiP7VmhHOM
Erstellt:	05.10.2021 06:05:12(UTC+0)
Zugegriffen:	05.10.2021 06:05:12(UTC+0)
Geändert:	05.10.2021 06:05:12(UTC+0)
Bearbeitet:	
Gelöschte:	
Extraktion:	Physisch
MD5:	9052ac9509ef91e302caded934d7bca3
Quelldatei:	9XQdliDCtULRF-gK-PiP7VmhHOM

Name:	pQRtmzvU4gdX3QH1ExSbiDjz5_Y
Typ:	Bilder
Größe (Bytes):	17037
Pfad:	data/Root/data/com.facebook.orca/cache/image/pQRtmzvU4gdX3QH1ExSbiDjz5_Y
Erstellt:	05.10.2021 06:05:12(UTC+0)
Zugegriffen:	05.10.2021 06:05:12(UTC+0)
Geändert:	05.10.2021 06:05:12(UTC+0)
Bearbeitet:	
Gelöschte:	
Extraktion:	Physisch
MD5:	0ac410877f7a7b0deba8534f70bf9d87
Quelldatei:	pQRtmzvU4gdX3QH1ExSbiDjz5_Y

Variante 2

Name:	received_4536112579786760.jpeg
Typ:	Bilder
Größe (Bytes):	67018
Pfad:	data/Root/media/0/Pictures/Messenger/ received_4536112579786760.jpeg
Erstellt:	05.10.2021 09:19:53(UTC+0)
Zugegriffen:	05.10.2021 09:19:53(UTC+0)
Geändert:	05.10.2021 09:19:53(UTC+0)
Bearbeitet:	
Gelöschte:	
Extraktion:	Physisch
MD5:	9052ac9509ef91e302caded934d7bca3
Quelldatei:	received_4536112579786760.jpeg

Name:	cwVNtboqP_rcT_CRbRMMOIP1rrl
Typ:	Bilder
Größe (Bytes):	43085
Pfad:	data/Root/data/com.facebook.orca/cache/ image/cwVNtboqP_rcT_CRbRMMOIP1rrl
Erstellt:	05.10.2021 09:19:49(UTC+0)
Zugegriffen:	05.10.2021 09:19:49(UTC+0)
Geändert:	05.10.2021 09:19:49(UTC+0)
Bearbeitet:	
Gelöschte:	
Extraktion:	Physisch
MD5:	278339f471c91fd51cb04fc9fd6c15b9
Quelldatei:	cwVNtboqP_rcT_CRbRMMOIP1rrl

B.9 Testszenario 9 – Versand von Geodaten: Snapchat

Auf den Testgeräten konnten die verschickten Snaps nicht festgestellt werden.

B.9.1 Apple iPhone 8

Zu dem Snap konnten nachfolgende Informationen auf dem Apple-Testgerät gefunden werden.

» Instant Message Gehe zu

Quelle:	Snapchat
Betreff:	
Zeitstempel:	30.09.2021 13:13:08(UTC+0)
Status:	
Nachrichttyp:	App-Nachricht
SMSC:	
Gerätebeschreibung:	
Ordner:	
Priorität:	
Extraktion:	Dateisystem
Quelldatei:	Apple_iPhone 8 (A1905).zip/root/private/var/mobile/Containers/Data/Application/9D377AE9-0026-4306-8F98-67B99AE741E5/Documents/user_scoped/d99052134ef33574a1c093cd19bc62ede66e2a3437f8428f38b7ddc7bc327fe8/arroyo/arroyo.db : 0xB9A7 (Tabelle: conversation_message, user_conversation, Größe: 184320 Bytes)

Von

Von: 45af9df5-57df-413e-a2f3-4a10da4e851f (Eigentümer)

An

Bis: 27409cd0-7900-4e3c-b184-48d004fb4738

B.9.2 Samsung Galaxy S8

Zu dem versendeten Snap konnten nachfolgende Informationen auf dem Samsung-Testgerät gefunden werden:

» Instant Message Gehe zu

Quelle:	Snapchat
Betreff:	
Zeitstempel:	30.09.2021 14:02:24(UTC+0)
Status:	
Nachrichttyp:	App-Nachricht
SMSC:	
Gerätebeschreibung:	
Ordner:	
Priorität:	
Extraktion:	Physisch
Quelldatei:	data/Root/data/com.snapchat.android/databases/arroyo.db : 0xB766 (Tabelle: conversation_message, Größe: 176128 Bytes) data/Root/data/com.snapchat.android/databases/main.db : 0xCD45C (Tabelle: Friend, Größe: 1150976 Bytes)

Von

Von: 45af9df5-57df-413e-a2f3-4a10da4e851f Geo Daten (Eigentümer)

Teilnehmer

27409cd0-7900-4e3c-b184-48d004fb4738	Lena Z
45af9df5-57df-413e-a2f3-4a10da4e851f	Geo Daten (Eigentümer)

B.10 Testszenario 10 – Upload von Geodaten: Facebook

Auf die Social-Media Plattform Facebook wurden die in den beiden Unterkapiteln dargestellten Bilder mit darin enthaltenen Geokoordinaten hochgeladen.

B.10.1Apple iPhone 8

Bei dem Testszenario wurde das nachfolgende Bild verschickt:

Dieses Bild konnte mit den nachfolgenden Informationen auf dem Apple-Testgerät gefunden werden:

Name:	FBImageDownloader-cb6f72ec15e6d159da7008a40e96a291.jpg
Typ:	Bilder
Größe (Bytes):	69339
Pfad:	Apple_iPhone 8 (A1905).zip/root/private/var/mobile/Containers/Data/Application/8754D65F-8F08-4F5E-8C69-CE3E6194AC30/Library/Caches/com.facebook.Facebook.MosaicIGImageDiskCache/FBImageDownloader-cb6f72ec15e6d159da7008a40e96a291.jpg
Erstellt:	23.09.2021 11:11:12(UTC+0)
Zugegriffen:	23.09.2021 11:11:12(UTC+0)
Geändert:	23.09.2021 11:11:12(UTC+0)
Bearbeitet:	23.09.2021 11:11:12(UTC+0)
Gelöschte:	
Extraktion:	Dateisystem
MD5:	bf6a04196b9018f2f2480cd2cb3ea1b5
Quelldatei:	FBImageDownloader-cb6f72ec15e6d159da7008a40e96a291.jpg

B.10.2Samsung Galaxy S8

Bei diesem Testszenario wurde das Bild „Reh“ aus dem Testszenario 5.2.2 verschickt:

Dieses Bild konnte mit den nachfolgenden Informationen auf dem Samsung-Testgerät gefunden werden:

Name:	d0fa26e9-917b05bfdd76e8ce.tmp
Typ:	Bilder
Größe (Bytes):	430308
Pfad:	data/Root/data/com.facebook.katana/app_uploads/6e5ac268-65ea-49c2-aa7b-cc0bc634c18a/d0fa26e9-917b05bfdd76e8ce.tmp
Erstellt:	21.09.2021 08:33:42(UTC+0)
Zugegriffen:	21.09.2021 08:33:42(UTC+0)
Geändert:	21.09.2021 08:33:43(UTC+0)
Bearbeitet:	
Gelöschte:	
Extraktion:	Physisch
MD5:	ab85beaf0660c3610f19c526a378ee3d
Quelldatei:	d0fa26e9-917b05bfdd76e8ce.tmp

Metadata

Kamerahersteller:	Xiaomi
Kameramodell:	Mi 9T Pro
Erfassungszeit:	22.07.2021 10:17:06
Pixelauflösung:	4000x3000
Auflösung:	72x72 (Einheit: Zoll)
Ausrichtung:	Horizontal (normal)
Lat/Lon:	49.033384 / 9.053364

B.11 Testszenario 11 – Standortmarkierung: Facebook

Auf beiden Testgeräten konnten die in Facebook angegebenen Standorte festgestellt werden. In den nachfolgenden beiden Unterkapiteln werden diese für jede Variante dargestellt.

B.11.1Apple iPhone 8

Die Standorte aus Facebook konnten mit den nachfolgenden Informationen auf dem Apple-Testgerät gefunden werden:

Name:	Böblingen Polizei
Beschreibung:	Local Business
Typ:	
Quelle:	
Zeitstempel:	
Endzeit:	
Position:	(48.684669, 9.000900)
Zusammengefasste Standorte:	
Kartenadresse:	
Genauigkeit:	
Konfidenz:	
Karte:	
Kategorie:	
Quelle:	Facebook
Konto:	
Adresse:	
Extraktion:	Dateisystem
Manuell decodiert:	False
Quelldatei:	Apple_iPhone 8 (A1905).zip/ root/private/var/mobile/ Containers/Data/ Application/8754D65F-8F08-4F 5E-8C69-CE3E6194AC30/ Library/Caches/graphStoreDB/ GraphStore_100070915526652. sqlite3-wal : 0xF6E64 (Größe: 1474992 Bytes)

Name:	McDonald's Böblingen
Beschreibung:	Fast-Food-Restaurant, Burger-Restaurant
Typ:	
Quelle:	
Zeitstempel:	
Endzeit:	
Position:	(48.682758, 9.000849)
Zusammengefasste Standorte:	
Kartenadresse:	
Genauigkeit:	
Konfidenz:	
Karte:	
Kategorie:	
Quelle:	Facebook
Konto:	
Adresse:	
Extraktion:	Dateisystem
Manuell decodiert:	False
Quelldatei:	Apple_iPhone 8 (A1905).zip/ root/private/var/mobile/ Containers/Data/ Application/8754D65F-8F08-4F 5E-8C69-CE3E6194AC30/ Library/Caches/graphStoreDB/ GraphStore_100070915526652. sqlite3-wal : 0x155732 (Größe: 1474992 Bytes)

Name:	Polizei Leonberg
Beschreibung:	Öffentliche Verwaltungs- und Regierungsbehörde
Typ:	
Quelle:	
Zeitstempel:	
Endzeit:	
Position:	(48.798480, 9.010660)
Zusammengefasste Standorte:	
Kartenadresse:	
Genauigkeit:	
Konfidenz:	
Karte:	
Kategorie:	
Quelle:	Facebook
Konto:	
Adresse:	
Extraktion:	Dateisystem
Manuell decodiert:	False
Quelldatei:	Apple_iPhone 8 (A1905).zip/ root/private/var/mobile/ Containers/Data/ Application/8754D65F-8F08-4F 5E-8C69-CE3E6194AC30/ Library/Caches/graphStoreDB/ GraphStore_100070915526652. sqlite3-wal : 0x10857B (Größe: 1474992 Bytes)

B.11.2Samsung Galaxy S8

Die Standorte aus Facebook konnten mit den nachfolgenden Informationen auf dem Apple-Testgerät gefunden werden.

Name:	Böblingen Polizei
Beschreibung:	Lokales Unternehmen
Typ:	
Quelle:	
Zeitstempel:	
Endzeit:	
Position:	(48.684669, 9.000900)
Zusammengefasste Standorte:	
Kartenadresse:	
Genauigkeit:	
Konfidenz:	
Karte:	
Kategorie:	
Quelle:	Facebook
Konto:	
Adresse:	
Extraktion:	Physisch
Manuell decodiert:	False
Quelldatei:	data/Root/data/com.facebook.katana/cache/graph_store_cache/100070915526652/GraphStore.sqlite3-wal : 0x71E6F (Größe: 711624 Bytes)

Name:	McDonald's Böblingen
Beschreibung:	
Typ:	
Quelle:	
Zeitstempel:	
Endzeit:	
Position:	(48.682758, 9.000849)
Zusammengefasste Standorte:	
Kartenadresse:	
Genauigkeit:	
Konfidenz:	
Karte:	
Kategorie:	
Quelle:	Facebook
Konto:	
Adresse:	
Extraktion:	Physisch
Manuell decodiert:	False
Quelldatei:	data/Root/data/com.facebook.katana/cache/graph_store_cache/100070915526652/GraphStore.sqlite3-wal : 0x77D4E (Größe: 711624 Bytes)

Name:	Polizei Ludwigsburg
Beschreibung:	
Typ:	
Quelle:	
Zeitstempel:	
Endzeit:	
Position:	(48.893260, 9.199909)
Zusammengefasste Standorte:	
Kartenadresse:	
Genauigkeit:	
Konfidenz:	
Karte:	
Kategorie:	
Quelle:	Facebook
Konto:	
Adresse:	
Extraktion:	Physisch
Manuell decodiert:	False
Quelldatei:	data/Root/data/com.facebook.katana/cache/graph_store_cache/100070915526652/GraphStore.sqlite3-wal : 0xA9835 (Größe: 711624 Bytes)

B.12 Testszenario 12 – Standortfreigabe: Facebook Messenger

Auf den Testgeräten konnten, wie in der Masterthesis in Kapitel 5.12 beschrieben, jeweils zwei Datensätze pro Variante festgestellt werden. Dies Informationen zu den Datensätzen können den nachfolgenden beiden Unterkapiteln entnommen werden.

B.12.1Apple iPhone 8

Die Standorte aus dem Facebook Messenger konnten mit den nachfolgenden Informationen auf dem Apple-Testgerät gefunden werden:

Sender		
	Name:	
	Beschreibung:	Fixierter Standort Steinbeisstraße 26, 71034 Böblingen, Deutschland
	Typ:	
	Quelle:	
	Zeitstempel:	04.10.2021 08:57:33(UTC+0)
	Endzeit:	
	Position:	(4868122482.000000, 900260639.000000)
	Zusammengefasste Standorte:	
	Kartenadresse:	
	Genauigkeit:	
	Konfidenz:	
	Karte:	
	Kategorie:	
	Quelle:	Facebook Messenger
	Konto:	
	Adresse:	
	Extraktion:	Dateisystem
	Manuell decodiert:	False
	Quelldatei:	Apple_iPhone 8 (A1905).zip/root/private/var/mobile/Containers/Shared/AppGroup/0BE94256-0B0D-4604-B01E-F65369AE708F/lightspeed-100070915526652.db-wal : 0xEB2ED (Tabelle: messages, Größe: 2846952 Bytes)

Name:	
Beschreibung:	
Typ:	
Quelle:	
Zeitstempel:	04.10.2021 08:57:33(UTC+0)
Endzeit:	
Position:	(4868122482.000000, 900260639.000000)
Zusammengefasste Standorte:	
Kartenadresse:	
Genauigkeit:	
Konfidenz:	
Karte:	
Kategorie:	
Quelle:	Facebook Messenger
Konto:	
Adresse:	
Extraktion:	Dateisystem
Manuell decodiert:	False
Quelldatei:	Apple_iPhone 8 (A1905).zip/root/private/var/mobile/Containers/Shared/AppGroup/0BE94256-0B0D-4604-B01E-F65369AE708F/lightspeed-100070915526652.db-wal : 0xEB2ED (Tabelle: messages, Größe: 2846952 Bytes)

Empfänger

Name:	
Beschreibung:	Polizei Leonberg Gerhart-Hauptmann-Straße 8, 71229 Leonberg
Typ:	
Quelle:	
Zeitstempel:	04.10.2021 08:58:17(UTC+0)
Endzeit:	
Position:	(4879848000.000000, 901066000.000000)
Zusammengefasste Standorte:	
Kartenadresse:	
Genauigkeit:	
Konfidenz:	
Karte:	
Kategorie:	
Quelle:	Facebook Messenger
Konto:	
Adresse:	
Extraktion:	Dateisystem
Manuell decodiert:	False
Quelldatei:	Apple_iPhone 8 (A1905).zip/root/private/var/mobile/Containers/Shared/AppGroup/0BE94256-0B0D-4604-B01E-F65369AE708F/lightspeed-100070915526652.db-wal : 0xEB374 (Tabelle: messages, Größe: 2846952 Bytes) Apple_iPhone 8 (A1905).zip/root/private/var/mobile/Containers/Shared/AppGroup/0BE94256-0B0D-4604-B01E-F65369AE708F/lightspeed-100070915526652.db : 0x3A65DE (Größe: 5640192 Bytes)

Name:	
Beschreibung:	
Typ:	
Quelle:	
Zeitstempel:	04.10.2021 08:58:17(UTC+0)
Endzeit:	
Position:	(4879848000.000000, 901066000.000000)
Zusammengefasste Standorte:	
Kartenadresse:	
Genauigkeit:	
Konfidenz:	
Karte:	
Kategorie:	
Quelle:	Facebook Messenger
Konto:	
Adresse:	
Extraktion:	Dateisystem
Manuell decodiert:	False
Quelldatei:	Apple_iPhone 8 (A1905).zip/root/private/var/mobile/Containers/Shared/AppGroup/0BE94256-0B0D-4604-B01E-F65369AE708F/lightspeed-100070915526652.db-wal : 0xEB374 (Tabelle: messages, Größe: 2846952 Bytes)

B.12.2Samsung Galaxy S8

Die Standorte aus dem Facebook Messenger konnten mit den nachfolgenden Informationen auf dem Samsung-Testgerät gefunden werden:

Sender

Name:	Fixierter Standort
Beschreibung:	Calwer Straße 6, 71034 Böblingen, Deutschland
Typ:	
Quelle:	
Zeitstempel:	04.10.2021 07:42:16(UTC+0)
Endzeit:	
Position:	
Zusammengefasste Standorte:	
Kartenadresse:	
Genauigkeit:	
Konfidenz:	
Karte:	
Kategorie:	
Quelle:	Facebook Messenger
Konto:	
Adresse:	
Extraktion:	Physisch
Manuell decodiert:	False
Quelldatei:	data/Root/data/com.facebook.orca/databases/threads_db2 : 0x17F29 (Tabelle: messages, Größe: 319488 Bytes)

Name:	
Beschreibung:	
Typ:	
Quelle:	
Zeitstempel:	04.10.2021 07:42:16(UTC+0)
Endzeit:	
Position:	(4868452200.000000, 900209400.000000)
Zusammengefasste Standorte:	
Kartenadresse:	
Genauigkeit:	
Konfidenz:	
Karte:	
Kategorie:	
Quelle:	Facebook Messenger
Konto:	
Adresse:	
Extraktion:	Physisch
Manuell decodiert:	False
Quelldatei:	data/Root/data/com.facebook.orca/databases/threads_db2 : 0x17F29 (Tabelle: messages, Größe: 319488 Bytes)

Empfänger

Name:	Polizei Ludwigsburg
Beschreibung:	Friedrich-Ebert-Straße 30, 71638 Ludwigsburg
Typ:	
Quelle:	
Zeitstempel:	04.10.2021 07:44:04(UTC+0)
Endzeit:	
Position:	
Zusammengefasste Standorte:	
Kartenadresse:	
Genauigkeit:	
Konfidenz:	
Karte:	
Kategorie:	
Quelle:	Facebook Messenger
Konto:	
Adresse:	
Extraktion:	Physisch
Manuell decodiert:	False
Quelldatei:	data/Root/data/com.facebook.orca/databases/threads_db2 : 0x17762 (Tabelle: messages, Größe: 319488 Bytes)

Name:	
Beschreibung:	
Typ:	
Quelle:	
Zeitstempel:	04.10.2021 07:44:04(UTC+0)
Endzeit:	
Position:	(4889326000.000000, 919990990.000000)
Zusammengefasste Standorte:	
Kartenadresse:	
Genauigkeit:	
Konfidenz:	
Karte:	
Kategorie:	
Quelle:	Facebook Messenger
Konto:	
Adresse:	
Extraktion:	Physisch
Manuell decodiert:	False
Quelldatei:	data/Root/data/com.facebook.orca/databases/threads_db2 : 0x17762 (Tabelle: messages, Größe: 319488 Bytes)

B.13 Testszenario 13 – Standortfreigabe: WhatsApp

Im Messenger WhatsApp wurde an einen Kontakt der Standort verschickt bzw. empfangen mit der Fragestellung, ob dieser im Image erkennbar ist. Bei beiden Testgeräten konnten die Geodaten sowohl in der Funktion als Empfänger, als auch des Senders des Standortes festgestellt werden.

B.13.1Apple iPhone 8

Die Standorte aus WhatsApp konnten mit den nachfolgenden Informationen auf dem Apple-Testgerät gefunden werden:

Sender

Name:	
Beschreibung:	
Typ:	
Quelle:	Gerät
Zeitstempel:	29.09.2021 06:50:28(UTC+0)
Endzeit:	
Position:	(48.68[redacted] 8.99[redacted])
Zusammengefasste Standorte:	
Kartenadresse:	
Genauigkeit:	
Konfidenz:	
Karte:	
Kategorie:	
Quelle:	WhatsApp
Konto:	
Adresse:	
Extraktion:	Dateisystem
Manuell decodiert:	False
Quelldatei:	Apple_iPhone 8 (A1905).zip/ root/private/var/mobile/ Containers/Shared/ AppGroup/ FBBA1361-1AB4-469D-B6CB-A1396336F0A2/ ChatStorage.sqlite-wal : 0x2009 (Tabelle: ZWAMESSAGE, Größe: 16512 Bytes) Apple_iPhone 8 (A1905).zip/ root/private/var/mobile/ Containers/Shared/ AppGroup/ FBBA1361-1AB4-469D-B6CB-A1396336F0A2/ ChatStorage.sqlite : 0x9FA8 (Tabelle: ZWAMEDIAITEM, Größe: 344064 Bytes)

Name:	
Beschreibung:	
Typ:	
Quelle:	Gerät
Zeitstempel:	29.09.2021 06:53:01(UTC+0)
Endzeit:	
Position:	(48.6[redacted], 9.00[redacted])
Zusammengefasste Standorte:	
Kartenadresse:	
Genauigkeit:	
Konfidenz:	
Karte:	
Kategorie:	
Quelle:	WhatsApp
Konto:	
Adresse:	
Extraktion:	Dateisystem
Manuell decodiert:	False
Quelldatei:	Apple_iPhone 8 (A1905).zip/ root/private/var/mobile/ Containers/Shared/ AppGroup/ FBBA1361-1AB4-469D-B6CB-A1396336F0A2/ ChatStorage.sqlite-wal : 0x1F03 (Tabelle: ZWAMESSAGE, Größe: 16512 Bytes) Apple_iPhone 8 (A1905).zip/ root/private/var/mobile/ Containers/Shared/ AppGroup/ FBBA1361-1AB4-469D-B6CB-A1396336F0A2/ ChatStorage.sqlite : 0x9F29 (Tabelle: ZWAMEDIAITEM, Größe: 344064 Bytes)

Empfänger

Name:	
Beschreibung:	
Typ:	
Quelle:	Extern
Zeitstempel:	30.09.2021 11:32:49(UTC+0)
Endzeit:	
Position:	(48.6[redacted], 9.00[redacted])
Zusammengefasste Standorte:	
Kartenadresse:	
Genauigkeit:	
Konfidenz:	
Karte:	
Kategorie:	
Quelle:	WhatsApp
Konto:	
Adresse:	
Extraktion:	Dateisystem
Manuell decodiert:	False
Quelldatei:	Apple_iPhone 8 (A1905).zip/ root/private/var/mobile/ Containers/Shared/ AppGroup/21605AF6-6204-4F0B-9E45-23DB4E4FAA8F/ ChatStorage.sqlite : 0xAF26 (Tabelle: ZWAMESSAGE, ZWAMEDIAITEM, Größe: 344064 Bytes)

B.13.2Samsung Galaxy S8

Die Standorte aus WhatsApp konnten mit den nachfolgenden Informationen auf dem Samsung-Testgerät gefunden werden:

Sender

Name:	
Beschreibung:	
Typ:	
Quelle:	
Zeitstempel:	30.09.2021 10:10:50(UTC+0)
Endzeit:	
Position:	(48.68[redacted], 9.00[redacted])
Zusammengefasste Standorte:	
Kartenadresse:	
Genauigkeit:	
Konfidenz:	
Karte:	
Kategorie:	
Quelle:	WhatsApp
Konto:	
Adresse:	
Extraktion:	Physisch
Quelldatei:	data/Root/data/com.whatsapp/ databases/msgstore.db-wal : 0x4C61C (Tabelle: messages, Größe: 524288 Bytes)

Name:	
Beschreibung:	
Typ:	
Quelle:	
Zeitstempel:	30.09.2021 10:12:04(UTC+0)
Endzeit:	
Position:	
Zusammengefasste Standorte:	
Kartenadresse:	
Genauigkeit:	
Konfidenz:	
Karte:	
Kategorie:	
Quelle:	WhatsApp
Konto:	
Adresse:	
Extraktion:	Physisch
Quelldatei:	data/Root/data/com.whatsapp/ databases/msgstore.db-wal : 0x4C556 (Tabelle: messages, Größe: 524288 Bytes)

Empfänger

Name:	
Beschreibung:	
Typ:	
Quelle:	
Zeitstempel:	30.09.2021 12:15:44(UTC+0)
Endzeit:	
Position:	(48.68[redacted]1, 9.00[redacted])
Zusammengefasste Standorte:	
Kartenadresse:	
Genauigkeit:	
Konfidenz:	
Karte:	
Kategorie:	
Quelle:	WhatsApp
Konto:	
Adresse:	
Extraktion:	Dateisystem
Quelldatei:	Samsung GSM_SM-G950F Galaxy S8.zip/data/data/ com.whatsapp/databases/ msgstore.db-wal : 0x1B188 (Tabelle: messages, Größe: 524288 Bytes)

B.14 Testszenario 10 – Live-Standortfreigabe: WhatsApp

Im Messenger WhatsApp wurde an einen Kontakt der Live-Standort verschickt bzw. empfangen mit der Fragestellung, ob dieser im Image erkennbar ist. Bei beiden Testgeräten konnten die Geodaten zum Startzeitpunkt sowohl in der Funktion als Empfänger, als auch des Senders des Standortes festgestellt werden.

B.14.1Apple iPhone 8

Die Standorte aus WhatsApp konnten mit den nachfolgenden Informationen auf dem Apple-Testgerät gefunden werden:

Sender

Name:	
Beschreibung:	
Typ:	
Quelle:	Gerät
Zeitstempel:	17.10.2021 13:54:31(UTC+0)
Endzeit:	
Position:	(48.77[redacted]7, 8.9[redacted]9)
Zusammengefasste Standorte:	
Kartenadresse:	
Genauigkeit:	
Konfidenz:	
Karte:	
Kategorie:	
Quelle:	WhatsApp
Konto:	
Adresse:	
Extraktion:	Dateisystem
Manuell decodiert:	False
Quelldatei:	Apple_iPhone 8 (A1905).zip/ root/private/var/mobile/ Containers/Shared/ AppGroup/11C38481-1B01-484 B-929C-33B80FA35919/ ChatStorage.sqlite : 0x832DA (Tabelle: ZWAMESSAGE, ZWAMEDIAITEM, Größe: 692224 Bytes)

Empfänger

Name:	
Beschreibung:	
Typ:	
Quelle:	Extern
Zeitstempel:	16.10.2021 09:41:42(UTC+0)
Endzeit:	16.10.2021 10:16:29(UTC+0)
Position:	(48.77[redacted], 8.90[redacted])
Zusammengefasste Standorte:	
Kartenadresse:	
Genauigkeit:	
Konfidenz:	
Karte:	
Kategorie:	
Quelle:	WhatsApp
Konto:	
Adresse:	
Extraktion:	Dateisystem
Manuell decodiert:	False
Quelldatei:	Apple_iPhone 8 (A1905).zip/ root/private/var/mobile/ Containers/Shared/AppGroup/ FB0CCE6C-0CD1-4EF8-91CE-3D 8E2C6A9D4E/ ChatStorage.sqlite : 0x8FAB6 (Tabelle: ZWAMESSAGE, ZWAMEDIAITEM, Größe: 720896 Bytes)

B.14.2Samsung Galaxy S8

Die Standorte aus WhatsApp konnten mit den nachfolgenden Informationen auf dem Samsung-Testgerät gefunden werden:

Sender	**Name:**	
	Beschreibung:	
	Typ:	
	Quelle:	
	Zeitstempel:	16.10.2021 09:41:41(UTC+0)
	Endzeit:	
	Position:	(48.77[redacted], 8.90[redacted])
	Zusammengefasste Standorte:	
	Kartenadresse:	
	Genauigkeit:	
	Konfidenz:	
	Karte:	
	Kategorie:	
	Quelle:	WhatsApp
	Konto:	
	Adresse:	
	Extraktion:	Physisch
	Quelldatei:	data/Root/data/com.whatsapp/ databases/msgstore.db : 0x5EC9 (Tabelle: messages, Größe: 1019904 Bytes)
Empfänger	**Name:**	
	Beschreibung:	4917[redacted]@s.whatsapp.net ,48.77[redacted],8.9[redacted] 92[redacted]
	Typ:	
	Quelle:	
	Zeitstempel:	17.10.2021 13:54:33(UTC+0)
	Endzeit:	
	Position:	(48.77[redacted], 8.90[redacted])
	Zusammengefasste Standorte:	
	Kartenadresse:	
	Genauigkeit:	
	Konfidenz:	
	Karte:	
	Kategorie:	
	Quelle:	WhatsApp
	Konto:	
	Adresse:	
	Extraktion:	Physisch
	Quelldatei:	data/Root/data/com.whatsapp/ databases/msgstore.db-wal : 0x2F25E (Tabelle: messages, Größe: 524288 Bytes)