HOCHSCHULE
MITTWEIDA
UNIVERSITY OF
APPLIED SCIENCES

Bachelorarbeit

Frau
Maxi Brückner

Reverse Engineering des Instant Messenger-Dienstes „Threema“

Mittweida, 2023

Fakultät Computer- und Biowissenschaften

Bachelorarbeit

Reverse Engineering des Instant Messenger-Dienstes „Threema“

Autor:
Frau

Maxi Brückner

Studiengang:
Allgemeine und Digitale Forensik

Seminargruppe:
FO19-w5

Erstprüfer:
Prof. Dr. rer. nat. Michael Spranger

Zweitprüfer:
B. Sc. Lukas Jaeckel

Einreichung:
Mittweida, 05.10.2023

Faculty Applied Computer Sciences & Biosciences

Bachelor Thesis

Reverse engineering of the instant messenger “Threema”

author:
Ms.

Maxi Brückner

course of studies:
General and Digital Forensic

seminar group:
FO19-w5

first examiner:
Prof. Dr. rer. nat. Michael Spranger

second examiner:
B. Sc. Lukas Jaeckel

submission:
Mittweida, 05.10.2023

Zusammenfassung[1]

Instant Messenger gehören zu den am häufigsten verwendeten Applikationen auf mobilen Endgeräten. Sie werden von nahezu allen Altersgruppen genutzt, dabei verwenden eine Vielzahl der Nutzer diese täglich zum Austausch von textuellen Nachrichten, Sprachnachrichten oder multimedialer Dateien. Die Anzahl der Nutzer nimmt seit Jahren kontinuierlich zu. Einer der verbreitetsten Anwendungen ist „Threema“, welche von 22 Prozent der Befragten in Deutschland genutzt wird. Weltweit beträgt die Anzahl der Nutzer elf Millionen. Im Kontext forensischer Untersuchungen wird die Bedeutung der Rekonstruktion von Artefakten von Instant Messenger-Diensten immer größer, da über diese auch ein Austausch von Informationen durch Täter, Opfer und Zeugen von Straftaten stattfindet. Solche Artefakte umfassen Bild- und Videomaterial sowie Standorte oder Textnachrichten. Diese können hilfreich sein, um den Tathergang zu rekonstruieren.

In der vorliegenden Bachelorarbeit werden die Artefakte der Instant Messengers „Threema“ anhand von Beispieldaten aufbereitet und ausgewertet. Dabei stehen Chatverläufe, ausgetauschte Standorte und Kontaktinformationen im Fokus, wobei sie keine Entschlüsselung der Daten oder Rekonstruktion von multimedialen Daten oder gelöschte Daten umfasst. Die Untersuchungen ergaben, dass die Daten in den SQLite-Datenbanken *ThreemaData.sqlite* und *Threema.sqlite-wal* abgelegt werden.

[1] Um die Lesbarkeit zu verbessern, wird in dieser Arbeit bei Personenbezeichnungen und personenbezogenen Hauptwörtern die männliche Form gewählt. Die Verwendung dieser Begriffe erfolgt im Sinne der Gleichbehandlung ausdrücklich für alle Geschlechter. Die verkürzte Sprachform ist wertneutral.

Abstract[2]

Instant messengers are among the most frequently used applications on mobile devices. They are used by almost all age groups, and a large number of users use them daily to exchange text messages, voice messages or multimedia files. The number of users has been increasing continuously for years. One of the most widespread applications is “Threema”, which is used by 22 percent of respondents in Germany. Worldwide, the number of users is eleven million. In the context of forensic investigations, the reconstruction of artefacts from instant messenger services is becoming increasingly important, as they are also used by perpetrators, victims and witnesses of crimes to exchange information. Such artefacts include images and video footage as well as locations or text messages. These can be helpful in reconstructing the course of events.

In this bachelor thesis, the artefacts of the instant messenger "Threema" are processed and evaluated using sample data. The focus is on chat histories, exchanged locations and contact information, although it does not include any decoding of the data or reconstruction of multimedia data or deleted data. The research revealed that the data is stored in the SQLite databases ThreemaData.sqlite and *Threema.sqlite-wal*.

[2] To improve readability, the masculine form is used in this work for personal names and personal nouns. In the interest of equal treatment, these terms are used expressly for all genders. The abbreviated form of language is value-neutral.

Inhalt

Zusammenfassung ..... **I**

Abstract ..... **II**

Inhalt ..... **III**

Abbildungsverzeichnis ..... **V**

Tabellenverzeichnis ..... **VII**

Abkürzungsverzeichnis ..... **IX**

1 Einleitung **1**

2 Grundlagen **6**

2.1 IT-Forensik *6*

2.2 Prozessmodell *8*

2.2.1 Strategische Vorbereitung (SV) 8

2.2.2 Operationale Vorbereitung (OV) 9

2.2.3 Datensammlung (DS) 9

2.2.4 Untersuchung (US) 11

2.2.5 Datenanalyse (DA) 12

2.2.6 Abschlussbericht (DO) 12

2.3 Methoden der IT-Forensik *12*

2.3.1 Betriebssystem (BS) 13

2.3.2 Dateisystem (FS) 14

2.3.3 Explizite Methoden der Einbruchserkennung (EME) 15

2.3.4 IT-Anwendung (ITA) 15

2.3.5 Skalierung von Beweismitteln (SB) 15

2.3.6 Datenbearbeitung und Auswertung (DBA) 15

2.4 Mobile Forensik *16*

2.5 Reverse Engineering *19*

2.6 Instant Messenger-Dienste (IM-Dienst) *22*

2.6.1 Begriffsdefinition und Abgrenzung 22

2.6.2 Threema 24

3 Verwandte Arbeiten **26**

4 Methodik: Untersuchung der Daten eines IM-Dienstes ... 28

4.1 Vorbereitungsphase ... 28

4.2 Analysephase ... 29

4.3 Aufbereitungsphase ... 29

5 Reverse Engineering der Messenger-App „Threema" unter iOS ... 31

5.1 Vorbereitungsphase ... 31

5.1.1 Design des Experiments ... 31

5.1.2 Analyse der Funktionen der Applikationen ... 32

5.2 Analyse- und Aufbereitungsphase ... 33

5.2.1 Analyse und Auswertung der Chatverläufe und angehängter Dateien ... 35

5.2.2 Analyse und Aufbereitung der Standortinformationen ... 52

5.2.3 Analyse und Aufbereitung der Kontaktinformationen ... 55

6 Diskussion ... 61

7 Fazit ... 63

Literatur ... 65

Anlagen ... 71

Abbildungen, Teil 1 ... 73

Tabellen, Teil 2 ... 79

Selbständigkeitserklärung ... 115

Abbildungsverzeichnis

Abbildung 1: Übersicht der beliebtesten Arten von Smartphone-Apps in Deutschland ..1

Abbildung 2: Übersicht über die genutzten Messenger Apps in Deutschland 2

Abbildung 3: Anzahl der Threema-Nutzer.....3

Abbildung 4: Vorgehensmodell nach BSI Leitfaden IT-Forensik, angelehnt an Bundesamt für Sicherheit in der Informationstechnik, 2011, S. 61 8

Abbildung 5: Prozess der Untersuchung von Mobiltelefonen, angelehnt an Dogan; Akbal, Analysis of mobile phones in digital forensics, 2017, S. 1242 16

Abbildung 6: Übersicht der fundamentalen Informationen der Untersuchung von Mobiltelefonen, angelehnt an Dogan; Akbal, Analysis of mobile phones in digital forensics, 2017, S. 1242.....17

Abbildung 7: Überblick über die Begriffe des Forward Engineerings und Reverse Engineerings angelehnt an Chikofsky; Cross, 1990, S. 14 20

Abbildung 8: IM Communications Model, angelehnt an Mannan; Oorschot, 2004, S. 324

Abbildung 9: Übersicht der Vorgehensweise einer forensischen Untersuchung eines IMs 28

Abbildung 10: Suchergebnisse des Suchbegriffes „threema“ mittels Cellebrite 34

Abbildung 11: Struktur der SQL-Datenbank.....35

Abbildung 12: Überblick über die Verzeichnisstruktur.....36

Abbildung 13: Eintrag (Hex-Dump) einer Textnachricht.....40

Abbildung 14: Eintrag (Hex-Dump) mit versendetem Anhang 41

Abbildung 15: Welche der folgenden Social-Media-Plattformen nutzen Sie?.....73

Abbildung 16: Anteil der Befragten, die am Tag vor der Erhebung einen Instant-Messaging-Dienst genutzt haben, nach Altersgruppen in Deutschland im Jahr 2022 74

Abbildung 17: Anzahl der Nutzer von Threema weltweit 75

Abbildung 18: Nutzung von Messenger-Apps weltweit in den Jahren 2018 bis 2020 sowie eine Prognose bis 2025 75

Abbildung 19: Smartphone-Nutzung weltweit von 2016 bis 2020 und Prognose bis 2024 76

Abbildung 20: Entwicklung der Weltbevölkerung.....77

Abbildung 21: Marktanteile der Betriebssysteme am Absatz vom Smartphones weltweit in den Jahren 2010 bis 2022 und Prognose bis 2027 78

Tabellenverzeichnis

Tabelle 1: Mapping der Methodenkategorien und der Phase des Prozessmodells, angelehnt an Bundesamt für Sicherheit in der Informationstechnik, 2011, S. 67 13

Tabelle 2: Testgeräte 32

Tabelle 3: Auszug aus exportierter Tabelle aus Cellebrite 38

Tabelle 4: Auszug aus exportierter Tabelle aus Cellebrite (Nachricht mit Anhang) 40

Tabelle 5: Tabelle ZMESSAGE der SQL-Datenbank 42

Tabelle 6: Übersicht der exportierten Standorte 53

Tabelle 7: Export der Informationen zu den Kontakten aus Cellebrite 56

Tabelle 8: Tabellentyp ZCONTACT der SQL-Datenbank 57

Tabelle 9: Experiment 1: Einzelchats Teil I 79

Tabelle 10: Experiment 1: Einzelchats Teil II 80

Tabelle 11: Experiment 1: Einzelchats Teil III 81

Tabelle 12: Experiment 1: Einzelchats Teil IV 81

Tabelle 13: Experiment 1: Einzelchats Teil V 89

Tabelle 14: Experiment 1: Einzelchats Teil VI 92

Tabelle 15: Experiment 2: Gruppenchat Teil I 95

Tabelle 16: Experiment 2: Gruppenchat Teil II 95

Tabelle 17: Experiment 2: Gruppenchat Teil III 96

Tabelle 18: Experiment 2: Gruppenchat Teil IV 107

Tabelle 19: Experiment 2: Gruppenchat Teil V 112

Tabelle 20: Experiment 2: Gruppenchat Teil VI 114

Abkürzungsverzeichnis

App	Applikation
BS	Betriebssystem
BSI	Bundesamt für Sicherheit in der Informationstechnik
ch.	länderspezifische Top-Level-Domain der Schweiz
DA	Datenanalyse
DBA	Datenbearbeitung und Auswertung
DO	Dokumentation
DS	Datensammlung
EEEMA	End-to-End Encrypted Messaging Application
EME	Explizite Methoden der Einbruchserkennung
FS	Dateisystem
GmbH	Gesellschaft mit beschränkter Haftung
HTML	Hypertext Markup Language (Hypertext Aufzeichnungssprache)
https	Hypertext Transfer Protocol Secure (Sicheres Hypertext-Übertragungs-protokoll)
ID	Identifikationsnummer
IDS	Intrusion Detection System
IM	Instant Messenger
Inc.	Incorporated

iOS	Internetwork Operation System
IT	Informationstechnologie
ITA	IT-Anwendungen
LTD.	Limited
NaCL	Networking and Cryptography Library
OV	Operationale Vorbereitung
SB	Skalierung von Beweismitteln
SQL	Structured Query Language
SV	Strategische Vorbereitung
TCP	Transmission Control Protocol
UFDR	Universal Forensic Extraction Device Report
US	Untersuchung
XML	Extensible Markup Language

1 Einleitung

Im Jahr 2023 gehören Messenger Apps zu den am meisten genutzten Smartphone-Anwendungen in Deutschland. Über 50 Prozent der Befragten benannten Messenger Applikationen (Apps) als beliebteste Art von Smartphones-Apps (vgl. Abbildung 1). Der Instant Messenger-Dienst (IM-Dienst) WhatsApp wird z.B. von mehr als 80 Prozent in allen befragten Altersgruppen genutzt (vgl. Abbildung 15). Dabei wurde dieser von über 60 Prozent mindestens den Tag vor der zugehörigen Umfrage verwendet (vgl. Abbildung 16). Insgesamt steigt die Anzahl der Nutzer des Messengers „Threema“ weltweit seit 2014 stetig an und erreichte im Jahre 2022 elf Millionen (vgl. Abbildung 17). Dies verdeutlicht die große Verbreitung.

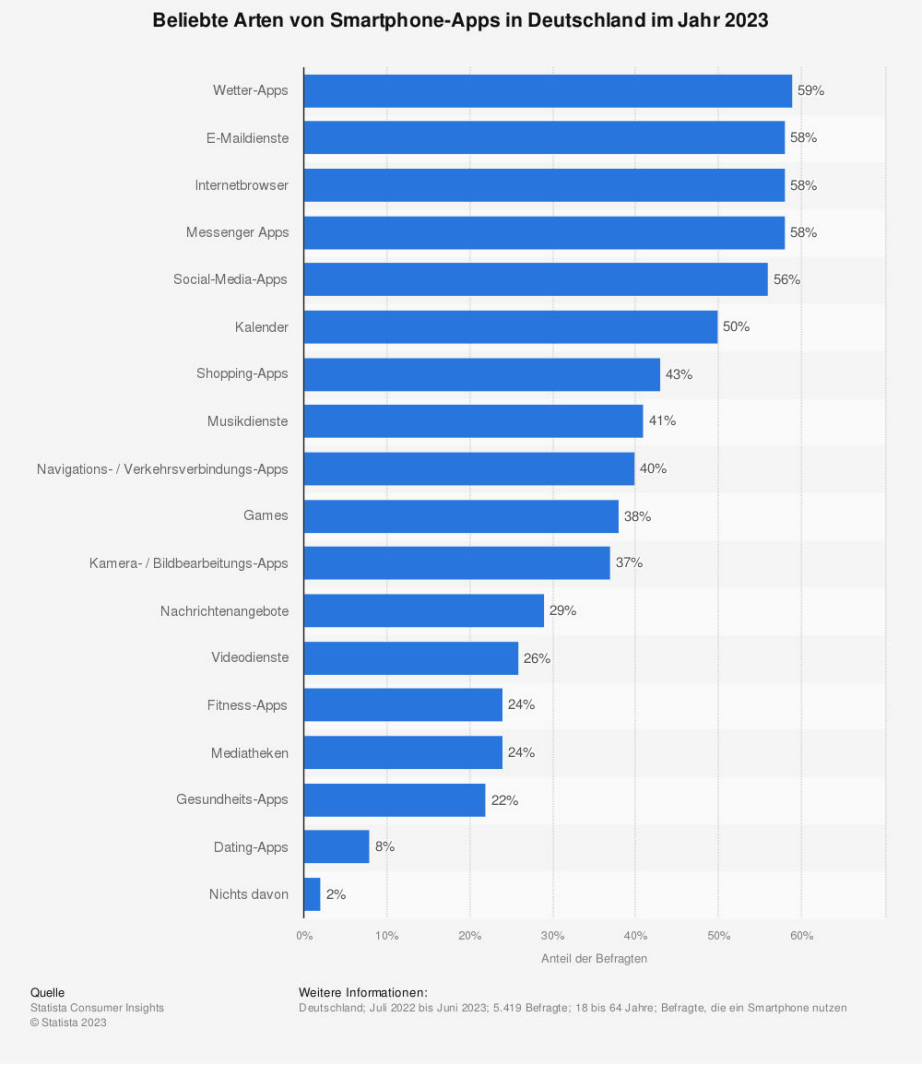

Abbildung 1: Übersicht der beliebtesten Arten von Smartphone-Apps in Deutschland

Insgesamt nahm die Nutzung von Instant Messenger-Diensten in den letzten Jahren stark zu (vgl. Abbildung 18). Im Folgenden wird der Messenger-Dienst „Threema“ betrachtet. Dieser wird im deutschen Raum von etwa zwölf Prozent der Befragten genutzt und gehört zu den am verbreitetsten Diensten in Deutschland (vgl. Abbildung 2). Dabei wurde diese Applikation bisher unter dem Betriebssystem Internetwork Operation System (iOS) noch nicht detailliert untersucht, was in Kapitel 3 detailliert erläutert wird.

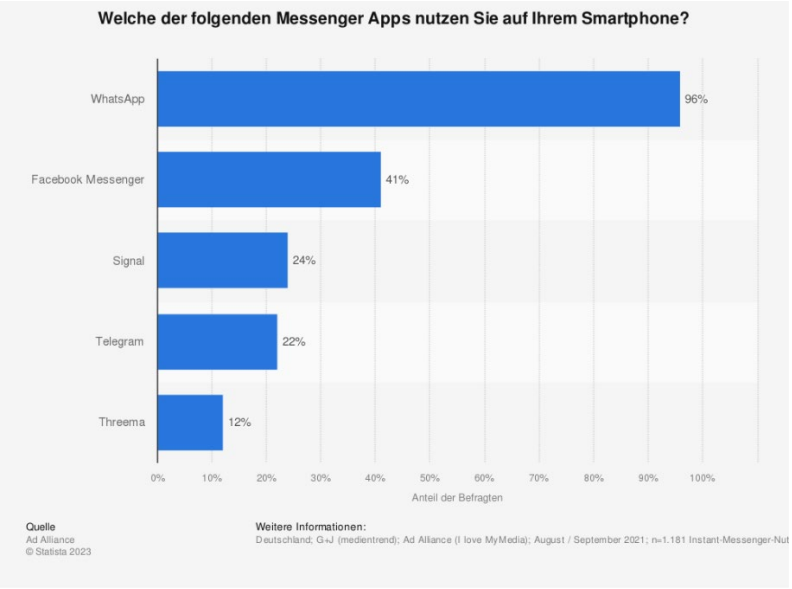

Abbildung 2: Übersicht über die genutzten Messenger Apps in Deutschland

Seit 2014 verzeichnet der Messenger-Dienst “Threema” eine kontinuierliche Zunahme der Nutzerzahlen, die im Jahr 2022 elf Millionen erreichte (vgl. Abbildung 17).

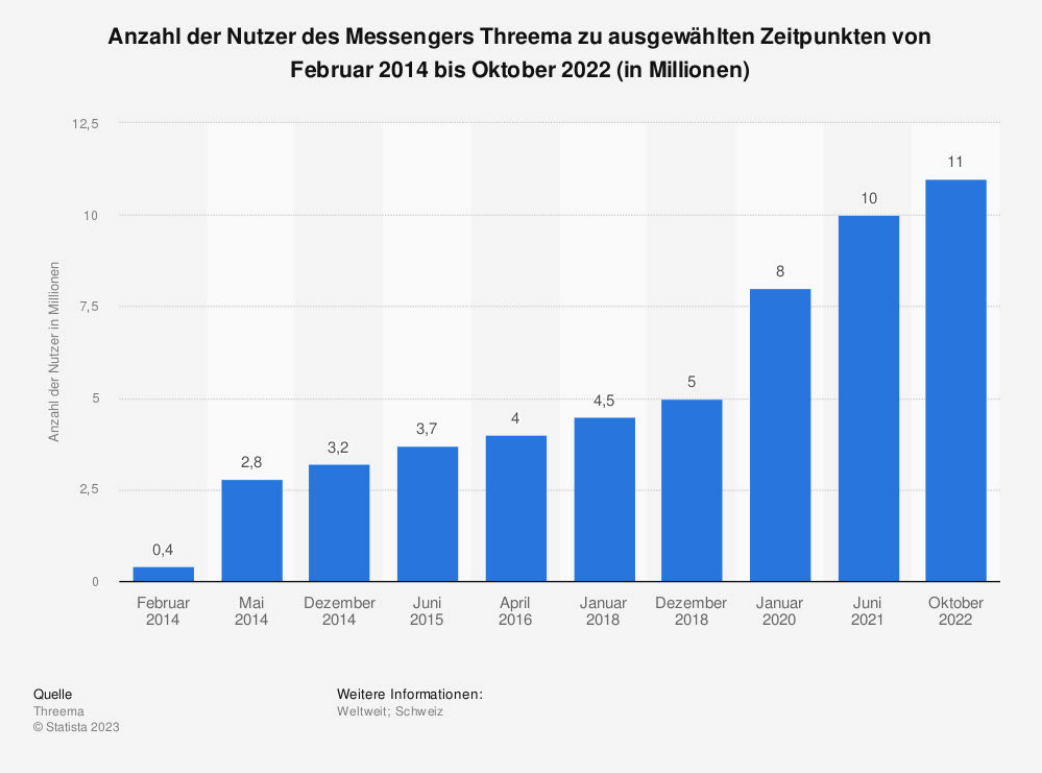

Abbildung 3: Anzahl der Threema-Nutzer

Im Verlaufe der Entwicklung der Applikation wurden diverse Sicherheitsfunktionen, einschließlich der Ende-zu-Ende-Verschlüsselung, integriert (Threema GmbH, 2023). Diese können die Analyse, Untersuchung und Sicherung für forensische Experten umständlicher und komplexer gestalten, was potenziell das Interesse von Kriminellen wecken könnte, da es die Ermittlungsprozesse erheblich erschweren würde.

Daraus wird ersichtlich, dass „Threema“ für forensische Untersuchungen relevant werden kann. Täter, Opfer und Zeugen können sich mittels des IMs über mögliche Straftaten austauschen, sowohl in Form von Textnachrichten als auch multimedialer Dateien. Dies kann vor der Tat infolge der Planung aber auch nach der Tat geschehen. Die Informationen können Ermittlern bei der Rekonstruktion des Tathergangs unterstützen. Zudem kann der IM-Dienst als Werkzeug zur Begehung von Straftaten wie Betrug benutzt werden. Um potenzielle Informationen und Beweise zu extrahieren, die im strafrechtlichen Kontext

relevant sein könnten, kann die Applikation mittels „Reverse Engineering“[3] untersucht und daraus resultierende Informationen wie z.B. die Ablageorte von Dateien erforscht werden. Dadurch können sowohl gelöschte Daten als auch solche, die nicht trivial zugänglich sind, sowie Sicherheitslücken oder Schwachstellen identifiziert werden. Am Ende zielt die Untersuchung darauf ab, alle Daten, die von der App gespeichert bzw. erzeugt wurden, zu sichern, um diese anschließend auszuwerten. Durch eine Vielzahl von Instant Messengern, die sich in Funktionen, Speicherorten und -formaten unterscheiden, wird die Arbeit der Ermittler komplex. Um forensisch relevante Informationen wie Chatverläufe zu sichern und auszuwerten, sind Kenntnisse über diese Spezifikationen notwendig. Die gewonnenen Erkenntnisse können dazu beitragen, Methoden und Werkzeuge zur effektiven Untersuchung von digitalen Beweismitteln aus „Threema“ Nachrichten zu entwickeln und zu verfeinern.

In dieser Bachelorarbeit wird der Messenger-Dienst „Threema“ in der Version 3.6.13 unter dem mobilen Betriebssystem iOS analysiert und in Form des „Reverse Engineerings“ detailliert analysiert. Diese Arbeit behandelt nicht die Entschlüsselung und Erzeugung der Daten. Besonderer Fokus liegt auf den Ablageorten von Standorten, multimedialer Dateien und Chatverläufen. Es soll folgende Forschungsfrage beantwortet werden:

Wie können forensische Experten Informationen, welche für die Aufklärung von potenziellen Straftaten hilfreich sein könnten, aus den Daten, welche durch die Nutzung des Instant-Messengers „Threema“ erzeugt werden, aufbereiten und auswerten?

Zuerst wird im zweiten Kapitel ein Überblick über die theoretischen Grundlagen geschaffen, indem die Grundsätze der Forensik, das Modell zu der allgemeinen Vorgehensweise in forensischen Untersuchungen vorgestellt und die Begriffe der IT-Forensik, der mobilen Forensik und des Reverse Engineerings definiert und abgegrenzt werden. Im Fokus des dritten Kapitels steht die Einordnung der Arbeit in den Kontext zu anderen wissenschaftlichen Arbeiten, welche IM-Dienste bereits rekonstruiert haben. Im vierten und fünften Kapitel wird die Vorgehensweise zur Untersuchung von Instant Messengern (IM) und die Ergebnisse der Analyse der Applikation „Threema“ vorgestellt. Hierbei wird im vierten Kapitel die Vorgehensweise und im fünften Kapitel die Analyse der IM-Dienstes “Threema” erläutert. Im Mittelpunkt des sechsten Kapitels steht die Diskussion der Annahmen und Grenzen der

[3] Siehe Kapitel 2.2 der vorliegenden Arbeit

vorliegenden Bachelorarbeit. Zuletzt werden im siebenten Kapitel die Ergebnisse konsolidiert sowie ein Ausblick gegeben.

2 Grundlagen

Im folgenden Kapitel werden die theoretischen Grundlagen des forensischen Vorgehens erläutert. Dabei wird auf die Anforderungen an die Untersuchungen sowie das Prozessmodell einer forensischen Untersuchung nach dem Bundesamt für Sicherheit in der Informationstechnik (BSI) eingegangen. Weitergehend wird insbesondere die mobile Forensik spezifiziert. Zudem wird der Begriff des “Reverse Engineering” definiert und Herausforderungen dessen benannt.

2.1 IT-Forensik

Der Begriff der Forensik leitet sich von dem lateinischen Worten „Forum“, das übersetzt „Markplatz“ bedeutet, ab (Siller, 2018). Das Forum stellte im antiken Rom den Ort der Gerichtsbarkeit dar. Es wurden Gerichtsverfahren sowie Untersuchungen durchgeführt, Urteile verkündet und ebenfalls wurde die Exekution strafrechtlicher Maßnahmen in diesem Umfeld durchgeführt (Siller, 2018).

Im Fokus der Forensik steht die Suche und Sicherung von Beweisen, welche vor Gericht verwertbar sind und durch den Einbezug dieser der Tathergang rekonstruiert werden kann (Dewald; Freiling, 2015, S. 8). Die IT-Forensik als Teilgebiet der allgemeinen Forensik beschreibt „[…] 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.“ (Dewald; Freiling, 2015, S. 8).

Dabei existieren zwei grundlegende Vorgehensweisen. Zum einen die Post-Mortem-Analyse, welche Untersuchungen beschreibt, die nach dem Abschluss des Vorfalls durchgeführt werden und zum anderen die Live-Forensik, welche die Untersuchungen während des Vorfalls umfasst (Bundesamt für Sicherheit in der Informationstechnik, 2011, S. 13).

Nach dem BSI-Leitfaden zu der IT-Forensik liegt bei der Post-Mortem-Analyse der Fokus auf der Sicherung des Speicherabbildes. Flüchtige Spuren werden nicht analysiert (Bundesamt für Sicherheit in der Informationstechnik, 2011, S. 13). Die Forensiker versuchen, gelöschte, umbenannte oder versteckte sowie verschlüsselte Dateien zu finden und zu rekonstruieren (Bundesamt für Sicherheit in der Informationstechnik, 2011, S. 13). Die Live-Forensik hingegen konzentriert sich auf flüchtige Spuren. In Zuge dieser werden

Hauptspeicherinhalte, Netzwerkverbindungen und gestartete Prozesse analysiert (Bundesamt für Sicherheit in der Informationstechnik, 2011, S. 13).

Die forensische Untersuchung zielt darauf ab, zu beantworten, was, wo, wann und wie passiert ist. Zudem wird beabsichtigt zu klären, wer die Tat begangen hat und wie eine Wiederholung vermieden werden kann. Dabei gilt es zu beachten, dass jeder und alles etwas am Tatort mitnimmt und zurücklässt (Dewald; Freiling, 2015, S. 8). Dieses Prinzip wurde durch den französischen Mediziner und Rechtswissenschaftler, Edmond Locard, im 19. Jahrhundert begründet und ist unter dem Locardschen Grundsatz des Austauschs bekannt (McDermid, 2016, S. 17 f.). Daher ist es erforderlich, sämtliche Veränderungen an Tatorten sorgfältig zu dokumentieren, damit diese Ermittler oder andere anwesende Personen nachvollziehen können.

Forensische Untersuchungen müssen nach Geschonneck (2014, S. 66 f.) folgenden Grundsätzen entsprechen:

- **Akzeptanz**: Die angewandten Methoden und Schritte müssen in der Fachwelt dokumentiert und akzeptiert sein (Geschonneck, 2014, S. 66 f.). Dabei ist besonders zu beachten, dass neue Verfahren und Methoden nur mit besonderem Nachweis der Korrektheit verwendet werden sollten (Geschonneck, 2014, S. 66 f.).
- **Glaubwürdigkeit**: Angewendete Methoden müssen robust sein (Geschonneck, 2014, S. 66 f.). Diese müssen fallweise bewiesen werden (Geschonneck, 2014, S. 66 f.).
- **Wiederholbarkeit:** Versuche müssen unter identischen Bedingungen (Methoden und Hilfsmittel), zu denselben Ergebnissen führen (Geschonneck, 2014, S. 66 f.).
- **Integrität**: Während der Durchführung der forensischen Untersuchungen dürfen keine Veränderungen erfolgen, welche nicht dokumentiert werden (Geschonneck, 2014, S. 66 f.). Es gilt, die Integrität jederzeit belegen zu können (Geschonneck, 2014, S. 66 f.).
- **Ursache und Auswirkungen:** Die Methodenauswahl sollte eine sinnvolle und nachvollziehbare Verknüpfung von Ereignissen, Beweisspuren und Personen ermöglichen (Geschonneck, 2014, S. 66 f.).
- **Dokumentation**: Jeder Schritt des Ermittlungsprozesses muss detailliert festgehalten werden (Geschonneck, 2014, S. 66 f.).

2.2 Prozessmodell

Das BSI empfiehlt zur forensischen Untersuchung das Modell, welches in Abbildung 4 dargestellt ist (Bundesamt für Sicherheit in der Informationstechnik, 2011, S. 8). Die einzelnen Phasen werden im Folgenden detailliert beschrieben. Prozessübergreifend ist die Dokumentation jedes Ermittlungsschrittes zu beachten. Diese ist insbesondere dafür notwendig, die Authentizität und Integrität der Beweisaufnahme zu ermöglichen (Bundesamt für Sicherheit in der Informationstechnik, 2011, S. 23 f.).

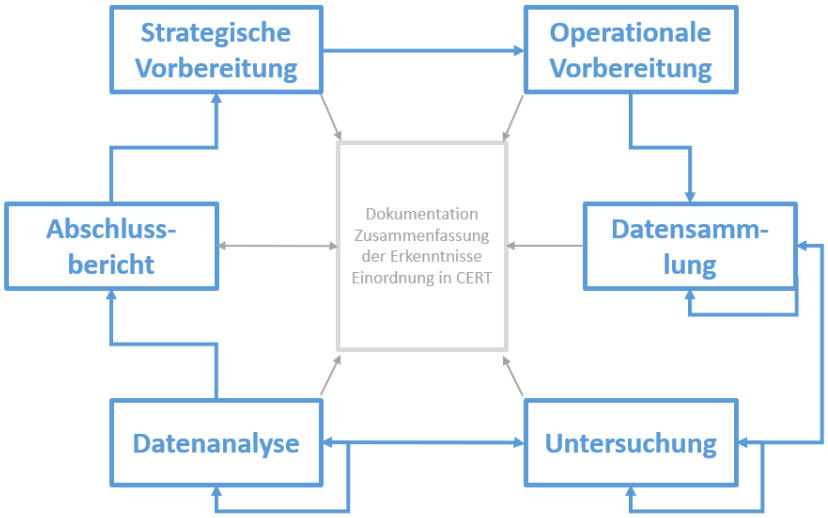

Abbildung 4: Vorgehensmodell nach BSI Leitfaden IT-Forensik, angelehnt an Bundesamt für Sicherheit in der Informationstechnik, 2011, S. 61

2.2.1 Strategische Vorbereitung (SV)

Die forensische Untersuchung beginnt mit der strategischen Vorbereitung (Bundesamt für Sicherheit in der Informationstechnik, 2011, S. 17 f.). Zu dieser werden die Maßnahmen zugeordnet, welche getroffen wurden, bevor es zu einem Vorfall gekommen ist (Bundesamt für Sicherheit in der Informationstechnik, 2011, S. 17 f.). Dazu gehört z.B. die Aktivierung von Logdiensten, die Zeitsynchronisation sowie die Definition von Sicherheits- und Forensik-Konzepten (Bundesamt für Sicherheit in der Informationstechnik, 2011, S. 17 f.). In dieser Phase bereiten Forensiker die Ermittlungen vor, indem sie geeignete

Sicherungstools[4] auswählen und testen, Vorgehenspläne erstellen und Hard- sowie Software vorbereiten (Bundesamt für Sicherheit in der Informationstechnik, 2011, S. 17 f.).

Damit werden in dieser Phase Prozesse geplant und aufgebaut, um im Falle eines Vorfalls schnellst- und bestmöglich reagieren und intervenieren zu können (Bundesamt für Sicherheit in der Informationstechnik, 2021, S. 17 f.).

2.2.2 Operationale Vorbereitung (OV)

Die operationale Vorbereitung umfasst Maßnahmen, welche direkt nach dem Eintreten des Vorfalls und vor der Datensammlung notwendig sind (Bundesamt für Sicherheit in der Informationstechnik, 2011, S. 62 f.). Die Untersuchung des eingetretenen Vorfalls beginnt mit einer ersten Bestandsaufnahme (Bundesamt für Sicherheit in der Informationstechnik, 2011, S. 62 f.). Dabei wird ein Überblick über ggf. betroffene Netzwerke sowie die verfügbaren Datenquellen erarbeitet und Datenquellen wie Mobiltelefone, Computer, USB-Sticks, externe Festplatten, RAM, Routerkonfigurationen, Netzwerkstatus, Logfiles u. ä. gesucht, identifiziert sowie beschriftet (Bundesamt für Sicherheit in der Informationstechnik, 2011, S. 62 f.).

2.2.3 Datensammlung (DS)

Im nächsten Schritt werden die in den vorherigen Phasen identifizierten, möglichen Daten gesichert (Bundesamt für Sicherheit in der Informationstechnik, 2011, S. 88 ff.). Eine große Herausforderung stellt die Flüchtigkeit von Daten sowie eine mögliche Veränderung durch Zugriffe o.ä. dar (Bundesamt für Sicherheit in der Informationstechnik, 2011, S. 88 ff.). Dabei empfiehlt das BSI folgende Reihenfolgen für die Datensammlung:

- Erfassung der aktuellen Systemzeit und des -datums
- Erfassung der laufenden Prozesse auf dem System
- Erfassung der geöffneten Netzwerkverbindungen

[4] Sicherungstools umfassen spezialisierte Softwareanwendungen, die verwendet werden, um digitale Beweise und Informationen forensisch zu sammeln und zu sichern. Diese müssen die Integrität der Daten gewährleisten können, damit diese in Folge der Sicherung unverändert bleiben (Bundesamt für Sicherheit in der Informationstechnik, 2011, S. 26 f.).

- Erfassung der angemeldeten Nutzer (Bundesamt für Sicherheit in der Informationstechnik, 2011, S. 88 ff.)

Die Erfassung der Systemzeit sowie des -datums dient dem Erkennen und Dokumentieren eventueller Abweichungen zur Referenzzeit (Bundesamt für Sicherheit in der Informationstechnik, 2011, S. 88 ff.). Es werden Images von den Massenspeichern erstellt (Bundesamt für Sicherheit in der Informationstechnik, 2011, S. 88 ff.). Dabei sind integritätssichernde Maßnahmen zwingend notwendig (Bundesamt für Sicherheit in der Informationstechnik, 2011, S. 88 ff.). Zudem sollte über das erhaltende Image zur Gewährleistung der Integrität eine sichere kryptografische Hashsumme berechnet werden (Bundesamt für Sicherheit in der Informationstechnik, 2011, S. 88 ff.). Dazu empfiehlt das BSI folgende Hashfunktionen:

- SHA-256, SHA-512/256, SHA-384 und SHA-512
- SHA3-256, SHA3-384, SHA3-51 (Bundesamt für Sicherheit in der Informationstechnik, 2023, S. 46).

Es ist außerdem ratsam, sämtliche laufende Prozesse zu dokumentieren (Bundesamt für Sicherheit in der Informationstechnik, 2011, S. 88 ff.). Diese Prozessdaten sollten idealerweise mithilfe von statisch kompilierten Programmen von einem schreibgeschützten Datenträger gesichert werden, um eine unbeabsichtigte Beeinflussung der Systemprogramme zu vermeiden (Bundesamt für Sicherheit in der Informationstechnik, 2011, S. 88 ff.). Zudem müssen jegliche notwendigen Veränderungen am System unbedingt in der Dokumentation festgehalten werden (Bundesamt für Sicherheit in der Informationstechnik, 2011, S. 88 ff.). Unvermeidbare Veränderungen am System müssen zwingend dokumentiert werden (Bundesamt für Sicherheit in der Informationstechnik, 2011, S. 88 ff.). Auch für die Prozessdaten gilt es, integritätssichernde Maßnahmen zu ergreifen (Bundesamt für Sicherheit in der Informationstechnik, 2011, S. 88 ff.). Hierzu empfiehlt es sich, Hashsummen über die Ausgaben der verwendeten Tools zu berechnen (Bundesamt für Sicherheit in der Informationstechnik, 2011, S. 88 ff.). Die Sicherung der Authentizität kann mittels des Vier-Augen-Prinzips im Zuge der prozessbegleitenden Dokumentation gewährleistet werden (Bundesamt für Sicherheit in der Informationstechnik, 2011, S. 88 ff.). Die Vertraulichkeit, welche aus der Notwendigkeit des Datenschutzes in dieser Phase resultiert, wird durch den Einsatz von Verschlüsselungen der gewonnenen Daten gewahrt (Bundesamt für Sicherheit in der Informationstechnik, 2011, S. 88 ff.).

Zusätzlich sollten alle offenen Netzwerkverbindungen festgehalten werden (Bundesamt für Sicherheit in der Informationstechnik, 2011, S. 88 ff.). Hierbei resultiert die Notwendigkeit primär aus der möglichen Übertragung von Schadsoftware. Fallweise ist hierbei eine Datenschutzrelevanz gegeben, weswegen in entsprechenden Fällen die gewonnenen Daten verschlüsselt werden (Bundesamt für Sicherheit in der Informationstechnik, 2011, S. 88 ff.). Gleiches gilt für die Erfassung aller eingeloggten Benutzer und der Erstellung der forensischen Duplikationen der betroffenen Massenspeicher (Bundesamt für Sicherheit in der Informationstechnik, 2011, S. 88 ff.).

Mit Beginn der Phase der Datensammlung muss detailliert und lückenlos dokumentiert werden, wann Beweismittel eingesehen werden und wo sich diese befinden (Bundesamt für Sicherheit in der Informationstechnik, 2011, S. 88 ff.). Außerdem muss die Beweismittelkette (engl. „Chain of Custody“) zwingend gewahrt werden, um die Verwertbarkeit der Beweise vor Gericht zu gewährleisten (Bundesamt für Sicherheit in der Informationstechnik, 2011, S. 88 ff.).

2.2.4 Untersuchung (US)

In der vierten Phase des Prozesses steht die Extraktion der relevanten Daten aus den gesammelten Datenquellen im Fokus (Bundesamt für Sicherheit in der Informationstechnik, 2011, S. 90 f.). Dabei werden Daten in andere, besser lesbare Formate überführt, wie z.B. durch das Einbinden eines Festplattenabbildes der zu untersuchenden IT-Komponente (Bundesamt für Sicherheit in der Informationstechnik, 2011, S. 90 f.). Einen Mehrwert bietet zudem die Untersuchung der Logdateien (Bundesamt für Sicherheit in der Informationstechnik, 2011, S. 90 f.). Dabei findet im Zuge der Untersuchung eine Vorfilterung statt, um die entsprechenden Einträge im nächsten Schritt der Datenanalyse auswerten zu können (Bundesamt für Sicherheit in der Informationstechnik, 2011, S. 90 f.). In Folge der Untersuchung kann es dazu kommen, dass weitere Datenquellen detektiert werden, welche für die Analyse relevant sein können (Bundesamt für Sicherheit in der Informationstechnik, 2011, S. 90 f.). Es resultiert daraus eine erneute Datensammlung (Bundesamt für Sicherheit in der Informationstechnik, 2011, S. 90 f.).

2.2.5 Datenanalyse (DA)

In der vorletzten Prozessphase, der Datenanalyse, erfolgt eine ausführlichere Analyse der Ergebnisse der vorangehenden Untersuchung (Bundesamt für Sicherheit in der Informationstechnik, 2011, S. 91). Hierbei werden z. B. Beziehungen zwischen mehreren Datenquellen gesucht und dokumentiert. Dies zielt darauf ab, zeitliche Abläufe zu rekonstruieren oder ggf. Schlussfolgerungen auf die Urheberschaft zu gewinnen (Bundesamt für Sicherheit in der Informationstechnik, 2011, S. 91). Während der Detailanalyse der gewonnenen Daten besteht die Möglichkeit, dass weitere Datenquellen identifiziert werden und daraus resultierend eine erneute Datensammlung notwendig ist (Bundesamt für Sicherheit in der Informationstechnik, 2011, S. 91). Es ist zwingend notwendig, bei der Datenanalyse jeden Schritt ausführlich zu dokumentieren (Bundesamt für Sicherheit in der Informationstechnik, 2011, S. 91).

2.2.6 Abschlussbericht (DO)

Zuletzt werden die gesammelten Dokumente und Ergebnisse der Analyse in Form eines Abschlussberichtes zusammengefasst (Bundesamt für Sicherheit in der Informationstechnik, 2011, S. 65).

2.3 Methoden der IT-Forensik

Das BSI unterscheidet zwischen folgenden sechs verschiedenen Methodenkategorien:

- Betriebssystem (BS)
- Dateisystem (FS)
- Explizite Methoden zur Einbruchserkennung (EME)
- IT-Anwendungen (ITA)
- Skalierung der Beweismöglichkeiten (SB)
- Datenbearbeitung und Auswertung (DBA) (Bundesamt für Sicherheit in der Informationstechnik, 2011, S. 10 f.), (vgl. Tabelle 1)

Tabelle 1: Mapping der Methodenkategorien und der Phase des Prozessmodells, angelehnt an Bundesamt für Sicherheit in der Informationstechnik, 2011, S. 67

	SV	OV	DS	US	DA	DO
BS	X	X	X	X	X	
FS			X	X		
EME	X		X			
ITA	X		X			
SB			X	X		
DBA			X	X	X	X

2.3.1 Betriebssystem (BS)

Ein Großteil der forensischen Datenquellen wird in dem Betriebssystem verwaltet, wodurch eine Vielzahl von forensisch wertvollen Informationen im Betriebssystem abliegen können (Bundesamt für Sicherheit in der Informationstechnik, 2011, S. 66 f.). Das Betriebssystem beschreibt die Programme eines digitalen Rechnersystems, welche mit den Eigenschaften der Rechenanlage das Fundament der möglichen Betriebsarten bilden und die Steuerung sowie Überwachung von Prozessen abwickeln (Richter, 1985, S. 3).

Es bestehen folgenden Speichermöglichkeiten:

- der flüchtige, der sogenannte Arbeitsspeicher und
- der nichtflüchtige, der Massenspeicher (Bundesamt für Sicherheit in der Informationstechnik, 2011, S. 66 f.).

Verschiedene Daten werden durch das BS erzeugt (Bundesamt für Sicherheit in der Informationstechnik, 2011, S. 66 f.). Dazu gehören z.B. aktuelle Netzwerkverbindungen und

Log-Einträge wie Sitzungsdaten oder Daten von laufenden Prozessen (Bundesamt für Sicherheit in der Informationstechnik, 2011, S. 66 f.).

Grundsätzlich findet sich die Methode in allen Phasen des forensischen Untersuchungsprozesses wieder (Bundesamt für Sicherheit in der Informationstechnik, 2011, S. 70 f.). Teilweise treten signifikante Einschränkungen auf, wodurch die Qualität der Informationen beeinträchtigt wird (Bundesamt für Sicherheit in der Informationstechnik, 2011, S. 70 f.). Eine Besonderheit des Betriebssystems stellt die minimale Anzahl an verfügbaren Methoden dar, wenn die strategische Vorbereitung nicht vorgenommen wurde (Bundesamt für Sicherheit in der Informationstechnik, 2011, S. 70 f.); (vgl. Tabelle 1).

2.3.2 Dateisystem (FS)

Die Methode des Dateisystems ist von großer Bedeutung für die Post-Mortem-Forensik, da es einen der bedeutsamsten Orte darstellt, um nichtflüchtige Daten zu finden (Bundesamt für Sicherheit in der Informationstechnik, 2011, S. 71 f.). Das Dateisystem gewährleistet, dass der Benutzer einen einheitlichen Zugriff auf gespeicherte Daten hat (Bundesamt für Sicherheit in der Informationstechnik, 2011, S. 71 f.). Dabei ist dieser unabhängig von den physischen Eigenschaften des Speichermediums (Bundesamt für Sicherheit in der Informationstechnik, 2011, S. 71 f.). Daraus resultieren insbesondere bei Mehrnutzerbetrieb eine Vielzahl von Informationen, die abgelegt werden müssen (Bundesamt für Sicherheit in der Informationstechnik, 2011, S. 71 f.). Dazu gehören Details wie die Erstellungsdaten und Eigentümer von Dateien (Bundesamt für Sicherheit in der Informationstechnik, 2011, S. 71 f.).

Nach Bunting; Wie (2006, S. 19 f.) existieren folgende fünf Anforderungen an ein Dateisystem:

- Verwaltung der Dateinamen,
- Verwaltung des Dateianfangs,
- Verwaltung der Dateilänge mit den Metadaten wie bspw. die Dateirechte,
- Verwaltung der benutzten Speichereinheiten und
- Verwaltung der belegten sowie freien Cluster.

Das Dateisystem ist auf einem Datenträger wie z. B. USB-Stick abgelegt (Bundesamt für Sicherheit in der Informationstechnik, 2011, S. 71 f.). Diese Methode ist den Abschnitten der Datensammlung und der Untersuchung des Prozesses zuzuordnen (vgl. Tabelle 1).

2.3.3 Explizite Methoden der Einbruchserkennung (EME)

Diese Methode beschreibt Maßnahmen, welche automatisiert und routinemäßig in der Phase der strategischen Vorbereitung aktiviert werden und der Erkennung von Zwischenfällen dienen (Bundesamt für Sicherheit in der Informationstechnik, 2011, S. 76). Dazu gehören z.B. „Intrusion Detection Systeme“ (IDS)[5] oder „On-Access-Virenscanner“[6] (Bundesamt für Sicherheit in der Informationstechnik, 2011, S. 76).

2.3.4 IT-Anwendung (ITA)

Die Methode der IT-Anwendungen umfasst alle Anwendungen eines IT-Systems (Bundesamt für Sicherheit in der Informationstechnik, 2011, S. 77). Das können z.B. Tabellenkalkulationen, Datenbanksoftware oder Webbrowser sein (Bundesamt für Sicherheit in der Informationstechnik, 2011, S. 77).

2.3.5 Skalierung von Beweismitteln (SB)

In dieser Kategorie finden sich alle Methoden, die nur in konkreten Verdachtsfällen eines Zwischenfalls eingesetzt werden (Bundesamt für Sicherheit in der Informationstechnik, 2011, S. 78). Ein Beispiel wäre ein Mitschnitt des gesamten Netzwerkverkehrs, welcher ineffizient ist und deshalb in den meisten Fällen nicht vorgenommen wird (Bundesamt für Sicherheit in der Informationstechnik, 2011, S. 78). In bestimmten Verdachtsfällen kann es jedoch notwendig sein (Bundesamt für Sicherheit in der Informationstechnik, 2011, S. 78).

2.3.6 Datenbearbeitung und Auswertung (DBA)

Diese Methode fasst all jene Methoden zusammen, welche die forensische Untersuchung ermöglichen, d.h. Ausgangsdaten zu analysieren und Daten zu extrahieren sowie zu rekonstruieren (Bundesamt für Sicherheit in der Informationstechnik, 2011, S. 79 f.). Dazu zählen

[5] Intrusion Detection Systeme dienen dazu, unbefugte Aktivitäten sowie Angriffe in ein Computersystem oder -netzwerk zu erkennen und zu reagieren. Es findet eine Überwachung des Datenverkehrs, die Analyse von Ereignissen und Benutzerverhalten statt (Debar, Dacier, & Wespi, 1999).

[6] On-Access-Virenscanner beschreiben Antivirensoftware, die spezialisiert ist, Dateien, Programme und Aktivitäten in Echtzeit zu überwachen und zu analysieren (Greveler & Wellmeyer, 2011).

z.B. Tools, die Log-Dateien parsen[7] bzw. zusammenführen oder Dateien aus Rohdaten extrahieren. Solche Werkzeuge ermöglichen eine Darstellung von Sachverhalten aus forensischer Perspektive.

2.4 Mobile Forensik

Die mobile Forensik beschreibt ein Teilgebiet der Forensik, welches die Wissenschaft, die auf die Gewinnung und Bearbeitung von digitalen Beweisen von mobilen Geräten mittels Techniken der digitalen Forensik abzielt, bezeichnet (Moreb, 2022, S. 3). Aufgrund der wachsenden Anzahl von potenziellen Messenger-Nutzern bei Smartphones sowie der zunehmenden Nutzerzahlen unter tatsächlichen Nutzern (vgl. Abbildung 18, Abbildung 17, Abbildung 19) gewinnt diese Forensik-Teildisziplin stetig an Bedeutung. In Abbildung 5 sind die grundlegenden Schritte der Untersuchung von Mobiltelefonen dargestellt (Dogan; Akbal, 2008, S. 1242).

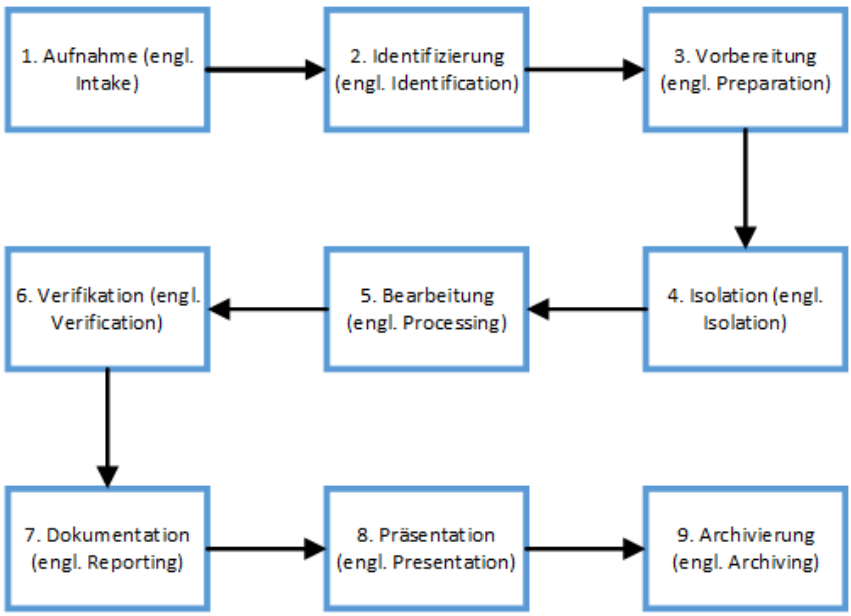

Abbildung 5: Prozess der Untersuchung von Mobiltelefonen, angelehnt an Dogan; Akbal, Analysis of mobile phones in digital forensics, 2017, S. 1242

[7] Das Parsen von Logdateien beschreibt den Prozess der Extraktion und der Analyse von Daten aus Protokolldateien, die durch Software, Betriebssystemen, Netzwerken oder anderen Systemen erzeugt werden (Restat, 2021, S. 6 f.).

Unabhängig von den Unterschieden der Mobiltelefone sind die in Abbildung 6 gezeigten Informationen zu extrahieren und zu untersuchen (Dogan; Akbal, Analysis of Mobile Phones in Digital Forensics, S. 1242).

Abbildung 6: Übersicht der fundamentalen Informationen der Untersuchung von Mobiltelefonen, angelehnt an Dogan; Akbal, Analysis of mobile phones in digital forensics, 2017, S. 1242

Dabei zeigen sich eine Vielzahl von Herausforderungen für Ermittler wie die unterschiedlichen Gerätetypen und Betriebssysteme, welche auf dem Markt existieren (Dogan; Akbal, 2008, S. 1242). Auf dem Markt sind verschiedene Marken, Smartphone- und Tabletmodelle mit unterschiedlicher Hardware, verschiedenen Speicherstrukturen und Betriebssystemen (Moreb, 2022). In den letzten Jahren stieg der Anteil und die Verbreitung von Android und „Internetwork Operation System“ (iOS) (vgl. Abbildung 21). Insbesondere iOS verfügt als „Closed Source“[8] über einige Sicherheitsmechanismen, die die Untersuchung erschweren (Spreitzenbarth, 2017, S. 14 ff.).

[8] In Bezug auf Software bedeutet der Begriff „Closed Source“, dass der Quellcode nicht öffentlich bereitgestellt wird (Donovan, 1994).

Die erste Stufe des Sicherheitsmodells stellt die „Secure Boot Chain"[9] dar. (Spreitzenbarth, 2017, S. 14 ff.). Dabei sind durch das Unternehmen Apple Inc. Signaturen implementiert, um während des Prozesses des Startens des Betriebssystems zu überprüfen und zu erkennen, ob Komponenten verändert wurden (Spreitzenbarth, 2017, S. 14 ff.). Der Mechanismus erschwert den Jailbreak[10] des Gerätes (Spreitzenbarth, 2017, S. 14 ff.).

Die zweite Stufe ist das „Dataprotection-Level" (Spreitzenbarth, 2017, S. 14 ff.). Dabei entwickelte das Unternehmen Apple Inc. die Schnittstelle „NSFileProtection", welche die Verschlüsselungen der gespeicherten Daten umfasst (Spreitzenbarth, 2017, S. 14 ff.). Folgende vier Stufen der Verschlüsselung wurden implementiert:

- „NSFileProtectionNone": Auf dieser Stufe sind die Daten ausschließlich verschlüsselt, wenn das Gerät ausgeschaltet ist (Spreitzenbarth, 2017, S. 14 ff.). Der Schlüssel ist als Variable auf dem Gerät gespeichert. Dadurch bietet diese Stufe praktisch keinen Schutz (Spreitzenbarth, 2017, S. 14 ff.).
- „NSFileProtetionCompleteUntilFirstUserAuthentication": Bei der seit iOS 7.0 als Standardwert gewählte Stufe setzt sich der Schlüssel aus Variablen des Gerätes und Passwortes des Nutzers zusammen und wird dadurch bei dem Ausschalten des Gerätes aus dem Speicher entfernt (Spreitzenbarth, 2017, S. 14 ff.). Diese Stufe kann mit der Festplattenverschlüsselung eines Computers gleichgesetzt werden (Spreitzenbarth, 2017, S. 14 ff.).
- „NSFileProtectionCompleteUnlessOpen": Auf dieser Stufe setzt sich der Schlüssel wie bei der vorherigen Stufe zusammen (Spreitzenbarth, 2017, S. 14 ff.). Jedoch wird dieser aus dem Speicher gelöscht, sobald dieser nicht mehr benötigt wird (Spreitzenbarth, 2017, S. 14 ff.).
- „NSFileProtectionComplete": Auf der höchsten Stufe wird der Schlüssel sofort aus dem Speicher gelöscht, wenn der Bildschirm gesperrt wird (Spreitzenbarth, 2017, S. 14 ff.).

[9] Die „Secure Boot Chain" ermöglicht den sicheren Bootvorgang durch den Schutz der untersten Ebenen der Software vor Manipulation. Dafür wurden durch das Unternehmen Apple Inc. Die Komponenten des Startvorgangs kryptografisch signiert und im Verlauf des Startvorgang einer Integritätsprüfung durchgeführt. Daraus folgt, dass zuerst die Vertrauenskette überprüft wird, bevor der Bootvorgang fortgesetzt wird (Apple Inc., 2023).

[10] Ein „Jailbreak" bezeichnet die Veränderung des Betriebssystems. Dadurch wird voller Zugriff auf das Dateisystem eines mobilen Gerätes mit Root-Rechten erlangt (Liu, Liu, Chang, & Wang, 2016).

Zudem existiert unter iOS die sogenannte „Keychain“, welche die Ablage von besonders schützenswerten Daten wie Passwörtern, Zertifikaten oder kryptografische Schlüsseln ermöglicht (Spreitzenbarth, 2017, S. 14 ff.).

Die Vermeidung von Veränderungen stellt einen essenziellen Grundsatz während der forensischen Untersuchung dar (Bundesamt für Sicherheit in der Informationstechnik, 2011, S. 26). Bei mobilen Geräten erweist es sich durch Veränderungen, welche ohne die Einwirkung der Ermittler verursacht werden, als besonders herausfordernd (Bundesamt für Sicherheit in der Informationstechnik, 2011, S. 26). Ein Beispiel dafür ist, dass im ausgeschalteten Zustand des Mobiltelefons akustische Benachrichtigungen ausgelöst werden, welche durch die Alarm-Funktion des Gerätes aktiviert werden (Bundesamt für Sicherheit in der Informationstechnik, 2011, S. 26). Folgende Hard- und Software-Tools werden häufig im Bereich der mobilen Forensik von den Forensikern benutzt:

- Cellebrite, (welches im Rahmen dieser Bachelorarbeit auch verwendet wurde)
- Paraben’s Device Seizure
- XRY
- EnCase Neutrino
- Oxygen Forensic
- MOBILedit
- Faraday
- Tarantula (Bundesamt für Sicherheit in der Informationstechnik, 2011, S. 26).

2.5 Reverse Engineering

Der traditionelle Software-Engineering-Prozess des Übergangs von Abstraktionen auf hoher Ebene und logischen, umsetzungsunabhängigen Entwürfen zur physischen Umsetzung eines Systems wird als „Forward Engineering“ bezeichnet (Nelson, 2005, S. 2). Dieser beginnt mit der Erarbeitung der Anforderungen und der Prozess des Reverse Engineerings endet in dieser Phase, wo hingegen für das Forward Engineering das Subjektsystem den Schlusspunkt darstellt (Nelson, 2005, S. 2). Dieser Prozess ist der Abbildung 7 dargestellt. Während des Prozesses des Reverse Engineerings wird ein Subjektsystem analysiert, um Komponenten des Systems sowie deren Wechselwirkungen zu identifizieren (Nelson, 2005, S. 2).

Hierbei beschreibt ein Subjektsystem ein einzelnes Programm, ein Codefragment, einen komplexen Satz, interagierende Programme, Arbeitssteuerungsanweisungen, Signalschnittstellen oder Datendateien (Chikofsky; Cross, 1990, S. 14).

Der Prozess zielt auf die Extraktion des Wissens ab (Eilam; Chikofsky, 2005, S. 3). Der Unterschied zwischen der herkömmlichen, wissenschaftlichen Forschung und dem Reverse Engineering liegt darin, dass beim Reverse Engineering die Artefakte manuell gesucht und erforscht werden (Eilam; Chikofsky, 2005, S. 3). Diese Methode dient der Erkenntnisgewinnung über fehlenden Informationen, wenn diese nicht verfügbar sind (Eilam; Chikofsky, 2005, S. 3).

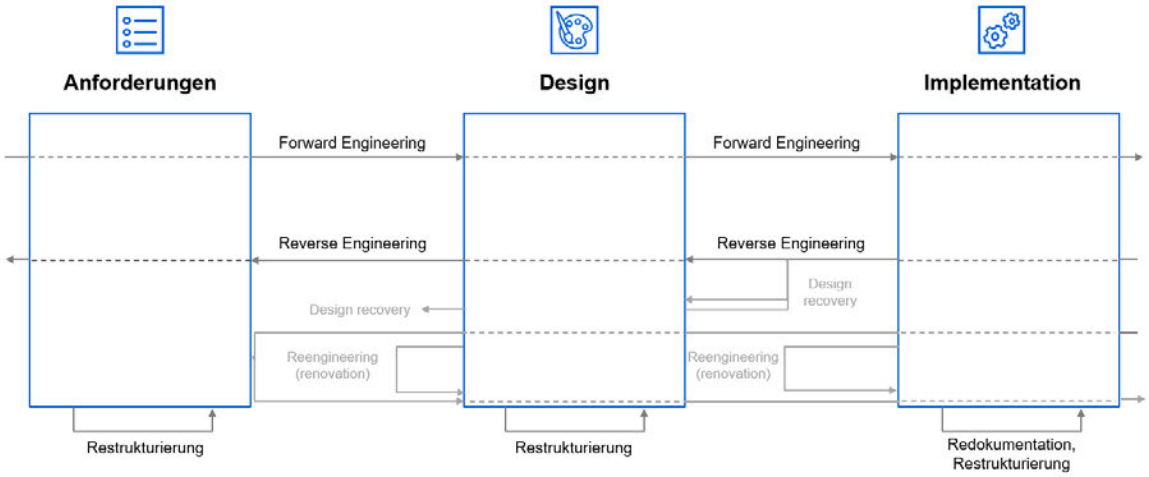

Abbildung 7: Überblick über die Begriffe des Forward Engineerings und Reverse Engineerings angelehnt an Chikofsky; Cross, 1990, S. 14

Das Reverse Engineering zielt vorrangig auf die allgemeine Verständlichkeit des Systems, als auch dessen Wartung sowie die Schaffung von Neuentwicklungen zu ermöglichen, ab (Eilam; Chikofsky, 2005, S. 16). Dieser Prozess umfasst sechs Hauptziele:

- Umgang mit Komplexität
- Erarbeitung von neuen Blickwinkeln
- Wiederherstellung von verlorenen Informationen
- Detektion von Nebeneffekten
- Synthetisierung von höheren Abstraktionen
- Erleichterung von Wiederverwendungen (Eilam; Chikofsky, 2005, S. 16)

Dabei werden keine Änderungen an Subsystemen vorgenommen oder neue Systeme geschaffen (Chikofsky; Cross, 1990, S. 15). Es steht nicht die Veränderung oder Replikation eines Systems im Fokus, sondern die Extraktion von Wissen über das Subjektsystem (Chikofsky; Cross, 1990, S. 15).

Es werden vier Spezialisierungen des Reverse Engineerings unterschieden (Nelson, 2005, S. 2). Die **Neudokumentation** zielt auf die Erstellung oder Überarbeitung der Systemdokumentation ab (Nelson, 2005, S. 2). Bei der **Design-Neuentdeckung** wird basierend auf dem Domänwissen und anderen externen Informationen ein Modell des Systems auf höheren Abstraktionsebenen erstellt (Nelson, 2005, S. 2). Die **Restrukturierung** dient der Transformation des Systems auf der gleichen Ebene der Abstraktion. Dabei bleiben Funktionalität und Semantik gleich (Nelson, 2005, S. 2). Die weitreichendste Spezialisierung ist das **Reengineering** (Nelson, 2005, S. 2). Dabei wird das Reverse Engineering zur Gewinnung von Verständnis über das Subjektsystem genutzt. Das Forward Engineering, um zu überprüfen, welche Funktionalitäten beibehalten, gelöscht oder hinzugefügt werden (Nelson, 2005, S. 2). “Reverse Engineering” dient dazu, ein Verständnis des Ausgangssystems zu erlangen, während Forward Engineering dazu verwendet wird, zu analysieren, welche Funktionen beibehalten, entfernt oder hinzugefügt werden sollen (Nelson, 2005, S. 2).

Bei dem Prozess ergeben sich speziell in fünf Bereichen verschiedene Herausforderungen:

- Eine Programmiersprache stellt eine Modellumgebung dar, welche ein Problem löst (Nelson, 2005, S. 3 f.). Dabei existieren Tools zur Gewinnung der Funktionsweise des Codes aus der Code-Perspektive, jedoch kaum solche, welche die Funktionsweise des Codes aus der Domänenperspektive erklären (Nelson, 2005, S. 3 f.).
- Durch die wenig intensive Ausbildung von Programmierern im Bereich der Zuordnung der detaillierten Implementierung zu den Zusammenfassungen kommen einfache, abstrakte Konzepte im Verlauf der Programmierung abhanden (Nelson, 2005, S. 3 f.).
- Aufgrund von Wartungen von Systemen weichen diese trotz ursprünglich detaillierter Dokumentation von der zugrundeliegenden Spezifikation ab (Nelson, 2005, S. 3 f.). Daraus ergibt sich die Notwendigkeit, dass im Laufe des Prozesses die aktuelle Implementierung sowie der ehemals dokumentierte Entwurf verglichen und die Dokumentation synchronisiert werden (Nelson, 2005, S. 3 f.).
- Im Prozess des Reverse Engineering müssen Einheiten aus erkennbaren Details von einer niederen auf eine hohe Ebene gebracht werden (Nelson, 2005, S. 3 f.).

Dies stellt eine Herausforderung dar, da Menschen üblicherweise in Form von assoziativen Dateneinheiten denken (Nelson, 2005, S. 3 f.).

- Gemeinhin wird die Codeanalyse in Form der Bottom-Up-Strategie durchgeführt (Nelson, 2005, S. 3 f.). Das bedeutet, dass von der unteren Ebene auf die höheren Ebenen überführt wird. Im Reverse Engineering-Prozess sollten Experten in der Lage sein, eine Abbildung von höheren zu niedrigeren Ebenen vorzunehmen (Nelson, 2005, S. 3 f.).
- Dafür müssen Codefragmente extrahiert und auf Implementierungen auf niedriger Ebene abgebildet werden (Nelson, 2005, S. 3 f.). Zusätzlich wird dies durch Verschleierung wie „Interleaving“[11] erschwert (Nelson, 2005, S. 3 f.).

2.6 Instant Messenger-Dienste (IM-Dienst)

2.6.1 Begriffsdefinition und Abgrenzung

IM-Dienste ermöglichen den Austausch von Nachrichten in Echtzeit mittels eigenständiger Anwendungen (Scarpati, 2020). Dabei findet die Kommunikation oftmals zwischen Nutzern statt, was diese von Chaträumen unterscheidet (Scarpati, 2020). Der Unterschied zur Kommunikation via E-Mail liegt darin, dass Nachrichten in Echtzeit übertragen werden, was bei E-Mails nicht der Fall ist (Mannan; Oorschot, 2004, S. 1).

Vier Bereiche grundlegender Funktionen sind historisch charakteristisch für IM Applikationen (Mannan; Oorschot, 2004, S. 3). Die erste Funktion ist die **Kommunikation zwischen mehreren Benutzern**. Die Nutzer können mittels des Dienstes Nachrichten versenden und empfangen (Mannan; Oorschot, 2004, S. 3). Es ist auch ein Versenden möglich, wenn einer der Teilnehmer nicht online ist (Mannan; Oorschot, 2004, S. 3). Zudem erlauben IM Dienste häufig das **Kontaktlistenmanagement** (Mannan; Oorschot, 2004, S. 3). Diese ermöglicht das Erstellen von Listen mit anderen Nutzern und die Organisation in Gruppen (Mannan; Oorschot, 2004, S. 3). Zusätzlich wird die Möglichkeit geboten, andere Nutzer zu blockieren (Mannan; Oorschot, 2004, S. 3). Das **Management der Verfügbarkeit der Nutzer** ist ein

[11] „Interleaving“ bezeichnet Zusammenlegungen von logisch getrennten Aufgaben innerhalb derselben Abfolge (Nelson, 2005, S. 3 f.).

weiterer Bereich (Mannan; Oorschot, 2004, S. 3). Die meisten Dienste zeigen den Nutzern außerdem den Status der Anderen an (Mannan; Oorschot, 2004, S. 3). Zudem können Nutzer eine **Benutzerdatenbanksuche** betreiben (Mannan; Oorschot, 2004, S. 3). Auf Grundlage von Interessen, von Namen oder E-Mail-Adressen können andere Benutzer gesucht werden (Mannan; Oorschot, 2004, S. 3).

Der Austausch von Textnachrichten stellte lange die Hauptfunktion der Anwendungen dar (Scarpati, 2020). Mittlerweile ermöglichen die meisten Anwendungen eine Vielzahl von Funktionen wie Video- und Sprachanrufe oder das Versenden von Bildern und Videos. In den Verbreitetsten wird der vierte Bereich der Benutzerdatenbanksuche der Basisfunktionalitäten nicht mehr angeboten. Die meisten IM-Systeme sind Client Server-basiert, wobei zur Authentifizierung zwischen Client und Server ein Austausch von Passwort-Hashes durchgeführt wird (Mannan; Oorschot, 2004). Ebenso werden die Nachrichten, die zwischen den Nutzern ausgetauscht werden, über den Server weitergeleitet. Audio- oder Videoanruf-Funktionalitäten werden in Form von Peer-to-Peer-Kommunikation[12] umgesetzt (Mannan; Oorschot, 2004). In Abbildung 8 ist die Kommunikation zwischen ein oder mehreren Servern mit den Clients dargestellt. Dabei erfolgt diese hauptsächlich über das Transmission Control Protocol (TCP), welches standardmäßig eingesetzt wird und den Aufbau und die Aufrechterhaltung einer Netzwerkkonversation charakterisiert, bei welcher Daten mittels Anwendungen ausgetauscht werden (Mannan; Oorschot, 2004); (Lutkevich, 2021).

[12] Peer-to-Peer Kommunikation beschreibt ein Netzwerkkommunikationsmodell, das keine zentralen Server oder Autorität zur Datenübertragung nutzt. Endgeräte kommunizieren direkt miteinander (Hasselbring; Bischofs; Warns, 2008, S. 433 f.).

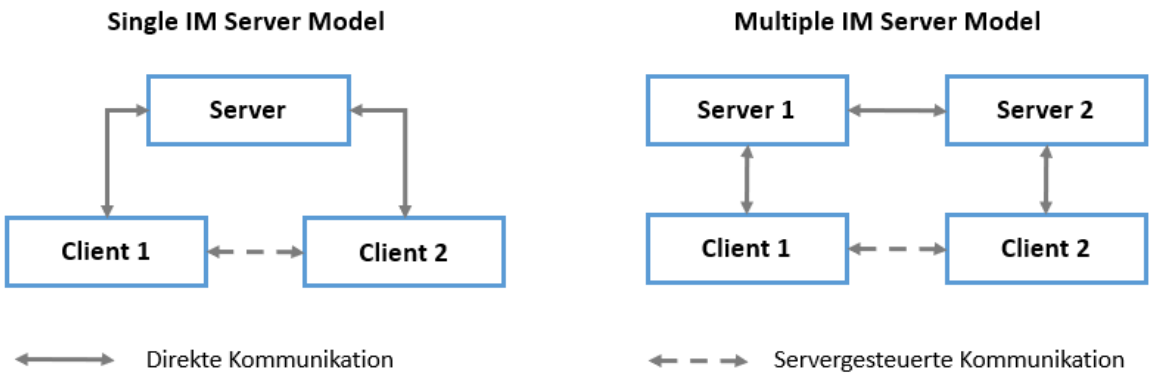

Abbildung 8: IM Communications Model, angelehnt an Mannan; Oorschot, 2004, S. 3

2.6.2 Threema

2012 wurde die erste Version der IM-Applikation „Threema“ in der Schweiz entwickelt (Threema GmbH, 2023). Zu diesem Zeitpunkt hieß diese „End-to-End Encrypted Messaging Application“ (EEEMA) (Threema GmbH, 2023). In den folgenden Jahren wurden die drei aufeinanderfolgenden E‘s durch das englische Wort „Three“, welches die drei E’s symbolisierte, ersetzt (Threema GmbH, 2023). Am 12. Dezember 2012 konnte diese Version im App-Store von Apple heruntergeladen werden (Threema GmbH, 2023). Knapp 1,5 Jahre später wurde das Unternehmen mit Sitz in Pfäffikon in der Schweiz gegründet. Seitdem verzeichnet die Anwendung 11 Millionen Nutzer (Threema GmbH, 2023).

Der Hersteller des IM-Dienstes wirbt damit, dass „Threema“ für Sicherheit, Vertraulichkeit und Metadaten-Sparsamkeit steht (Threema GmbH, 2023). Die Sicherheit und der Schutz der Privatsphäre werden durch die Sparsamkeit hinsichtlich der Metadaten erreicht. Durch Vermeidung der Erzeugung von Daten ist der spätere Missbrauch laut den Entwicklern des Unternehmens ausgeschlossen (Threema GmbH, 2023). Die Server fungieren als Relaisstation (Threema GmbH, 2023). Das bedeutet, dass die Nachrichten nach erfolgter Zustellung automatisiert gelöscht werden. Zusätzlich ist der Quellcode öffentlich zugänglich (Threema GmbH, 2023). Externe Experten werden regelmäßig durch die Threema GmbH beauftragt, die Applikation zu überprüfen (Threema GmbH, 2023).

Die gesamte Kommunikation wird Ende-zu-Ende-verschlüsselt, wobei sie auf der Verschlüsselungstechnologie NaCL basiert (Threema GmbH, 2023). Auch die auf dem Mobilgerät gespeicherten Daten, Chats und Medien sind verschlüsselt (Threema GmbH, 2023).

Die Daten werden nicht auf den Servern gespeichert (Threema GmbH, 2023). Durch diese dezentrale Architektur unterscheidet sich der IM zu anderen Messenger-Diensten (Threema GmbH, 2023). Die bereitgestellten Funktionalitäten werden in den folgenden Kapiteln weiter erläutert (Threema GmbH, 2023).

3 Verwandte Arbeiten

Die forensische Analyse von IM-Anwendungen auf mobilen Endgeräten wurden in verschiedenen Werken der Literatur thematisiert, wobei Android und iOS im Fokus stehen (Skulkin; Tindall; Tamma, 2018); (Tamma; Skulkin; Mahalik; Bommisetty; Bommisetty, 2020). Dies resultiert aus der dominanten Verbreitung der beiden Betriebssysteme (vgl. Abbildung 21). In dieser Untersuchung standen insbesondere IM-Dienste unter Android im Fokus. Dabei wurden neben „WeChat“ und „WhatsApp“ analysiert, sondern auch „ChatSecure“, „Threema“ und „Wickr“ (Wu; Zhang; Wang; Xiong; Du, 2016); (Anglano; Canonico; Guazzone, 2016); (Anglano, 2014); (Son; Kim; Oh; Kim, 2022); (Mehtre; Mehrotra, 2013); (Thakur N. , 2013); (Zhang; Yu; Ji, 2016).

Die 20 beliebtesten IM-Anwendungen wurden bereits unter Android analysiert (Walnycky; Baggili; Marrington; Moore; Breitinger, 2015). Zusätzlich wurde die Analyse weiterer IM-Anwendungen wie „Skype“ durchgeführt, wobei der Fokus auf der Identifizierung der Verschlüsselungsalgorithmen lag (Azfar; Raymond Choo; Lui, 2016).

Dabei wurde der Messenger „Threema“ betrachtet, wobei keine forensische Untersuchung unter iOS durchgeführt wurde (Son; Kim; Oh; Kim, 2022). Zwischen iOS und Android bestehen Unterschiede sowohl in der Verzeichnisstruktur als auch in der Art der Datenablage. Unter Android wurde „Threema“ in der Version v4.55 betrachtet. Alle erzeugten Dateien wie Datenbanken, Multimediadateien, Protokolldateien und Konfigurationsdateien wurden gesammelt. Während der Untersuchung wurden Nachrichten versendet und empfangen oder gelesen und weitere Aktionen durch den Nutzer ausgeführt. Abhängig davon wurden Veränderungen in den Dateien und Einstellungen beobachtet. Die Untersuchung ergab, dass zwei Datenbanken erzeugt werden, welche verschlüsselt vorliegen. Zudem existiert eine weitere Datenbank, die nicht verschlüsselt ist. In ihr werden verschiedene „Nonces“[13] abgelegt. Alle Daten im Verzeichnis INTERNAL/files/ sind binär abgelegt, außer die „device_id“. Die multimedialen Daten liegen verschlüsselt in einer versteckten Datei im Verzeichnis EXTERNAL/Android/data. Des Weiteren wird die Verschlüsselung der IM-Anwendung unter Android beschrieben (Son; Kim; Oh; Kim, 2022). In der vorliegenden Arbeit wird dieser IM unter iOS betrachtet, da hierzu noch keine veröffentlichten Forschungen

[13] Der Begriff „Nonce“ beschreibt im Kontext der Kryptografie eine zufällig generierte Zahl oder Zeichenfolge, welche nur einmalig verwendet werden (Needham; Schroeder, 1978). So kann gewährleistet werden, dass Nachrichten oder ein Datenpacket nicht wiederverwendet oder manipuliert werden.

vorliegen. Dazu wurden Suchmaschinen, welcher der Literaturrecherche von wissenschaftlichen Dokumenten diene, verwendet, um Begriffe wie „Forensische Untersuchung von IM-Diensten“, „Forensische Untersuchung von IM“, „Forensische Analyse von IM“ oder „Forensische Analyse von IM-Diensten“ als Suchbegriffe eingesetzt.

IM-Anwendungen wie „AIM“, „Yahoo! Messenger“ und „Google Talk“ sowie weitere Dienste unter iOS wurden bereits forensisch analysiert (Husain; Sridhar, 2010); (Tso; Wang; Huang; Wang, 2012). Auch der IM-Dienst „Kik“ wurde bereits unter iOS analysiert (Ovens; Morison, 2016). Hierbei unterscheiden sich die IM-Applikationen von der in dieser Arbeit untersuchten. Das Betriebssystem ist gleich. Die Untersuchung der verbreiteten Dienste „Telegram“ und „Whatsapp“ unter iOS wurde bereits erarbeitet. Zusätzlich wurden in einer Studie mehr als 30 Anwendungen unter iOS untersucht (Salamh; Mirza; Hutchinson; Yoon; Karabiyik, 2021). Dazu gehören z.B. „Snapchat“, „WhatsApp“, „Telegram“ und der „Facebook Messenger“ (Salamh; Mirza; Hutchinson; Yoon; Karabiyik, 2021). Es wurden die alten Versionen der Anwendungen aus vorherigen Studien miteinander verglichen. Alle verwandten Arbeiten verwendeten virtualisierte „Smartphones“ statt der physischen Geräte, um die Allgemeingültigkeit und Reproduzierbarkeit zu gewährleisten (Anglano; Canonico; Guazzone, 2017). Es laufen zwei parallele Prozesse ab. Auf der einen Seite werden die Funktionen analysiert, anschließend das Design des Experimentes beschrieben. Diese Experimente werden, wenn nötig, wiederholt, um die Artefakte und Beziehungen zu dokumentieren. Auf der anderen Seite wird die Applikation installiert, um die gewonnenen Informationen aus den Experimenten mit dem Zustand nach der Installation zu vergleichen. Direkt nach dieser wird der Status mit dem vor der Installation abgeglichen. So kann erforscht werden, welche Verzeichnisse und Dateien erzeugt werden. Zusätzlich können unterstützend durch die Analyse des Sourcecodes Informationen über erzeugte Daten gewonnen werden (Anglano; Canonico; Guazzone, 2017).

Die forensische Untersuchung der IM-Applikation „Threema“ wurde bisher nicht unter der Plattform iOS in wissenschaftlichen Arbeiten behandelt. Die Bachelorarbeit befasst sich mit dieser Untersuchung. Dabei fokussiert sie sich auf Informationen über Standorte, den Austausch von Textnachrichten und multimedialen Daten und Artefakte über die Kommunikationspartner. Andere Arbeiten betrachten die Sicherheit des Designs von „Threema“ (Paterson; Scarlata; Troung, 2023).

4 Methodik: Untersuchung der Daten eines IM-Dienstes

Im folgenden Kapitel wird die Vorgehensweise, welche auf (Wiedeking, 2019) basiert, zur Analyse eines Instant Messengers erläutert. Basierend auf dieser wurde der Messenger unter iOS untersucht. In Abbildung 9 sind die einzelnen Phasen dargestellt. Die Untersuchung beginnt mit der Vorbereitungsphase, worauf die Auswertungs- und Analysephase folgt. Am Ende wird die Aufbereitungsphase durchgeführt. Im folgenden Kapitel wird jede dieser Phasen konkreter beschrieben.

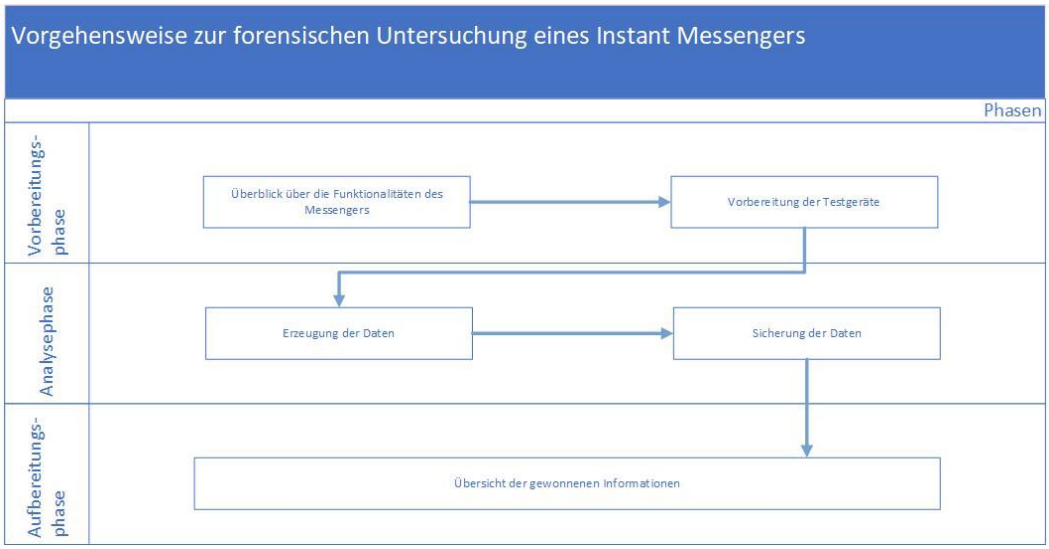

Abbildung 9: Übersicht der Vorgehensweise einer forensischen Untersuchung eines IMs

4.1 Vorbereitungsphase

In der ersten Phase der Untersuchung werden zuerst die Funktionalitäten des Messengers recherchiert. Dabei können diese auch durch die Installation des Messengers getestet werden. In dem Schritt sollte basierend auf den Funktionen dokumentiert werden, welche Daten möglicherweise erzeugt werden und welche von ihnen forensisch relevant sein könnten. In den folgenden Schritten sollte auf diesen ein besonderer Fokus liegen. Als nächstes werden die Testgeräte zur Untersuchung vorbereitet. Dazu sind mindestens zwei Testgeräte nötig. Jedoch ist es zu empfehlen, auch ein drittes zu verwenden, um Funktionalitäten wie Verteilerlisten oder Gruppennachrichten nutzen zu können. Um zu

evaluieren, wie viele Testgeräte benötigt oder welche Art von Daten erzeugt werden sollen, müssen die Funktionalitäten der Applikation festgelegt werden, welche für die Untersuchung relevant sein könnten. Hierbei müssen diese auf Werkszustand zurückgesetzt werden. Dies ist nötig, um zu verhindern, dass ungewollte Daten von vorheriger Nutzung auf den Testgeräten abgelegt sind, welche die Untersuchung verfälschen könnten. Zudem ist zu beachten, dass „Automatische Updates“ im App-Store des Mobiltelefons deaktiviert sind. Die Notwendigkeit dessen resultiert daraus, dass durch das Update der Anwendung z. B. neue Funktionen implementiert, werden könnten. Das hat Einfluss auf die erzeugten Daten und wo diese abgelegt werden.

4.2 Analysephase

In der Phase werden gezielt Daten erzeugt. Abhängig von den Ergebnissen der vorherigen Phasen werden z. B. Nachrichten versendet oder Sprachanrufe getätigt. Es gilt auch in dieser Phase jede Aktivität zu dokumentieren, um im Weiteren gezielt nach den erzeugten Daten suchen zu können. Verbreitet ist auch im Reverse Engineering von IMs zuerst die Sicherung der Daten direkt nach der Installation und die nächste Sicherung nach der Erzeugung der Daten durchzuführen. Im nächsten Schritt kann der Messenger installiert und die Daten erzeugt werden. Zur Datenerzeugung muss ein Nutzeraccount erstellt werden und anschließend abhängig von den Funktionalitäten der App z. B. Nachrichten versendet werden. Zur gezielten Untersuchung der Daten ist es notwendig detailliert zu dokumentieren, was genau getan wurde. Dadurch kann verglichen werden, welche Daten durch das Experiment erzeugt worden sind.

4.3 Aufbereitungsphase

Die Aufbereitung der exportierten Daten wurde mittels *Cellebrite* vorgenommen, welches ein bekanntes Tool zur Untersuchung von mobilen Endgeräten ist. Das Werkzeug ermöglicht die Suche nach den Daten, welche durch „Threema“ abgelegt werden. Dabei bereitet das Tool eine Vielzahl von Informationen auf. Zu den Daten sind neben dem Inhalt auch der Ablageort sowie die Größe des Eintrages angegeben. Dadurch ist es möglich, in den gesicherten Daten der Anwendung in den angegebenen Datenbanken nach den entsprechenden Inhalten zu suchen und diese zu dokumentieren. Das Tool bietet die Möglichkeit, die Daten in verschiedenen Formaten wie Excel-Datei oder PDF-Datei zu exportieren. Weitere Formate wie HTML, Word und XML sind ebenso möglich zu exportieren, wodurch diese

auf jedem Computer mittels Standardprogrammen zu öffnen sind. In der folgenden Untersuchung von „Threema“ wurde diese in Form von Excel-Dateien exportiert und untersucht.

5 Reverse Engineering der Messenger-App „Threema” unter iOS

Im folgenden Kapitel wird der Messenger-Dienst „Threema“ untersucht. Das umfasst die Analyse und Auswertung der Ergebnisse. Hierbei wird die Methodik, wie in Kapitel 4 vorgestellt wurden, angewendet.

5.1 Vorbereitungsphase

5.1.1 Design des Experiments

Zur Untersuchung der Messenger-App „Threema“ unter dem Betriebssystem iOS wurden Daten erzeugt. Dafür wurden die Versionen 3.6.13 und 4.6 Build 3000705 des Instant-Messengers aus den App-Stores heruntergeladen und Nachrichten zwischen den mobilen Endgeräten versendet, welche in Tabelle 2 näher erläutert werden. Dabei wurden sowohl Bild-, Video-, Audio- als auch Textnachrichten zwischen den Geräten versendet. Zudem wurden Standortinformationen ausgetauscht. Die untersuchten Daten wurden nicht im Rahmen der Bachelorarbeit erzeugt, sondern bereitgestellt. Im Anhang sind die dazugehörigen Protokolle zu finden. Dabei wurden die Daten von Testgerät 1 mittels des Tools *Cellebrite* UFED Touch gesichert und danach die Extraktion der Daten über den *Cellebrite* Reader durchgeführt. Es werden ausschließlich die Artefakte dieses Gerätes untersucht. Dabei wurde neben der UFED-Datei auch die erzeugten Verzeichnisse, welche durch „Threema“ erzeugt wurden, bereitgestellt. Diese Daten wurden bereits entschlüsselt übergeben. Deshalb war kein Entschlüsselungsprozess notwendig.

Tabelle 2: Testgeräte

Testgeräte	Testgerät 1: iPhone 7	Testgerät 2: Samsung S 8	Testgerät 3: iPhone SE
Betriebssystem-Version	14.7.1	10	15.0
Model Name	iPhone 7	Samsung S8	iPhone SE
Version des IM- Dienst	4.6.13 (2663)	4.6 Build 3000705	4.6.13 (2663)

5.1.2 Analyse der Funktionen der Applikationen

Der Messenger-Dienst „Threema“ ermöglicht den Nutzern eine Vielzahl von Funktionen, welche über den Austausch von Textnachrichten hinausgeht. Neben dem Versenden von Text- und Sprachnachrichten ist es möglich, Dateien, Medien sowie Standorte mit anderen Nutzern der Applikation zu teilen. Dabei kann dies an einzelne Nutzer oder Gruppen aber auch Verteilerlisten erfolgen. Zudem können Video- als auch Sprachnachrichten von mehreren Nutzern genutzt werden.

Von besonderem Interesse der forensischen Untersuchung sind folgende Funktionalitäten und Daten.

Threema-ID

Der Austausch von Nachrichten mittels „Threema“ ist ohne Angabe der Handynummer möglich (Threema GmbH, 2023). Das schafft zusätzliche Anonymität für die Nutzer (Threema GmbH, 2023). Diese Funktionalität kann besonders für Kriminelle nützlich sein, da sie besonderes Interesse an erschwerter Identifikation ihrer Person haben. Der IM ermöglicht dies durch die Zuweisung einer zufällig erzeugten achtstelligen ID, wobei sie aus Zahlen und Buchstaben besteht (Threema GmbH, 2023).

Austausch von Nachrichten

„Threema“ bieten dem Nutzer die Möglichkeit, mittels Chats, Kanälen oder Gruppen mit einer oder mehreren Personen zu kommunizieren (Threema GmbH, 2023). Es können Text- und Sprachnachrichten, Standorte, Umfragen, Bild- und Videoformate oder andere Dokumente versendet werden (Threema GmbH, 2023). Durch Rekonstruktion der Chronologie und der Inhalte können Ermittler feststellen, welche Nutzer über welche Sachverhalte zu welchem Zeitpunkt kommuniziert haben. Dadurch können die „W-Fragen“ beantwortet werden und Informationen über den Fall gewonnen werden. Dabei kann neben dem Inhalt, den Gesprächspartnern und dem Zeitpunkt auch die Art der Kommunikation relevant sein. Der IM bietet den Nutzern die Möglichkeit von privaten Chats (Threema GmbH, 2023). Sie sind durch zusätzliche Mechanismen wie einem festgelegten Code oder der Face-ID geschützt (Threema GmbH, 2023). Diese Art der Chats kann außerdem ausgeblendet werden (Threema GmbH, 2023). Die Vorgehensweise könnte darauf hindeuten, dass die Nutzer beabsichtigten, die Kommunikation zu verbergen. Insbesondere Kriminelle könnten daran Interesse haben.

Video- und Sprachanrufe

Von besonderem Interesse der forensischen Untersuchung sind die zeitliche Abfolge, Dauer sowie Gesprächspartner der Ende-zu-Ende-verschlüsselten Anrufe, da dies einen Mehrwert zur Rekonstruktion des Tatherganges bietet. So ist es z. B. möglich festzustellen, wann potenzielle Tatverdächtige miteinander gesprochen haben.

5.2 Analyse- und Aufbereitungsphase

Zunächst wurde ein Export mittels des Tools *Cellebrite* erstellt. Wie in Abbildung 10 zu sehen ist, wurde über das Feld *„Analysierte Daten“* der Suchbegriff „threema“ eingegeben. Das Tool liefert die Chatverläufe, Anhänge und Informationen zu Kontakten. Dabei wird ebenso angegeben, wo sich diese befinden (vgl. Tabelle 3).

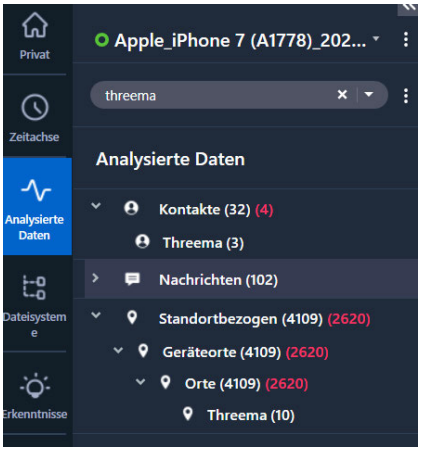

Abbildung 10: Suchergebnisse des Suchbegriffes „threema“ mittels Cellebrite

Die gelieferten Daten dienen als Grundlage für die weitere Untersuchung der Rohdaten. Es wurden jeweils zu den Daten der genaue Ablageort als auch die Größe des Eintrages extrahiert. Um die Untersuchungen ohne das Tool *Cellebrite* zu ermöglichen und fehlerhafte Extraktionen zu umgehen, wurden auch die Rohdaten untersucht. Aus den Untersuchungen der Aufbereitung mittels *Cellebrite* ging hervor, dass viele forensisch relevante Daten in der SQL-Datenbank abgelegt wurden. Diese wurde mittels des SQL-Viewers betrachtet (https://sqliteviewer.app/). Bei der Analyse lag ein Schwerpunkt auf Tabellen, in denen Chatverläufe, Orte und andere Dateien sowie Kontakte abgelegt wurden. Die Struktur der Datenbank ist in Abbildung 11 dargestellt. Die Datenbank besteht aus 20 Tabellen. Mittels *Cellebrite* wurden die folgenden Tabellen analysiert: *ZCONTACT*, *ZMESSAGE* und *ZBALLOT*.

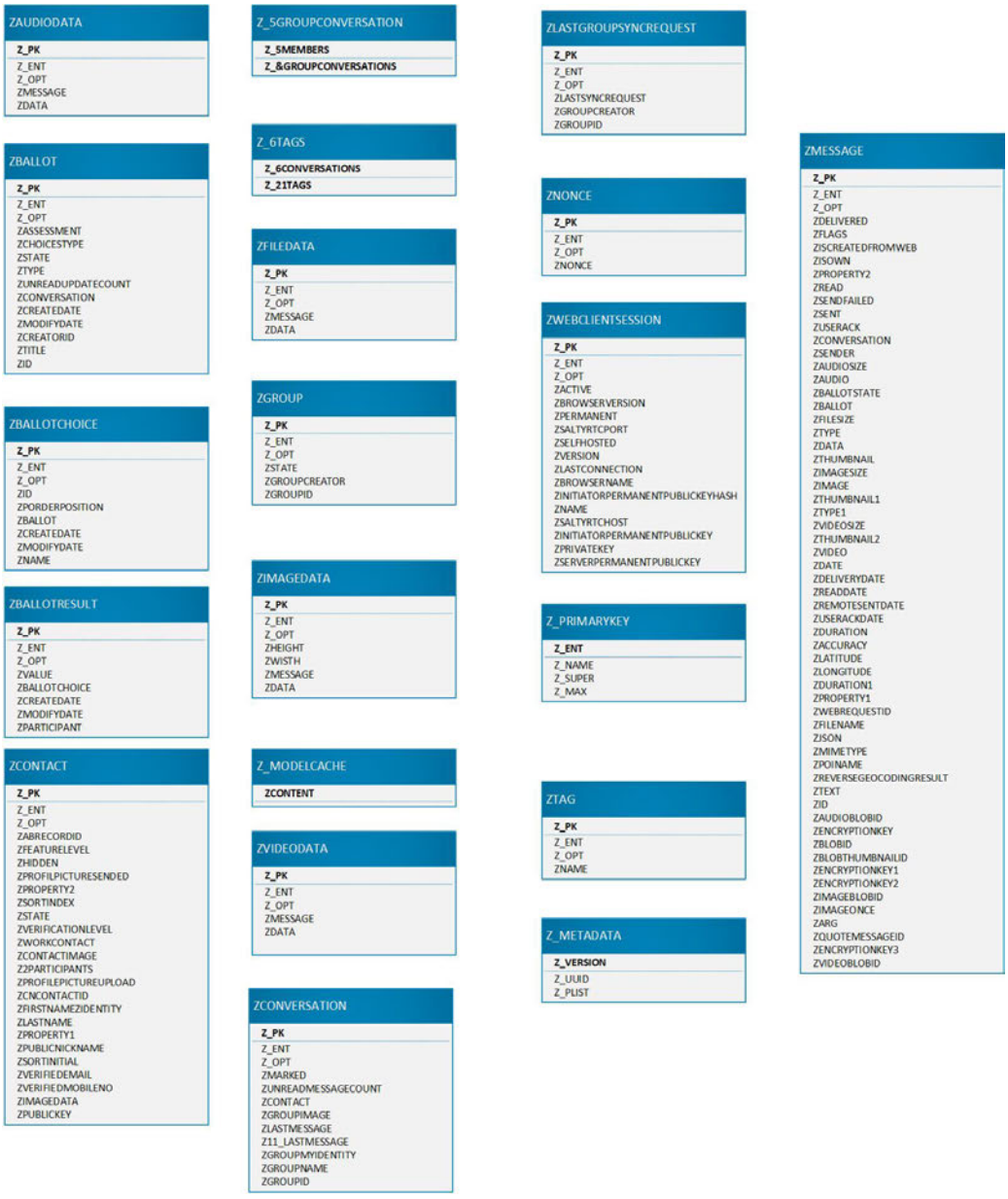

Abbildung 11: Struktur der SQL-Datenbank

5.2.1 Analyse und Auswertung der Chatverläufe und angehängter Dateien

Aus den exportierten Daten geht hervor, dass Chatverläufe und die zugehörigen Daten vorwiegend in den Datenbanken *ThreemaData.sqlite* und *Threema.sqlite-wal* abgelegt sind. Ebenso werden die Daten hinsichtlich der Kontakte in der *ThreemaData.sqlite-wal* Datenbank abgelegt. Somit finden sich die forensisch relevanten Informationen in diesen beiden

SQLite-Datenbanken. In Abbildung 12 ist ein Überblick über alle Verzeichnisse, welche den Daten des Messenger-Dienstes zuzuordnen sind, dargestellt.

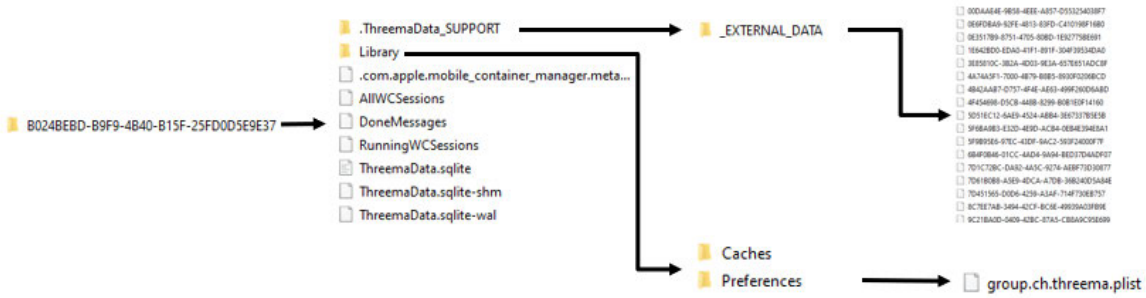

Abbildung 12: Überblick über die Verzeichnisstruktur

In Tabelle 3 ist ein Auszug des Exports aus *Cellebrite*. ihm ist zu entnehmen, dass folgende Einträge hinterlegt sind:

#

Diese Spalte dient ausschließlich der Nummerung der Einträge. In Tabelle 3 ist der erste Eintrag zu finden.

Typ

Der Typ kennzeichnet die Art der Herkunft des Eintrags. Im Fall „Threema“ ist dies der Begriff des Instant Messengers.

Richtung

Die Richtung charakterisiert, ob die Nachricht von dem Nutzer versendet wurde oder ob dieser die Nachricht empfangen hat. Dabei kann dieser Wert „*Eingehend“* oder „*Ausgehend“* sein.

Anhänge

Der Eintrag „Anhänge“ gibt die Anzahl der angehängten Dateien der jeweiligen Nachrichten an. In den erzeugten Daten wurde bei diesem *1* oder *2* hinterlegt, wobei bei Nachrichten, welche keine weitere Datei enthalten, kein Wert abgelegt wird.

Orte

Im Falle, dass ein Standort versendet wurde, nimmt diese Spalte den Wert *Ja* an.

Datum

In dieser Spalte ist das Datum, an welchem die Nachricht versendet wurde, hinterlegt.

Zeit

Das Feld beinhaltet den genauen Zeitstempel, welcher aus dem Datum und der Angabe der Uhrzeit besteht.

Teilnehmer

In dieser Spalte wird der Absender und Empfänger hinterlegt. Es wird sowohl die Threema-ID als auch, wenn zusätzlich durch den Nutzer der Kontakt abgespeichert ist, der entsprechende Name abgelegt. Sollte der Kontakt nicht eingespeichert sein, wird die Threema-ID zweifach hinterlegt.

Beschreibung

Hier findet sich der Inhalt der versendeten oder empfangenen Nachricht.

Quelle

Gibt die Applikation an, durch welche die Daten erzeugt werden.

Anhang #1 und Anhang #2

Diese Einträge enthalten die Namen von versendeten Dateien.

Anhang #3

Dieser Eintrag beinhaltet den Breitengrad, wenn ein Standort versendet wird.

Längengrad

Dieser Eintrag umfasst den Längengrad bei dem Versenden von Standorten.

Adresse

Hierzu sind in den bereitgestellten Daten keine Einträge vorhanden, weshalb diese Spalte nicht weiter ausgewertet werden kann. Im Falle des Versendens eines Standortes kann es ausgeschlossen werden, dass dieses Feld verwendet wird.

Gelöschte

In dieser Spalte wird bei dem Löschen von Nachrichten der Wert *Ja* abgelegt.

Tag-Hinweis

Hierzu sind in den bereitgestellten Daten keine Einträge vorhanden. Deshalb kann die Spalte nicht weiter ausgewertet werden.

Quelldatendatei-Informationen

Diesem Eintrag ist zu entnehmen, wo die Daten abgelegt sind. Hierbei wird der genau Ablageort beschrieben sowie die Größe dessen. Alle Einträge, welche versendete oder empfangene Nachrichten enthalten, sind in der *ThreemaData.sqlite* abgelegt und umfassen eine Größe von 4247552 Bytes.

Tabelle 3: Auszug aus exportierter Tabelle aus Cellebrite

#	1
Typ	Instant Messages
Richtung	Eingehend
Anhänge	
Orte	

Datum	09.11.2021 [Zeitstempel]
Zeit	09.11.2021 12:39:40(UTC+1) [Zeitstempel]
Teilnehmer	**Von:** From: 2S65VP2B Schrödi ;) **An:** To: XNYZKFYJ XNYZKFYJ **An:** To: XNYZKFYJ XNYZKFYJ
Beschreibung	Hallo
Quelle	Threema
Anhang #1	
Anhang #2	
Anhang #3	
Längengrad	
Adresse	
Gelöschte	
Tag-Hinweis	
Quelldatei-Informationen	Apple_iPhone 7 (A1778).zip/root/private/var/mobile/Containers/Shared/AppGroup/B024BEBD-B9F9-4B40-B15F-25FD0D5E9E37/ThreemaData.sqlite : 0x5E933 (Tabelle:

	ZMESSAGE, ZBALLOT, Größe: 4247552 Bytes) Apple_iPhone 7 (A1778).zip/root/private/var/mobile/Containers/Shared/AppGroup/B024BEBD-B9F9-4B40-B15F-25FD0D5E9E37/ThreemaData.sqlite-wal : 0x2F8550 (Größe: 3221872 Bytes)

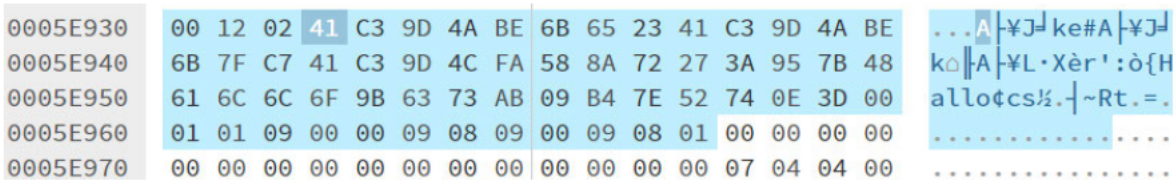

Abbildung 13: Eintrag (Hex-Dump) einer Textnachricht

In Abbildung 13 ist der Eintrag aus der Datenbank zu dem in Tabelle 3 dargestellten Beispiel abgebildet. Er konnte auf Grundlage der Aufbereitung durch *Cellebrite* entnommen werden, da dort der genaue Ablageort, in dem Beispiel 0x5E933, angegeben wurde. Der Eintrag ist 4.247.552 Bytes groß.

Der IM-Dienst ermöglicht neben dem Versenden von Textnachrichten, auch Dateien angehängt werden. Die durch den Cellebrite Reader aufbereiteten Daten in Tabelle 4 dargestellt. Der äquivalente Bereich der Rohdaten ist in Abbildung 14 dokumentiert.

Tabelle 4: Auszug aus exportierter Tabelle aus Cellebrite (Nachricht mit Anhang)

#	102
Von	XNYZKFYJ XNYZKFYJ
An	**Teilnehmer:** 2S65VP2B Schrödi ;), XNYZKFYJ XNYZKFYJ (owner), CEWRPNRP Nele
Richtung	Ausgehend
Betreff	

Status	Gesendet
Nachrichtentyp	09.11.2021
Zeitstempel-Datum	09.11.2021 14:18:04(UTC+1)
Gelesen-Datum	09.11.2021
Gelesen-Zeit	09.11.2021 14:25:28(UTC+1)
Quelldatei-Informationen	Apple_iPhone 7 (A1778).zip/root/private/var/mobile/Containers/Shared/AppGroup/B024BEBD-B9F9-4B40-B15F-25FD0D5E9E37/ThreemaData.sqlite : 0x10E5B6 (Tabelle: ZMESSAGE, ZBALLOT, Größe: 4247552 Bytes)

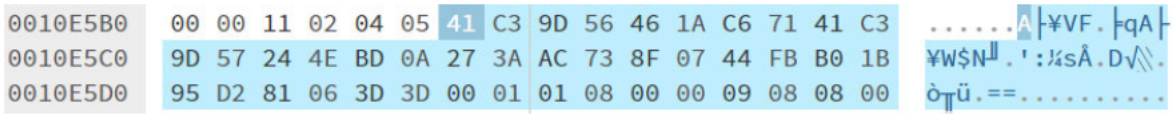

Abbildung 14: Eintrag (Hex-Dump) mit versendetem Anhang

In der Datenbank sind in der Tabelle ZMESSAGE die höchste Anzahl an Attributen abgelegt. Dabei sind verschiedene Informationen zu finden, welche forensisch relevant sein könnten. Dazu gehören z.B. der Zeitpunkt der Zustellung der Nachricht und der Inhalt der versendeten Nachrichten, die in im Attribut ZTEXT zu finden sind. Die Datentypen sind in Tabelle 5 aufgelistet.

Tabelle 5: Tabelle ZMESSAGE der SQL-Datenbank

Attribut	Datentyp	Beobachtungen
Z_PK	Integer	Dieser Wert fungiert als primär Schlüssel der Tabelle.
Z_ENT	Integer	
Z_OPT	Integer	
ZDELIVERED	Integer	Dieses Attribut weist entweder den Wert „1“ oder „0“ auf und gibt an, ob eine Nachricht zugestellt werden konnte.
ZFLAGS	Integer	Dieses Attribut weist entweder den Wert „1“, „17“ oder null auf. Aus den vorliegenden Daten geht nicht hervor, welche Bedeutung diese haben.
ZISCREATEDFROMWEB	Integer	In den vorliegenden Daten sind keine Einträge vorhanden. Resultierend aus der Bezeichnung könnte dieses Attribut angeben, ob die Nachrichten mittels der Web-Version des Dienstes versendet wurden. In der Untersuchung wurden allerdings ausschließlich Daten mittels Smartphones erzeugt.

ZISOWN	Integer	Das Attribut weist entweder den Wert „1“ oder „0“ auf. Aus den vorliegenden Daten konnte nicht erschlossen werden, was inhaltlich umfasst wird.
ZPROPERTY2	Integer	Das Attribut weist ausschließlich den Wert „1“ auf. Aus den vorliegenden Daten konnte nicht erschlossen werden, was inhaltlich umfasst wird
ZREAD	Integer	Das Attribut weist entweder den Wert „1“ oder „0“ auf. Dieser gibt an, ob eine Nachricht gelesen wurde oder nicht.
ZSENDFAILED	Integer	Das Attribut weist ausschließlich den Wert „0“ oder NULL auf. Aus den vorliegenden Daten konnte nicht erschlossen werden, was inhaltlich umfasst wird. Aufgrund der Bezeichnung könnte der Wert angeben, ob das Senden einer Nachricht nicht erfolgen konnte.
ZSENT	Integer	Das Attribut weist entweder den Wert „1“ oder „0“ auf. Aus den vorliegenden Daten konnte nicht erschlossen werden, was inhaltlich umfasst wird. Vermutlich wird der Wert „1“ gesetzt, wenn das Senden einer Nachricht erfolgen konnte.

ZUSERBACK	Integer	Das Attribut weist ausschließlich den Wert „0“ auf. Aus den vorliegenden Daten konnte nicht erschlossen werden, was inhaltlich umfasst wird.
ZCONVERSATION	Integer	Das Attribut dient dieses Attribut der Zuordnung der jeweiligen Chats, in denen die Nachrichten versendet wurden.
ZSENDER	Integer	Das Attribut gibt an, welche der Kontakte die Nachricht versendet hat. Hierbei wird NULL eingetragen, wenn der Versender der Nutzer des untersuchten Accounts ist.
ZAUDIOSIZE	Integer	Das Attribut weist entweder den Wert „1“ oder „0“ auf. Aus den vorliegenden Daten kann nicht erschlossen werden, was dieses angibt. Jedoch lässt die Bezeichnung vermuten, dass das Attribut die Größe von versendeten Audionachrichten enthält.

ZAUDIO	Integer	Aus den vorliegenden Daten kann nicht erschlossen werden, was dieses angibt. Es liegt nur der Wert null vor.
ZBALLOTSTATE	Integer	Aus den vorliegenden Daten geht hervor, dass keine Werte im Attribut ZTEXT abgelegt sind, wenn dieser Wert nicht null ist. Aufgrund dessen und der Bezeichnung des Attributs, welche übersetzt Abstimmungsstatus bedeutet, kann vermuten werden, dass dieser Wert angibt, wie ein Nutzer abgestimmt hat, in der Umfragefunktion.
ZBALLOT	Integer	Das Attribut gibt einen Index an, welcher der Zuordnung zu der jeweiligen Abstimmung dient.
ZFILESIZE	Integer	Aus den erzeugten Daten geht hervor, wie groß eine versendete Datei ist, da nur wenn dieser Wert ungleich null ist, ein Wert im Attribut ZFILENAME, der die Bezeichnung einer Datei enthält, abgelegt ist. Auch weitere Attribute, welche im Zusammenhang mit dem Versenden von Dateien stehen, beinhalten nur einen Wert, wenn auch in diesem Attribut ein Wert enthalten ist.

ZTYPE	Integer	Aus den vorliegenden Daten kann nicht erschlossen werden, was dieses angibt.
ZDATA	Integer	Aus den vorliegenden Daten kann nicht erschlossen werden, was dieses angibt. Die Bezeichnung des Attributs lässt vermuten, dass dieses in Zusammenhang mit versandten Daten steht.
ZTHUMBNAIL1	Integer	Aus den vorliegenden Daten kann nicht erschlossen werden, was dieses angibt.
ZTYPE1	Integer	Aus den vorliegenden Daten kann nicht erschlossen werden, was dieses angibt.
ZVIDEOSIZE	Integer	Aus den vorliegenden Daten kann nicht erschlossen werden, was dieses angibt. Die Bezeichnung des Attributs lässt vermuten, dass es die Größe von entsendeten Videodateien enthält.
ZTHUMBNAIL2	Integer	Aus den vorliegenden Daten kann nicht erschlossen werden, was dieses angibt.

ZVIDEO	Integer	Aus den vorliegenden Daten kann nicht erschlossen werden, was dieses angibt. Die Bezeichnung des Attributs lässt vermuten, dass dieses in Zusammenhang mit Videonachrichten steht.
ZDATE	Timestamp	Dieses Attribut umfasst den Zeitpunkt, an welchem eine Nachricht durch den Nutzer des Accounts versendet wurde.
ZDELIVERYDATE	Timestamp	Dieses Attribut umfasst den Zeitpunkt, an welchem eine Nachricht zugestellt wird. Dabei ist nicht für jede Nachricht ein Wert hinterlegt.
ZREADDATE	Timestamp	Dieses Attribut umfasst den Zeitpunkt, an welchem eine Nachricht gelesen wird.
ZREMOTESENTDATE	Timestamp	Aus den vorliegenden Daten kann nicht erschlossen werden, was dieses angibt. Wobei der Name vermuten lässt, dass in diesem Attribut ein Datum hinterlegt ist, wenn die Nachricht ohne einen Zugang zu Internet versucht wurde, zu versenden.

ZUSERBACKDATE	Timestamp	Aus den vorliegenden Daten kann nicht erschlossen werden, was dieses angibt. Es sind ausschließlich null Werte hinterlegt.
ZDURATION	Float	
ZACCURACY	Float	Dieser Wert enthält vermutlich die Genauigkeit einer Standortangabe, wobei in den Daten nur „0“ hinterlegt ist, weswegen keine abschließende Ausgabe getroffen werden kann. Jedoch steht dieses Attribut definitiv in Zusammenhang mit Nachrichten, die einen Standort umfassen. Dies ist erkennbar anhand dessen, dass in allen Zeilen, in denen ein Wert für den Längen- und Breitengrad abgelegt ist, ein Wert für diese Attribut vorliegt.
ZLATITUDE	Float	Aufgrund des Namens und der Daten geht hervor, dass dieses Attribut den Breitengrad eines versendeten Standortes umfasst.
ZLONGITUDE	Float	Aufgrund des Namens und der Daten geht hervor, dass dieses Attribut den Längengrad eines versendeten Standortes umfasst.

ZDURATION1	Float	Aus den vorliegenden Daten kann nicht erschlossen werden, was dieses angibt. Es sind ausschließlich null Werte hinterlegt.
ZWEBREQUESTID	Varchar	Aus den vorliegenden Daten kann nicht erschlossen werden, was dieses angibt. Es sind ausschließlich null Werte hinterlegt.
ZPROBERTY1	Varchar	Aus den vorliegenden Daten kann nicht erschlossen werden, was dieses angibt. Es sind ausschließlich null Werte hinterlegt.
ZFILENAME	Varchar	Auf Grundlage der vorliegenden Daten kann entnommen werden, dass dieses Attribut den Namen einer versendeten Datei enthält.
ZJSON	Varchar	Auf Grundlage der vorliegenden Daten kann entnommen werden, dass dieses Attribut Informationen einer versendeten Datei enthält.
ZMIMETYPE	Varchar	Auf Grundlage der vorliegenden Daten kann entnommen werden, dass dieses Attribut Verzeichnispfade zu versendeten Daten enthält.

ZPOINAME	Varchar	Auf Grundlage der vorliegenden Daten kann entnommen werden, dass dieses Attribut Informationen zu versandten Standorten enthält. Korrekt umfasst der Werte Orte.
ZREVERSEGEOCODINGRESULT	Varchar	Auf Grundlage der vorliegenden Daten kann entnommen werden, dass dieses Attribut Informationen zu versandten Standorten enthält. Diese Spalte liefert Adressen.
ZTEXT	Varchar	Auf Grundlage der vorliegenden Daten kann entnommen werden, dass dieses Attribut den Inhalt von textuellen Daten umfasst.
ZID	Blob	Aus den vorliegenden Daten kann nicht erschlossen werden, was dieses angibt.
ZAUDIOBLOBID	Blob	Aus den vorliegenden Daten kann nicht erschlossen werden, was dieses angibt.
ZENCRYPTIONKEY	Blob	Aus den vorliegenden Daten kann nicht erschlossen werden, was dieses angibt. Aufgrund des Namens kann vermuten werden, dass dieses Feld einen Schlüssel zur Entschlüsselung beinhaltet.

ZBLOBID	Blob	Aus den vorliegenden Daten kann nicht erschlossen werden, was dieses angibt.
ZBLOBTHUMBNAILID	Blob	Aus den vorliegenden Daten kann nicht erschlossen werden, was dieses angibt.
ZENCRYPTIONKEY1	Blob	Aus den vorliegenden Daten kann nicht erschlossen werden, was dieses angibt. Aufgrund des Namens kann vermuten werden, dass dieses Felds einen Schlüssel zur Entschlüsselung beinhaltet.
ZENCRYPTIONKEY2	Blob	Aus den vorliegenden Daten kann nicht erschlossen werden, was dieses angibt. Aufgrund des Namens kann vermuten werden, dass dieses Felds einen Schlüssel zur Entschlüsselung beinhaltet.
ZIMAGEBLOBID	Blob	Aus den vorliegenden Daten kann nicht erschlossen werden, was dieses angibt.
ZIMAGEONCE	Blob	Aus den vorliegenden Daten kann nicht erschlossen werden, was dieses angibt.

ZARB	Blob	Aus den vorliegenden Daten kann nicht erschlossen werden, was dieses angibt.
ZQUOTEMESSAGEID	Blob	Aus den vorliegenden Daten kann nicht erschlossen werden, was dieses angibt.
ZENCRYPTIONKEY3	Blob	Aus den vorliegenden Daten kann nicht erschlossen werden, was dieses angibt. Aufgrund des Namens kann vermuten werden, dass dieses Felds einen Schlüssel zur Entschlüsselung beinhaltet.
ZVIDEOBLOBID	Blob	Aus den vorliegenden Daten kann nicht erschlossen werden, was dieses angibt.

5.2.2 Analyse und Aufbereitung der Standortinformationen

Aus den exportierten Daten, die durch *Cellebrite* aufbereitet wurden, ist zu erkennen, dass Standorte, welche in Form von Nachrichten versendet werde, in der *ThreemaData.sqlite* Datenbank abgelegt werden. Diese werden in dem Tabellenformat ZMESSAGE in der festen Größen 4247552 Bytes abgelegt. Die Struktur wird in Tabelle 5 detailliert erläutert. Neben dem Breiten- und Längengrad werden auch fallweise Adressen sowie Zeitstempel übergeben. Diese werden ausschließlich bei dem Versenden von Standorten abgelegt.

Tabelle 6: Übersicht der exportierten Standorte

#	Zeit	Breiten-grad	Längen-grad	Adresse	Quelldatei-Information
1	10.11.2021 10:40:08 (UTC+1)	54.567376	13.1040478		Apple_iPhone 7 (A1778).zip/root/private/var/mobile/Containers/Shared/AppGroup/B024BEBD-B9F9-4B40-B15F-25FD0D5E9E37/ThreemaData.sqlite : 0x2D963B (Tabelle: ZMESSAGE, Größe: 4247552 Bytes)
2	10.11.2021 10:39:49 (UTC+1)	57.114343	9.058375	Thistedvej 671, 9690 Fjerritslev, Dänemark	Apple_iPhone 7 (A1778).zip/root/private/var/mobile/Containers/Shared/AppGroup/B024BEBD-B9F9-4B40-B15F-25FD0D5E9E37/ThreemaData.sqlite : 0x2D96B3 (Tabelle: ZMESSAGE, Größe: 4247552 Bytes)
3	09.11.2021 15:53:34 (UTC+1)	51.502286	-0.16227	Serpentine Walk, London, SW1X, England	Apple_iPhone 7 (A1778).zip/root/private/var/mobile/Containers/Shared/AppGroup/B024BEBD-B9F9-4B40-B15F-25FD0D5E9E37/ThreemaData.sqlite : 0x24FDCD (Tabelle: ZMESSAGE, Größe: 4247552 Bytes)
4	09.11.2021 15:28:09 (UTC+1)	53.7701408	7.6937222		Apple_iPhone 7 (A1778).zip/root/private/var/mobile/Containers/Shared/AppGroup/B024BEBD-B9F9-4B40-B15F-25FD0D5E9E37/ThreemaData.sqlite : 0x1F94EE (Tabelle: ZMESSAGE, Größe: 4247552 Bytes)
5	09.11.2021 15:27:53 (UTC+1)	48.408928	12.19421	Kölnberg 1, 84171 Baierbach,	Apple_iPhone 7 (A1778).zip/root/private/var/mobile/Containers/Shared/AppGroup/B024BEBD-B9F9-4B40-B15F-25FD0D5E9E37/ThreemaData.sqlite :

				Deutsch-land	0x1F9A83 (Tabelle: ZMESSAGE, Größe: 4247552 Bytes)
6	09.11.2021 15:13:13 (UTC+1)	54.417243	13.4305343		Apple_iPhone 7 (A1778).zip/root/private/var/mobile/Containers/Shared/AppGroup/B024BEBD-B9F9-4B40-B15F-25FD0D5E9E37/ThreemaData.sqlite : 0x18633D (Tabelle: ZMESSAGE, Größe: 4247552 Bytes)
7	09.11.2021 15:12:58 (UTC+1)	51.004539	11.005643	Berliner Straße 1A, 99091 Erfurt, Deutsch-land	Apple_iPhone 7 (A1778).zip/root/private/var/mobile/Containers/Shared/AppGroup/B024BEBD-B9F9-4B40-B15F-25FD0D5E9E37/ThreemaData.sqlite : 0x1863A9 (Tabelle: ZMESSAGE, Größe: 4247552 Bytes)
8	09.11.2021 13:48:01 (UTC+1)	57.046915	9.920213		Apple_iPhone 7 (A1778).zip/root/private/var/mobile/Containers/Shared/AppGroup/B024BEBD-B9F9-4B40-B15F-25FD0D5E9E37/ThreemaData.sqlite : 0xC44A5 (Tabelle: ZMESSAGE, Größe: 4247552 Bytes)
9	09.11.2021 13:47:15 (UTC+1)	71.169566	25.783566		Apple_iPhone 7 (A1778).zip/root/private/var/mobile/Containers/Shared/AppGroup/B024BEBD-B9F9-4B40-B15F-25FD0D5E9E37/ThreemaData.sqlite : 0xC441C (Tabelle: ZMESSAGE, Größe: 4247552 Bytes)

10	09.11.2021 13:32:03 (UTC+1)	48.8611968051426	2.3351043878137 8		Apple_iPhone 7 (A1778).zip/root/private/var/mobile/Containers/Shared/AppGroup/B024BEBD-B9F9-4B40-B15F-25FD0D5E9E37/ThreemaData.sqlite : 0x5F6DF (Tabelle: ZMESSAGE, Größe: 4247552 Bytes)

5.2.3 Analyse und Aufbereitung der Kontaktinformationen

Die Informationen der Kontakte konnte durch *Cellebrite* extrahiert und exportiert werden. Alle Einträge sind in dem Tabellentyp ZCONTACT in der *ThreemaData.sqlite-wal* Datenbank abgelegt. Die Einträge wurden aufeinanderfolgend abgelegt. In der Tabelle 7 sind die abgelegten Daten dargestellt.

Tabelle 7: Export der Informationen zu den Kontakten aus Cellebrite

#	Name	Eingaben	Quelle	Quelldatei-Informationen
1		**User ID-:** ECHO-ECHO	Threema	Apple_iPhone 7 (A1778).zip/root/private/var/mobile/Containers/Shared/AppGroup/B024BEBD-B9F9-4B40-B15F-25FD0D5E9E37/ThreemaData.sqlite-wal : 0x2F85AE (Tabelle: ZCONTACT, Größe: 3221872 Bytes)
2	Nele	**User ID-:** CEWRPNRP	Threema	Apple_iPhone 7 (A1778).zip/root/private/var/mobile/Containers/Shared/AppGroup/B024BEBD-B9F9-4B40-B15F-25FD0D5E9E37/ThreemaData.sqlite-wal : 0x2F8649 (Tabelle: ZCONTACT, Größe: 3221872 Bytes)
3	Schrödi ;)	**User ID-:** 2S65VP2B	Threema	Apple_iPhone 7 (A1778).zip/root/private/var/mobile/Containers/Shared/AppGroup/B024BEBD-B9F9-4B40-B15F-25FD0D5E9E37/ThreemaData.sqlite-wal : 0x2F8561 (Tabelle: ZCONTACT, Größe: 3221872 Bytes)

Dem Nutzeraccount des Nutzers des untersuchten Mobilgerätes wird die User-ID ECHO-ECHO zugeordnet. Bei anderen Nutzern, mit welchen dieser Nutzer kommuniziert hat, sind außerdem die Namen, die er gewählt hat, ablegt. Die Informationen reichen nicht aus, um eine Person zu identifizieren. Sie können jedoch Hinweise liefern. Zudem ist die User-ID hinterlegt, welche einzigartig ist und bei der Erstellung der Nutzeraccounts erzeugt wird. Sie kann verwendet werden, um Nutzer zu identifizieren. Die Struktur des Tabellentypes als Teil der SQLite-Datenbank ist in Tabelle 8 dargestellt. Dazu sind der Online SQL-Viewer (https://sqliteviewer.app/) verwendet worden. Die Untersuchungen bestätigten die drei Einträge, wie sie durch *Cellebrite* aufbereitet wurden. In der Datenbank ist neben der Threema-ID der vollständige Name eingetragen. Die Informationen können hilfreich sein, um die Kommunikationsparteien zu identifizieren.

Tabelle 8: Tabellentyp ZCONTACT der SQL-Datenbank

Attribut	Datentyp	Beobachtungen
Z_PK	Integer	Dieser Wert fungiert als primär Schlüssel der Tabelle.
Z_ENT	Integer	Aus den vorliegenden Daten kann nicht erschlossen werden, was dieses Feld angibt. Es sind ausschließlich Nullen abgelegt.
Z_OPT	Integer	Aus den vorliegenden Daten kann nicht erschlossen werden, was dieses Feld angibt. Es sind ausschließlich Nullen abgelegt.
ZABRECORDID	Integer	
ZFEATURELEVEL	Integer	Aus den vorliegenden Daten kann nicht erschlossen werden, was dieses Feld angibt.
ZHIDDEN	Integer	Aus den vorliegenden Daten kann nicht erschlossen werden, was dieses Feld angibt.
ZPROFILEPIC-TURESENDED	Integer	Aus den vorliegenden Daten kann nicht erschlossen werden, was dieses Feld angibt.

ZPROBERTY2	Integer	Aus den vorliegenden Daten kann nicht erschlossen werden, was dieses Feld angibt.
ZSORTINDEX	Integer	Aus den vorliegenden Daten kann nicht erschlossen werden, was dieses Feld angibt.
ZSTATE	Integer	Aus den vorliegenden Daten kann nicht erschlossen werden, was dieses Feld angibt.
ZVERIFICATIONLEVEL	Integer	Aus den vorliegenden Daten kann nicht erschlossen werden, was dieses Feld angibt.
ZWORKCONTACT	Integer	Aus den vorliegenden Daten kann nicht erschlossen werden, was dieses Feld angibt. Es sind ausschließlich Nullen abgelegt.
ZCONTACTIMAGE	Integer	Aus den vorliegenden Daten kann nicht erschlossen werden, was dieses Feld angibt.
Z2PARICIPANTS	Integer	Aus den vorliegenden Daten kann nicht erschlossen werden, was dieses Feld angibt. Es sind ausschließlich Nullen abgelegt.

ZPROFILEPICTUREUP-LOAD	Timestamp	Das Attribut enthält vermutlich das Datum, an welchem das Profilbild hochgeladen wurden. Dies kann bei der Identifikation von Beteiligten Personen eines Verbrechens unterstützen.
ZCNCONTACTID	Varchar	Das Attribut der Indexierung der Kontakte. Hierbei ist kein Wert für den angemeldeten Nutzers hinterlegt.
ZFIRSTNAME	Varchar	Das Attribut enthält für jeden Kontakt den vollständigen Vornamen. Dies kann bei der Identifikation von Beteiligten Personen eines Verbrechens unterstützen.
ZIDENTITY	Varchar	Dieses Attribut enthält die Threema-ID des jeweiligen Kontaktes. Auffällig ist, dass für den Nutzer des untersuchten Testgerätes der Wert „ECHOECHO“ hinterlegt ist.
ZLASTNAME	Varchar	Das Attribut enthält für jeden Kontakt den vollständigen Nachnamen. Dies kann bei der Identifikation von Beteiligten Personen eines Verbrechens unterstützen.
ZPROPERTY1	Varchar	Aus den vorliegenden Daten kann nicht erschlossen werden, was dieses Feld angibt. Es sind keine Werte, in dieser Spalte zu finden.

ZPUBLICNICKNAME	Varchar	Dieses Attribut umfasst den öffentlichen Nickname der Nutzer. Für den Nutzer des untersuchten Gerätes ist kein Wert hinterlegt.
ZSORTINITIAL	Varchar	Das Attribut enthält jeweils den Anfangsbuchstaben des Nachnamens. Nur den Nutzer des untersuchten Gerätes ist der Anfangsbuchstabe des Wertes aus dem Attribut ZPUBLICNICKNAME entnommen.
ZVERIFIEDEMAIL	Varchar	Dieses Attribut umfasst den öffentlichen Nickname der Nutzer. Für den Nutzer des untersuchten Gerätes ist kein Wert hinterlegt.
ZVERIFIEDMOBILENO	Varchar	Dieses Attribut umfasst den öffentlichen Nickname der Nutzer. Für den Nutzer des untersuchten Gerätes ist kein Wert hinterlegt.
ZIMAGEDATA	Blob	Dieses Attribut umfasst den öffentlichen Nickname der Nutzer. Für den Nutzer des untersuchten Gerätes ist kein Wert hinterlegt.
ZPUBLICKEY	Blob	Dieses Attribut umfasst den öffentlichen Nickname der Nutzer. Wobei es sich vermutlich, um einen öffentlichen Schlüssel handelt.

6 Diskussion

In diesem Abschnitt werden die Erkenntnisse dieser Bachelorarbeit interpretiert und diskutiert. Die Analyse der Artefakte, welche durch den IM-Dienst „Threema“ erzeugt werden, ergab, dass Informationen, die durch die Kommunikation von Nutzern generiert wurden, in den SQL-Datenbanken abgelegt werden. Dies konnte durch die Aufbereitung und Sicherung durch das Tool *Cellebrite* rekonstruiert werden

Die ausgetauschten Nachrichten werden in der Tabelle *ZMESSAGE* der Datenbanken *ThreemaData.sqlit*e und *ThreemaData.sqlite-wal* abgelegt. In der vorliegenden Arbeit konnte für einige Attribute der Tabelle nicht abgeleitet werden, welche Information abgelegt werden. Die Ursache liegt an den erzeugten Daten. Für weiterführende Forschungen werden die einzelnen Attribute interessant sein, dazu müssen im Prozess der Erzeugung Daten konkrete Anwendungsfälle entwickelt werden. Die Erkenntnisse dieser Arbeit ermöglichen, dass eine effizientere Untersuchung von dem IM-Dienst vorgenommen werden kann, da die Struktur sowie Hex-Dumps umfassend aufgebarbeitet sind. Der Prozess zur Aufbereitung und Analyse wird für Experten der Forensik anhand „Threema“ erläutert. Im Kontext der Nachrichten wurden versendete bzw. empfangene Standorte separat betrachtet, da diese von besonderer Relevanz für forensische Ermittlungen sind. Das liegt dem zu Grunde, dass diese hilfreich sein können, um den Tatort einzugrenzen und dahingehende weitere Untersuchungen vor Ort durchzuführen. Zusätzlich hilft es den Tathergang zu rekonstruieren, da Bewegungsmuster erkennbar sein könnten, wodurch detektiert werden kann, ob ein Beschuldigter sich an dem Tatort aufgehalten hat.

Zudem wurde die Tabelle *ZCONTACT* detaillierter analysiert. Die Informationen können forensisch wertvoll für die Identifizierung der Gesprächsparteien sein. Dieser Bereich wurde in dieser Arbeit ausführlich untersucht.

Weiterer Forschungsbedarf besteht in der Wiederherstellung von. Videos oder Fotos, welche über „Threema“ ausgetauscht wurden und möglicherweise Straftaten dokumentieren haben könnten. Die vorliegende Arbeit kann die Grundlage hierfür darstellen, da die Ablageorte dokumentiert sind.

Weitere Informationen können mittels der Aufbereitung der Konversationsinhalte detektiert werden, da sich potenzielle Verdächtige möglicherweise über die Tat ausgetauscht haben könnten. Die Strukturen der Verzeichnisse wurden in vorangegangenen Arbeiten nur unter

Android untersucht. Diese Arbeit, welche erstmalig die Untersuchung unter iOS behandelt, umfasst nicht die Entschlüsselung der Daten, die Sicherung und Extraktion.

In zukünftigen Untersuchungen besteht ein Forschungsbedarf insbesondere in der Entschlüsselung der Daten.

In dieser Arbeit wurde ausschließlich der Struktur der Artefakte unter iOS untersucht. Der Fokus lag nicht auf gelöschten Daten, woraus die Notwendigkeit von weiteren Untersuchungen resultiert. Die Untersuchungen des IM-Dienstes in der Desktop-Version wurden bisher noch nicht durchgeführt. Außerdem ist es lohnend, in zukünftigen Forschungen die Enkodierung der Rohdaten näher zu betrachten.

Zusammenfassend zeigt die Diskussion, dass die Ergebnisse forensischen Experten helfen können, relevante Daten, die durch den IM-Dienst erzeugt werden, zu identifizieren. Die Aufbereitung und Auswertung von Artefakten der Gesprächspartner ist detailliert dokumentiert. Die Analyse der Einträge in der Datenbanktabelle *ZMESSAGE* konnte nicht umfänglich vorgenommenen werden, da die vorliegenden Datenbasis nicht alle möglichen Anwendungsfälle abdecken konnte. Der Austausch von textuellen Daten und Standorten wurden tiefgehend untersucht. In folgenden Forschungsarbeiten sollte ein Fokus auf weiteren Anwendungsfällen liegen. Die gewonnenen Kenntnisse über die Art und Weise wie „Threema“ Daten ablegt, kann genutzt werden, um Skripte oder vollständige Programme zu entwickeln, welche automatisiert die Artefakte des IM-Dienstes auswerten und aufbereiten.

7 Fazit

Zur Rekonstruktion des Tathergangs im Verlauf eines Ermittlungs- und Strafverfahrens können Daten, die durch IM-Anwendungen erzeugt werden, potenziell relevante Informationen liefern. Sie können durch Täter, Opfer und Zeugen genutzt werden, um Informationen über eine strafrechtlich relevante Handlung auszutauschen. IM-Dienste gelten als sehr verbreitete und beliebte Applikationen auf mobilen Endgeräten, wodurch die Bedeutung der Daten für die Forensik kontinuierlich steigt. Auf dem Markt existiert eine Vielzahl von verschiedenen Anwendungen und Betriebssystemen sowie Hardware, weshalb die Auswertung und Aufbereitung dieser Daten eine Herausforderung darstellen kann. Die IM-Anwendung „Threema“ gehört zu den beliebtesten Messengern im deutschen Raum und bietet den Nutzern verschiedene Sicherheitsmechanismen, um die Daten vor unbefugten Personen zu schützen. Das erschwert den Untersuchungsprozess erheblich. Aus diesem Grund wurde in der Bachelorarbeit mittels des Reverse Engineering Prozesses der Dienst analysiert. Dazu wurde in den ersten Kapiteln die theoretischen Grundlagen erläutert. Diese umfasst die Definition der Begriffe der IT-Forensik und mobile Forensik. Zudem wurden IM-Anwendungen erläutert und der analysierte Dienst detailliert erklärt. Des Weiteren wurden die Anforderungen und das Prozessmodell der forensischen Untersuchungen beschrieben. Diese sollten, während jeder Begutachtung beachtet werden. In den folgenden Kapiteln wurde das Untersuchungsobjekt, der IM-Dienst „Threema“, in drei Phasen erforscht. Besonderer Fokus lag auf den Ablageorten und der Ablageart von Informationen über den textuellen Nachrichtenaustausch, den Austausch von Standorten sowie Informationen über die Kontakte.

Nachfolgend wird die Forschungsfrage erläutert und Einsicht in die Ergebnisse gewährt.

Wie können forensische Experten Informationen, welche für die Aufklärung von potenziellen Straftaten hilfreich sein könnten, aus den Daten, welche durch die Nutzung des Instant-Messengers „Threema“ erzeugt werden, aufbereiten und auswerten?

Infolge der weiten Verbreitung von Messenger-Diensten und der stetig wachsenden Verbreitung von Smartphones steigt die Bedeutung der mobilen Forensik. Die Artefakte der IM-Dienste können wichtige Informationen zu der Aufklärung von Verbrechen liefern. Täter, Opfer und Zeuge von Verstößen gegen gesetzliche Regelungen könnten diese z.B. zur Kommunikation über diese Vergehen nutzen. Somit können forensisch relevante Kenntnisse gesichert und ausgewertet werden. In dieser Arbeit wurde die Untersuchung für

„Threema“ vorgenommen. Die Analyse ergab, dass die für die Forensik am bedeutsamsten Daten wie Chatverläufe, Standortinformationen und Kontaktinformationen, in SQL-Datenbanken abgelegt werden. Durch die Aufbereitung der exportierten Daten mittels des Tools *Cellebrite*, konnten die Daten anschließend ausgewertet und analysiert werden. Somit konnten fallweise forensisch relevante Erkenntnisse erzielt werden. Die Analyse ergab, dass die in den SQL-Datenbanken abgelegten Daten zu der Aufklärung von Straftaten, durch die Rekonstruktion der Kommunikation der Beteiligten, die Standortnachverfolgung und die Identifizierung der Kontaktpersonen, beitragen können. Dem ist hinzuzufügen, dass teils durch mangelnde Informationen, keine Aussage über den Inhalt mancher Attribute getroffen werden konnte. Des Weiteren werden Standortinformationen ausschließlich bei dem Versenden von Standorten abgelegt und nicht standardmäßig erfasst. Die Kotaktinformationen können lediglich hilfreich sein, die Kommunikationsparteien zu identifizieren, die Voraussetzung ist dennoch die korrekte Angabe des vollständigen Namens durch die Kommunikationspartei selbst. Abschließend kann somit festgehalten werden, dass die Aufbereitung und Analyse der Artefakte des IM-Dienstes „Threema“ den Prozess der Aufklärung von Straftaten unterstützen kann, dies allerdings fallabhängig ist und stark von der fundamentalen Beweislage und dem Kenntnisstand der ermittelnden Personen/Forensiker abhängig ist.

Literatur

Anglano, C. (2014): Forensic analysis of WhatsApp Messenger on Android smartphones. In: Digital Investigation Journal, Volume 11, Issue 3, 2014, S. 201-213. (doi: https://doi.org/10.1016/j.diin.2014.04.003, verfügbar am 20.08.2023)

Anglano, C.; Canonico, M.; Guazzone, M. (2016): Forensic Analysis of the ChatSecure Instant Messaging Application on Android Smartphones. In: Digital Investigation Journal, Volume 19, 2016, S. 44-59, ISSN 1742-2876. (doi: https://doi.org/10.1016/j.diin.2016.10.001, verfügbar am 25.09.2023).

Anglano, C.; Canonico, M.; Guazzone, M. (2017): Forensic analysis of Telegram Messenger on Android smartphones. In: Digital Investigation Journal, Volume 23, 2017, S. 31-49; ISSN 1742-2876. (doi: https://doi.org/10.1016/j.diin.2017.09.002, verfügbar am 17.09.2023).

Apple Inc. (Hrsg.) (2023): Sicherheit der Apple-Plattformen, Startvorgang bei iOS-und iPadOS-Geräten. (https://support.apple.com/guide/security/boot-process-for-ios-and-ipados-devices-secb3000f149/web, verfügbar am 28.08.2023).

Azfar, A.; Raymond Choo, K.-K.; Lui, L. (2016): An Android Communication App Forensic Taxonomy. In: JOURNAL OF FORENSIC SCIENCES, Volume 61, Issue 5, September 2016, S. 1337-1350. (https://doi.org/10.1111/1556-4029.13164, verfügbar am 25.09.2023).

Bundesamt für Sicherheit in der Informationstechnik (Hrsg.) (2011): Leitfaden "IT-Forensik" Version 1.0.1 (März 2011). (https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Leitfaden_IT-Forensik.pdf?__blob=publicationFile&v=1, verfügbar am 01.07.2023).

Bundesamt für Sicherheit in der Informationstechnik (Hrsg.) (2021): DER.2.2 Vorsorge für die IT-Forensik. (https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2023/05_DER_Detektion_und_Reaktion/DER_2_2_Vorsorge_fuer_die_IT_Forensik_2023.pdf?__blob=publicationFile&v=3, verfügbar am 20.07.2023).

Bundesamt für Sicherheit in der Informationstechnik (Hrsg.) (2023): BSI – Technische Richtlinie, Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Version 2023-01. (https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf?__blob=publicationFile&v=10, verfügbar am 20.08.2023).

Bunting, S.; Wei, W. (2006): EnCase Computer Forensics: The official EnCE: EnCase Certified Examiner Study Guide. Indianapolis, IN: Wiley Publishing, Inc.

Chikofsky, E.; Cross, J. H. (1990): Reverse engineering and design recovery: a taxonomy. In: Journals & Magazines, IEEE Software, Volume 7 Issue: 1, S. 13 – 17. (https://ieeexplore.ieee.org/abstract/document/43044, verfügbar am 01.07.2023).

Debar, H.; Dacier, M.; Wespi, A. (1999): Towards a taxonomy of intrusion-detection systems. In: Computer Networks, Volume 31, Issue 8, 1999, S. 805-822, ISSN 1389-1286 (https://doi.org/10.1016/S1389-1286(98)00017-6, verfügbar am 15.07.2023).

Dewald, A.; Freiling, F. C. (2015): Forensische Informatik. 2. Aufl. Norderstedt: BoD - Books on Demand.

Dogan, S.; Akbal, E. (2017): Analysis of mobile phones in digital forensics. In: 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Kroatien, 2017, S. 1241-1244, (doi: https://doi.org/10.23919/MIPRO.2017.7973613, verfügbar am 15.07.2023).

Donovan, S. (1994): Patent, copyright and trade secret protection for software. In: IEEE Potentiales, 13, S. 20-24. (https://ieeexplore.ieee.org/document/310923, verfügbar am 19.07.2023).

Eilam, E.; Chikofsky, E. (2005): Reversing: Secrets of Reverse Engineering. 1. Aufl. Indianapolis, Indiana, USA: Wiley Publishing, Inc.

Geschonneck, A. (2014): Computer-Forensik Computerstraftaten erkennen, ermitteln, aufklären. 6. Aufl. Heidelberg: dpunkt.verlag.

Greveler, U.; Wellmeyer, M. (2011): Spionage via Webcam: Welchen Schutz bieten Personal Firewalls und Virenscanner. In: Schartner und Taeger (Hrsg.), D.A.CH Security '11, Reihe IT-Security und IT-Management, syssec. (https://1lab.de/pub/SpionageviaWebcam.pdf, verfügbar am 29.07.2023)

Hasselbring, W.; Bischofs; L.; Warns, T. (2008): Peer-to-Peer-Architekturen. (https://oceanrep.geomar.de/id/eprint/14499/1/HandbuchP2P2008.pdf, verfügbar am 04.09.2023).

Husain, M. I.; Sridhar, R. (2010.): iForensics: Forensic Analysis of Instant Messaging on Smart Phones. In: Goel, S. (eds) Digital Forensics and Cyber Crime. ICDF2C 2009. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 31. Springer, Berlin, Heidelberg. (https://doi.org/10.1007/978-3-642-11534-9_2, verfügbar am 25.09.2023).

Liu, F.; Liu, K.-S.; Chang, C.; Wang, Y. (2016): Research on the Technology of iOS Jailbreak. Sixth International Conference on Instrumentation & Measurement, Computer, Communication and Control (IMCCC), Harbin, China, 2016, S. 644-647. (doi: https://doi.org/10.1109/IMCCC.2016.178, verfügbar am 19.07.2023).

Lutkevich, B. (2021): Definition: TCP (Transmission Control Protocol). In: TechTarget, ComputerWeekly.de. (https://www.computerweekly.com/de/definition/TCP-Transmission-Control-Protocol, verfügbar am 22.07.2023).

Mannan, M.; Oorschot, P. v. (Hrsg.) (2004): Secure Public Instant Messaging: A Survey. (http://users.encs.concordia.ca/~mmannan/publications/pst04.pdf, verfügbar am 22.07.2023).

McDermid, V. (2016): Anatomie des Verbrechens Meilensteine der Forensik. 1. Aufl. München: Albrecht Knaus Verlag.

Mehtre, B.; Mehrotra, T. (2013): Forensic analysis of Wickr application on android devices. In: 2013 IEEE International Conference on Computational Intelligence and Computing Research. S. 1-6. Enathi, Indien, (doi: https://doi.org/10.1109/ICCIC.2013.6724230, verfügbar am 25.09.2023).

Moreb, M. (2022): Practical Forensic Analysis of Artifacts on iOS and Android Devices Investigating Complex Mobile Devices. APress Media, LLC, part of Springer Nature. (doi: https://doi.org/10.1007/978-1-4842-8026-3, verfügbar am 25.07.2023).

Needham, R. M.; Schroeder, M. D. (1978): Using encryption for authentication in large networks of computers. In: Communications of the ACM, Volume 21, Issue 12, December 1987, S. 993-999). (DOI: https://dl.acm.org/doi/10.1145/359657.359659, verfügbar am 25.07.2023).

Nelson, M. L. (2005): A Survey of Reverse Engineering and Program Comprehension. (https://arxiv.org/abs/cs/0503068, verfügbar am 01.07.2023).

Ovens, K. M.; Morison, G. (2016): Forensic analysis of Kik messenger on iOS devices. In: Digital Investigation, Volume 17, 2016. S. 40-52, ISSN 1742-2876. (doi: https://doi.org/10.1016/j.diin.2016.04.001, verfügbar am 25.08.2023).

Paterson, K.; Scarlata, M.; Troung, K. T. (2023): Three Lessons From Threema: Analysis of a Secure Messenger. 32nd USENIX Security Symposium, 9.-11. August 2023, Anaheim, CA, USA. (https://www.usenix.org/system/files/usenixsecurity23-paterson.pdf, verfügbar am 20.09.2023).

Restat, V. (2021): Automatisierte Fehlererkennung einer Microservice-Anwendung basierend auf Log-Dateien. Abschlussarbeit zur Erlangung des akademischen Grades Master of Science. Hochschule Darmstadt, Fachbereich Informatik & Fachbereich Mathematik und Naturwissenschaften. (https://fbmn.h-da.de/fileadmin/Dokumente/Studium/DS/2021_MDS_RestatValerie_THE.pdf, verfügbar am 16.08.2023.

Richter, L. (1985): Betriebssysteme: 2. Aufl. Stuttgart: B. G. Teubner Verlag

Salamh, F. E.; Mirza, M. M.; Hutchinson, S.; Yoon, Y. H.; Karabiyik, U. (2021): What's on the Horizon? An In-Depth Forensic Analysis of Android and iOS Applications. In: IEEE Access, Volume 9, S. 99421-99454, 2021. (https://ieeexplore.ieee.org/document/9477591, verfügbar am 15.09.2023).

Scarpati, J. (2020): Definition Instant Messaging. In: TechTarget ComputerWeekly.de. (https://www.computerweekly.com/de/definition/Instant-Messaging, verfügbar am 22.07.2023).

Siller, H. (2018). In: Gabler Wirtschaftslexikon, Springer Gabler Verlag (Hrsg.), Stichwort: Forensik (https://wirtschaftslexikon.gabler.de/definition/forensik-53390, verfügbar am 15. August 2023).

Skulkin, O.; Tindall, D.; Tamma, R. (2018): Learning Android Forensic Second Editiion Analyze Android deices with the latest forensic tools and techniques. 2. Aufl. Birmingham: Packt Publishing Ltd.

Son, J.; Kim, Y. W.; Oh, D. B.; Kim, K. (2022): Forensic analysis of instant messengers: Decrypt Signal, Wickr, and Threema, Forensic Science International. In: Digital Investigation, Volume 40, 2022, 301347, ISSN 2666-2817. (https://doi.org/10.1016/j.fsidi.2022.301347, verfügbar am 25.09.2023).

Spreitzenbarth, M. (2017): Mobile Hacking: Ein kompakter Einstieg ins Penetration Testing mobiler Applikationen - iOS, Android und Windows Mobile. 1. Aufl. Heidelberg: dpunkt.verlag GmbH.

Tamma, R.; Skulkin, O.; Mahalik, H.; Bommisetty, H.; Bommisetty, S. (2020): Practical Mobile Forensics Fourth Edition Forensically investigate and analyze iOS, Android, and Windows 10 devices. 4. Aufl. Birmingham: Packt Publishing Ltd.

Thakur, N. S. (2023): Forensic Analysis of WhatsApp on Android Smartphones. Theses and Dissertations, 1706, University of New Orleans. (https://scholarworks.uno.edu/td/1706/, verfügbar am 13.07.2023)

Threema GmbH (Hrsg.) (2023): Threema legt den Fokus auf Sicherheit und umfassenden Datenschutz. (https://threema.ch/de/security, verfügbar am 21.07.2023).

Threema GmbH (Hrsg.) (2023): Open Source. (https://threema.ch/de/open-source, verfügbar am 17.08.2023).

Threema GmbH (Hrsg.) (2023): Vielseitige Funktionen ohne überflüssige Spielereien: (https://threema.ch/de/funktionen, verfügbar am 10.07.2023).

Threema GmbH (Hrsg.) (2023): Threema ist ein Statement: (https://threema.ch/about, verfügbar am 10.07.2023).

Threema GmbH (Hrsg.) (2023): Was ist eine Threema-ID?. (https://threema.ch/de/faq/threema_id, verfügbar am 27.07.2023).

Threema GmbH (Hrsg.) (2023): Was sind private Chats und wie funktionieren sie?. (https://threema.ch/de/faq/private_chats, verfügbar am 27.07.2023)

Tso, Y.-C.; Wang, S.-J.; Huang, C.-T.; Wang, W.-J. (2012): iPhone social networking for evidence investigations using iTunes forensics. In: ICUIMC '12: Proceedings of the 6th International Conference on Ubiquitous Information Management and Communication, February 2012, Article No.: 62, S. 1-7. (doi: https://doi.org/10.1145/2184751.2184827, verfügbar am 20.09.2023).

Vogiazou, Y. (2002): Wireless Presence and Instant Messaging. The Open University, MK7 6AA, Milton Key, UA. (https://kmi.open.ac.uk/publications/papers/kmi-tr-124.pdf, verfügbar am 22.07.2023).

Walnycky, D.; Baggili, I.; Marrington, D.; Moore, J.; Breitinger, F. (2015): Network and device forensic analysis of Android social-messaging applications. In: Digital Investigation, Volume 14, Supplement1, 2015, S. S77-S84, ISSN 1742-2876. (https://doi.org/10.1016/j.diin.2015.05.009, verfügbar am 25.09.2023).

Wiedeking, H. (2019): Reverse Engineering von Messengerdaten auf Mobiltelefonen am Beispiel der Datenbanken des Dienstes TamTam. Bachelorarbeit. Hochschule Mittweida, Fachbereich Angewandte Computer- und Biowissenschaften. (https://monami.hs-mittweida.de/frontdoor/deliver/index/docId/12475/file/Bachelorarbeit_Hannah_Wiedeking.pdf, verfügbar am 15.07.2023).

Wu, S.; Zhang, Y.; Wang, X.; Xiong, X.; Du, L. (2016): Forensic analysis of WeChat on Android smartphones. In: Digital Investigation, Volume 21, 2017, Seiten 3-10, ISSN 1742-2876. (https://doi.org/10.1016/j.diin.2016.11.002, verfügbar am 25.09.2023).

Zhang, L.; Yu, F.; Ji, Q. (2016): The Forensic Analysis of WeChat Message. In: *2016 Sixth International Conference on Instrumentation & Measurement, Computer, Communication and Control (IMCCC)*, Harbin, China, 2016, S. 500-503.
(doi: https://doi.org/10.1109/IMCCC.2016.24, verfügbar am 20.07.2023).

Anlagen

Teil 1 ..... A-I

Teil 2 ..... A-III

Abbildungen, Teil 1

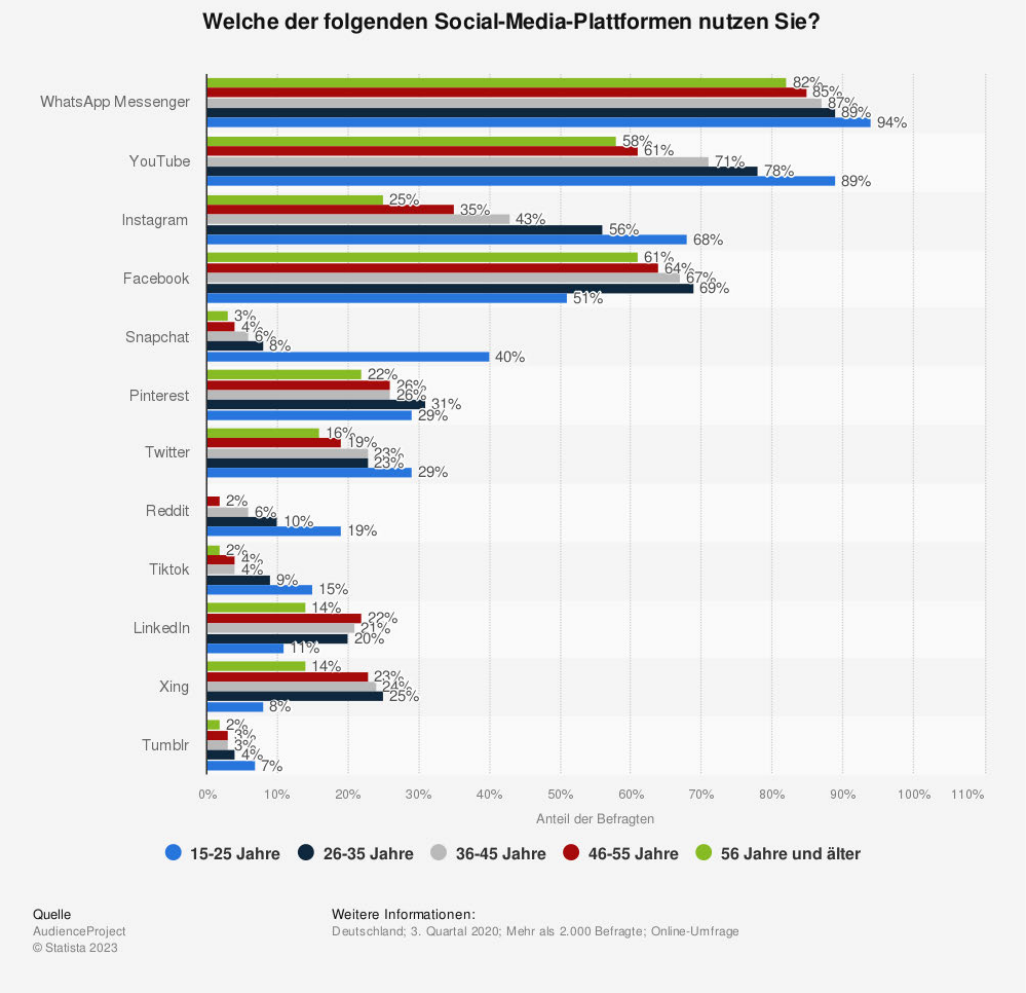

Abbildung 15: Welche der folgenden Social-Media-Plattformen nutzen Sie?

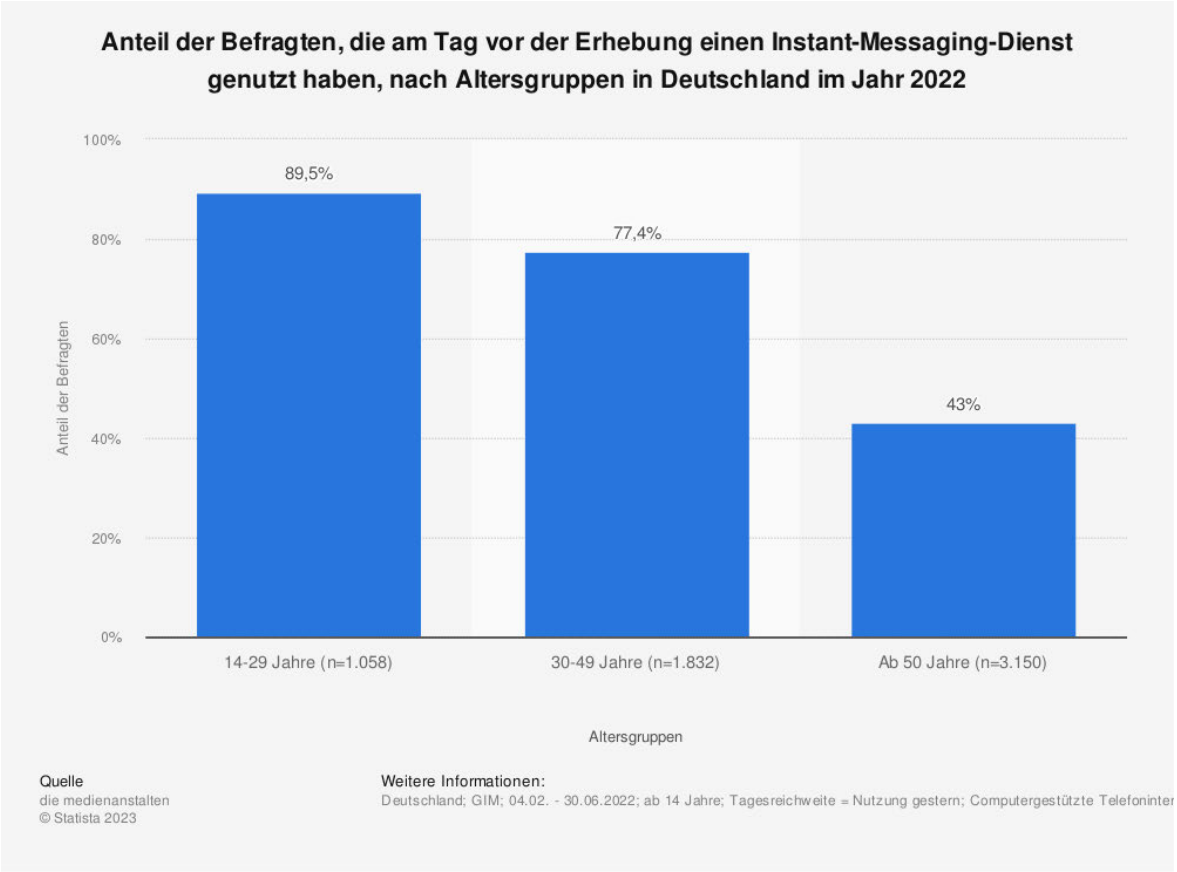

Abbildung 16: Anteil der Befragten, die am Tag vor der Erhebung einen Instant-Messaging-Dienst genutzt haben, nach Altersgruppen in Deutschland im Jahr 2022

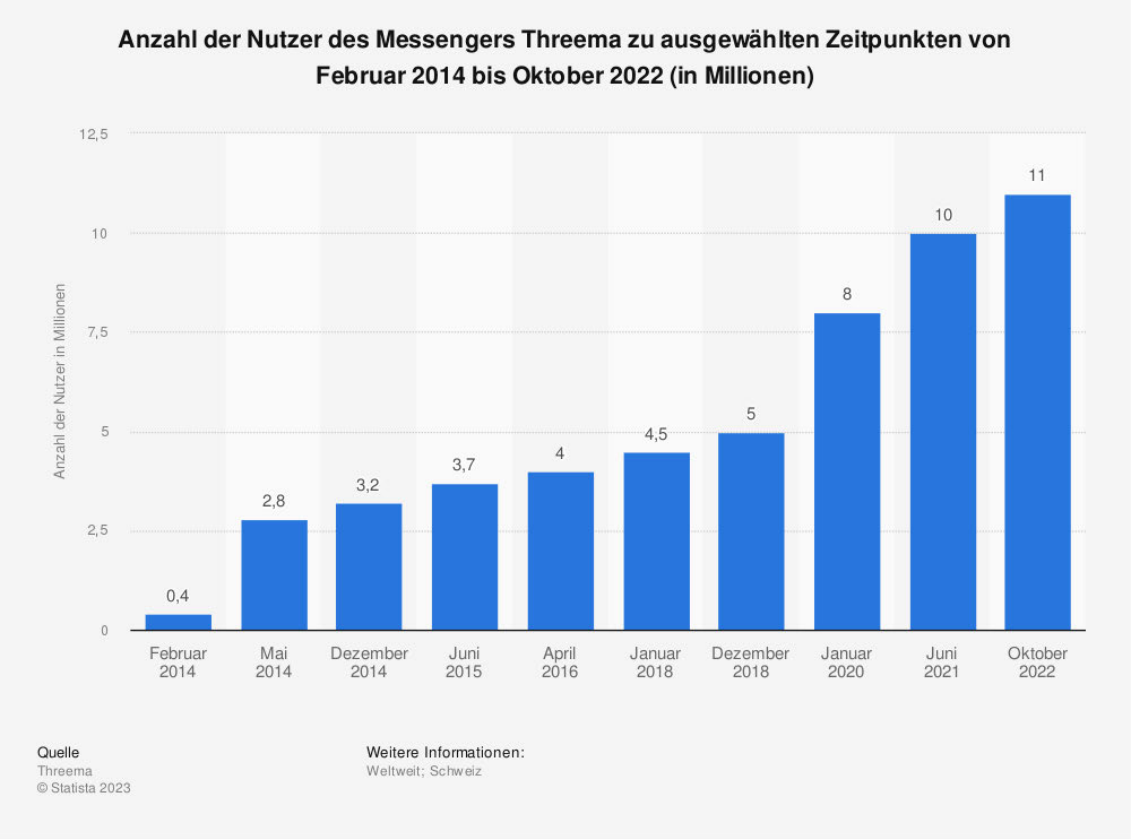

Abbildung 17: Anzahl der Nutzer von Threema weltweit

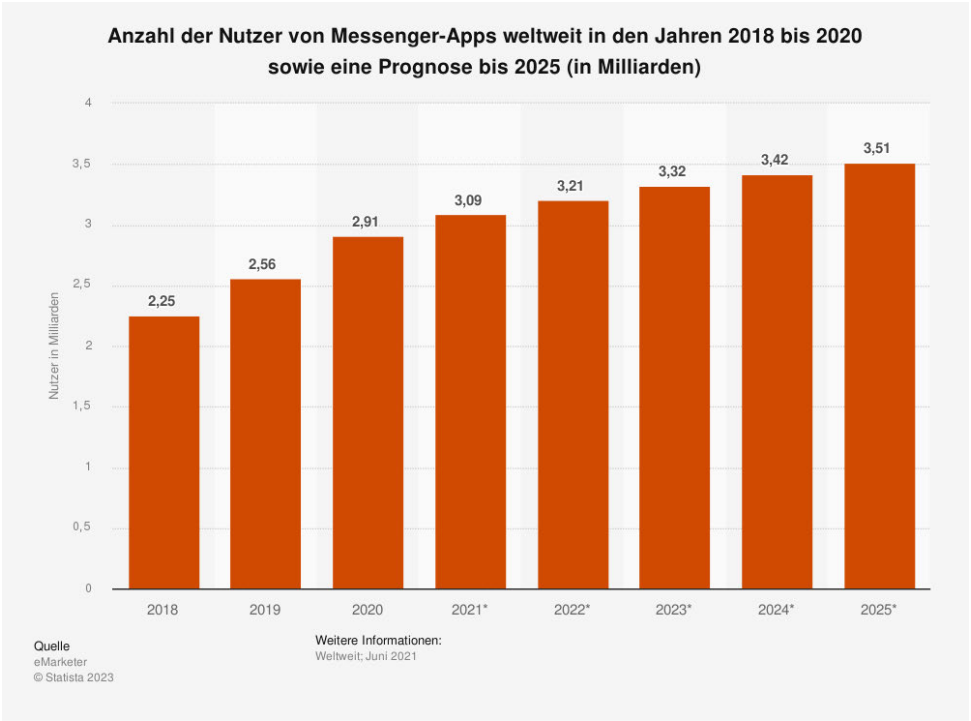

Abbildung 18: Nutzung von Messenger-Apps weltweit in den Jahren 2018 bis 2020 sowie eine Prognose bis 2025

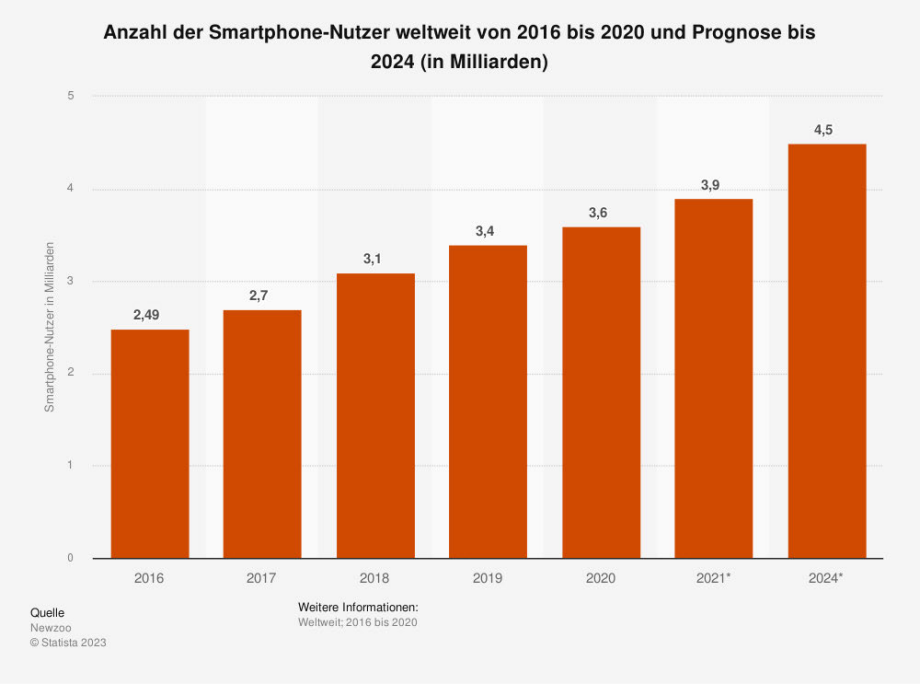

Abbildung 19: Smartphone-Nutzung weltweit von 2016 bis 2020 und Prognose bis 2024

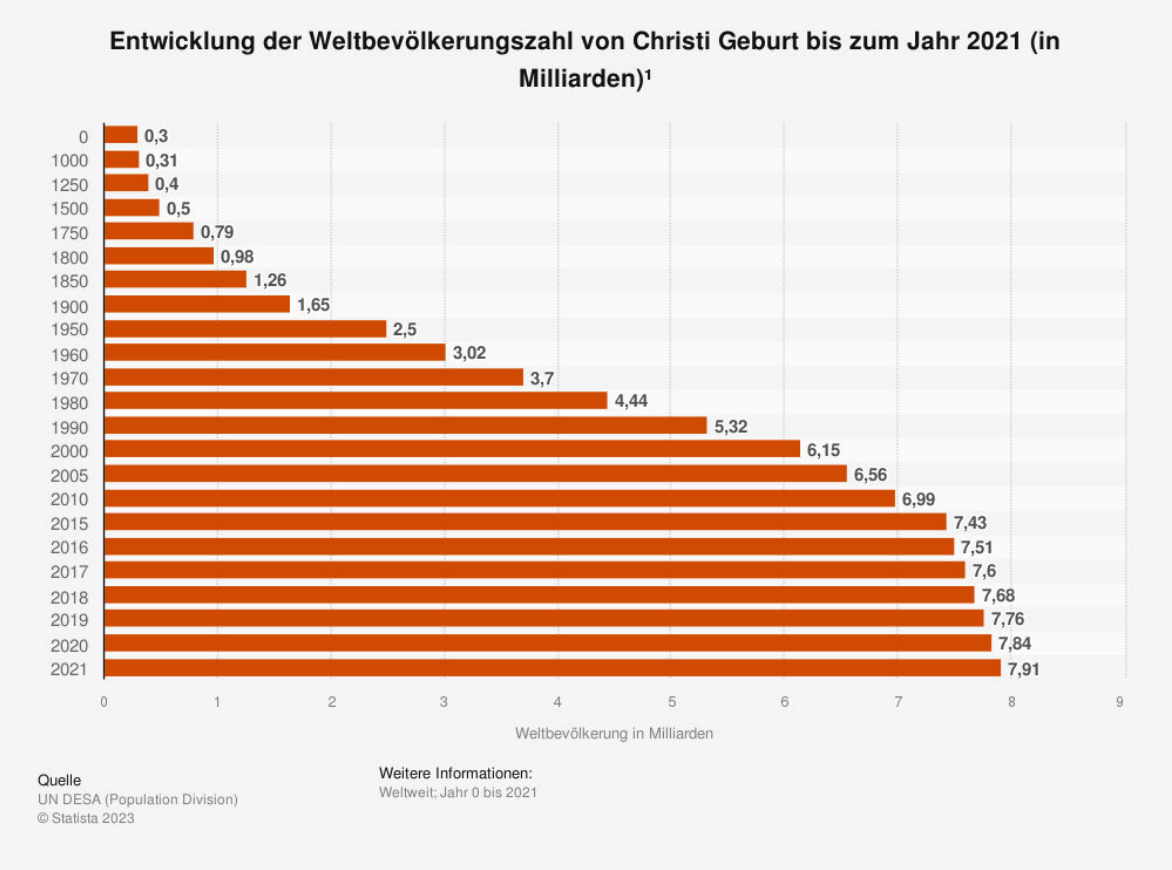

Abbildung 20: Entwicklung der Weltbevölkerung

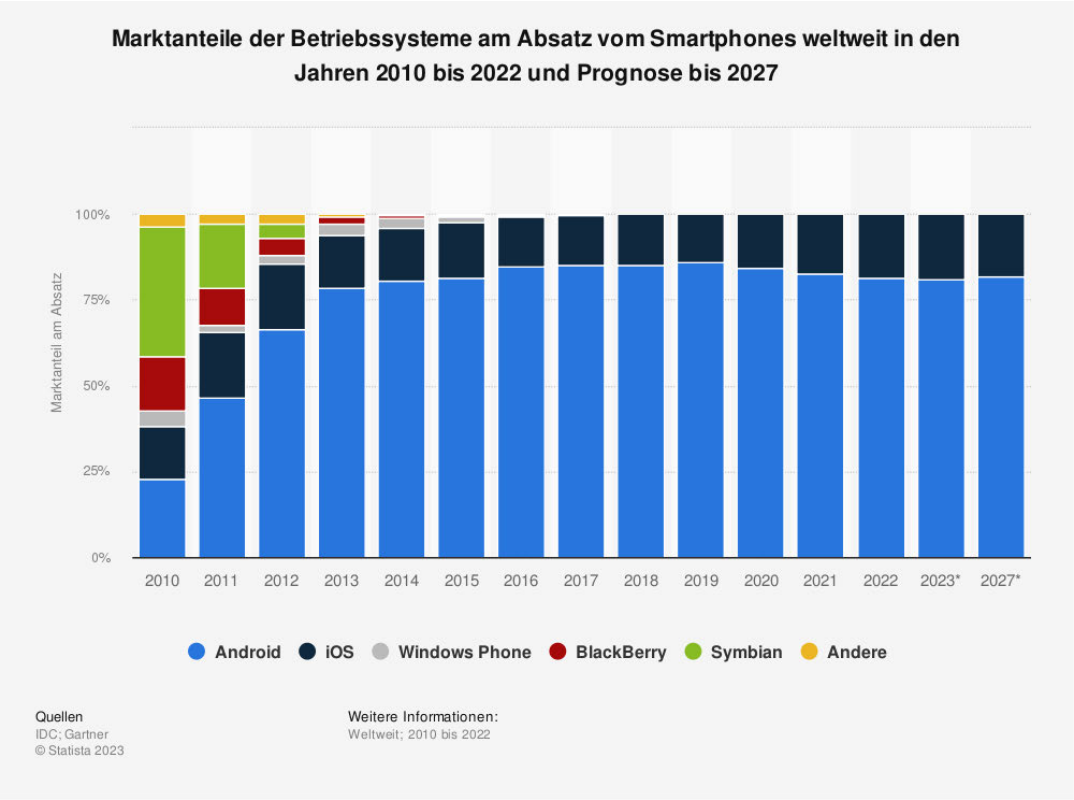

Abbildung 21: Marktanteile der Betriebssysteme am Absatz vom Smartphones weltweit in den Jahren 2010 bis 2022 und Prognose bis 2027

Tabellen, Teil 2

Tabelle 9: Experiment 1: Einzelchats Teil I

Experiment	Nickname	Sender/Gerät	Dateiname(n) + kurze Inhaltsbeschreibung (oder Originaldatei)	Datum/Uhrzeit
Nicknamen ändern	Nele	Helen, iPhone SE	Ändern des Nicknamens von Helen auf Nele	09.11.21, 12:19
Nicknamen ändern	Schrödi ;)	Jonas, S9	Änderung des Nicknamens von Schrödi auf Schrödi ;)	09.11.21, 12:19
Nicknamen ändern	MJ	Josefine, iPhone 8	Änderung des Nicknamens von Josefine auf MJ	09.11.21, 12:23
Kontaktname anpassen	Nele	Helen, iPhone SE	Name geändert von Josefine Müller auf Maria Justine	09.11.21, 12:27
Kontaktname anpassen	Schrödi ;)	Jonas, S9	Name geändert von Josefine Müller auf Maria Justine	09.11.21, 12:27
Kontaktname anpassen	Schrödi ;)	Jonas, S9	Name geändert von Helen Zentek auf Nele Neumann	09.11.21, 12:26
Kontaktname anpassen	MJ	Josefine, iPhone 8	Name geändert von Helen Zentek auf Nele Neumann	09.11.21, 12:31
Kontaktname anpassen	MJ	Josefine, iPhone 8	Name geändert von Schrödi Schröder auf Jochen Schreiner	09.11.21, 12:30

Kontaktname anpassen	Nele	Helen, iPhone SE	Name geändert von Schrödi Schröder auf Jochen Schreiner	09.11.21, 12:32
Profilbild geändert	Nele	Helen, iPhone SE	IMG_0577 + Latte Art Blüte	09.11.21, 12:33
Profilbild geändert	Schrödi ;)	Jonas, S9	20211109_123327.jpg + Milchschaum	09.11.21, 12:34
Profilbild geändert	MJ	Josefine, iPhone 8	IMG_0412 + Schrift einer Speisekarte	09.11.21, 12:34

Tabelle 10: Experiment 1: Einzelchats Teil II

Experiment	Kontaktname	Sender/Gerät	Hinzugefügt (Datum/Uhrzeit)	Chat gestartet (Datum/Uhrzeit)
Chat starten	Maria	Jonas, S9 (Jochen)	09.11.21, 12:39	09.11.21, 12:39
Chat starten	Nele	Josefine, 8 (Maria)	09.11.21, 12:40	09.11.21, 12:40
Chat starten	Jochen	Helen, SE (Nele)	09.11.21, 12:41	09.11.21, 12:41

Tabelle 11: Experiment 1: Einzelchats Teil III

Experiment	Chatname	Sender/Gerät	Nachricht	Datum/Uhrzeit
Chat starten	Maria	Jonas, S9 (Jochen)	Hallo	09.11.21, 12:39
Chat starten	Nele	Josefine, 8 (Maria)	Hey	09.11.21, 12:40
Chat starten	Jochen	Helen, SE (Nele)	Moin	09.11.21, 12:41

Tabelle 12: Experiment 1: Einzelchats Teil IV

Experiment	Sender	Empfänger	Nachricht	Datum/Uhrzeit
Nachrichtenaustausch Chat A-B	Nele	Jochen	Moin	09.11.21, 12:41
Nachrichtenaustausch Chat A-B	Jochen	Nele	Hallo :)	09.11.21, 12:43
Nachrichtenaustausch Chat A-B	Nele	Jochen	Ich hab lange nicht von dir gehört.	09.11.21, 12:43
Nachrichtenaustausch Chat A-B	Nele	Jochen	Cool dass du jetzt auch bei Threema bist (Emoji)	09.11.21, 12:43

Nachrichten-austausch Chat A-B	Jochen	Nele	Ja ich wollte es mal testen	09.11.21, 12:44
Nachrichten-austausch Chat A-B	Jochen	Nele	Überzeugt mat mich das aber bisher noch nicht	09.11.21, 12:44
Nachrichten-austausch Chat A-B	Nele	Jochen	Das kommt bestimmt noch	09.11.21, 12:47
Nachrichten-austausch Chat A-B	Nele	Jochen	Fand es am Anfang auch we-niger intuitiv	09.11.21, 12:47
Nachrichten-austausch Chat A-B	Jochen	Nele	Naja wenn du das sagst…	09.11.21, 12:47
Nachrichten-austausch Chat A-B	Jochen	Nele	Ich lass mich mal überraschen	09.11.21, 12:47
Nachrichten-austausch Chat A-B	Nele	Jochen	Immerhin ist hier alles sicher	09.11.21, 12:48
Nachrichten-austausch Chat A-B	Nele	Jochen	Daten und so	09.11.21, 12:48

Nachrichten-austausch Chat A-B	Jochen	Nele	Da bin ich mir nicht so sicher. Aber ich hab davon auch keine Ahnung	09.11.21, 12:49
-----	-------	----------	----------	----------
Nachrichtenaus-tausch Chat B-C	Maria	Nele	Hey	09.11.21, 12:40
	Nele	Maria	Hey :) schön von dir zu hören	09.11.21, 12:52
	Maria	Nele	Jaa lang ist‘s her	09.11.21, 12:52
	Maria	Nele	Wie geht’s (ohne`) dir?	09.11.21, 12:52
	Nele	Maria	Ach ganz okay soweit. Wäre lieber wieder in der Schule als mich durch die Uni zu quälen (Emoji)	09.11.21, 12:54
	Nele	Maria	Dir?	09.11.21, 12:54
	Maria	Nele	Ja ähnlich wie dir	09.11.21, 12:54
	Maria	Nele	Ist aktuell echt stressig	09.11.21, 12:54
	Maria	Nele	Aber was will man machen	09.11.21, 12:55
	Nele	Maria	Ich sehne mich schon nach dem Ende	09.11.21, 12:56
	Nele	Maria	Wie weit bist du mit deinem Studium?	09.11.21, 12:56

	Maria	Nele	Bin jetzt seit knapp zwei Jahren dabei	09.11.21, 12:57
	Maria	Nele	Dauert also noch ne Weile :(	09.11.21, 12:57
---	---	---	---	---
Nachrichtenaustausch Chat A-C	Jochen	Maria	Hallo	09.11.21, 12:39
	Maria	Jochen	Moinsens	09.11.21, 13:01
	Maria	Jochen	Weißt du schon wann du da bist?	09.11.21, 13:02
	Jochen	Maria	Du kennst mich	09.11.21, 13:02
	Jochen	Maria	Bin bissl spät dran	09.11.21, 13:02
	Maria	Jochen	Ich habe nichts anderes erwartet (Emoji)	09.11.21, 13:04
	Maria	Jochen	Dann kann ich ja langsam loslaufen, dann sind wir vielleicht sogar gleichzeitig da	09.11.21, 13:04
	Jochen	Maria	Ich beeil mich auch	09.11.21, 13:04
	Jochen	Maria	Ehrenwort !!	09.11.21, 13:04
	Maria	Jochen	Das hoffe ich für dich	09.11.21, 13:05
	Maria	Jochen	Sonst spendierst du mir einen Kaffee	09.11.21, 13:05

	Jochen	Maria	Ja kann ich machen	09.11.21, 13:06
	Jochen	Maria	Bis gleich	09.11.21, 13:06
---	---	---	---	---
Nachrichtenaus-tausch A-B	Nele	Jochen	Kommst du mittlerweile klar mit Threema?	10.11.2021, 11:18
	Nele	Jochen	Oder überlegst du wieder zu wechseln?	10.11.2021, 11:18
	Jochen	Nele	Also an sich finde ich es ja ganz okay	10.11.2021, 11:18
	Jochen	Nele	Hab nur das Gefühl, dass es langsamer läuft als andere Messenger	10.11.2021, 11:19
	Jochen	Nele	Kommt nur mir das so vor?	10.11.2021, 11:19
	Nele	Jochen	Hmm (Emoji)	10.11.2021, 11:20
	Nele	Jochen	Ist mir nie aufgefallen ehrlich gesagt	10.11.2021, 11:20
	Nele	Jochen	Liegt vielleicht an deinem wlan	10.11.2021, 11:20
	Jochen	Nele	Ne das ist ja das gleiche wie sonst auch	10.11.2021, 11:20

	Jochen	Nele	Ich denke mal ich warte bis Sonntag	10.11.2021, 11:21
	Jochen	Nele	Und dann entscheide ich mich	10.11.2021, 11:21
	Nele	Jochen	Klingt gut	10.11.2021, 11:22
------	---	------	----------	----------
Nachrichtenaus-tausch B-C	Nele	Maria	Sorry für die späte Antwort	10.11.2021, 11:23
	Nele	Maria	Zwei Jahre…	10.11.2021, 11:23
	Nele	Maria	Dann bist doch aber fast fertig	10.11.2021, 11:23
	Maria	Nele	Ja kein Ding	10.11.2021, 11:23
	Maria	Nele	Naja theoretisch schon, aber wenn ich irgendeine Prüfung nicht schaffe dauerts halt noch	10.11.2021, 11:24
	Nele	Maria	Hmm ja klar	10.11.2021, 11:25
	Nele	Maria	Aber bist du bisher gut durch-gekommen?	10.11.2021, 11:25

	Maria	Nele	Ja das schon	10.11.2021, 11:25
	Maria	Nele	Ich hoffe auch, dass es so bleibt	10.11.2021, 11:25
	Maria	Nele	Naja mal sehen wie das Semester wird	10.11.2021, 11:25
	Nele	Maria	Wenn es bisher gut gelaufen ist würde ich mir da mal keine Sorgen machen	10.11.2021, 11:26
	Nele	Maria	Du packst das schon	10.11.2021, 11:26
	Maria	Nele	Danke dir (Emoji)	10.11.2021, 11:27
----------	----------	----------	----------	----------
Nachrichtenaustausch A-C	Jochen	Maria	Hast du mal auf die Uhr geguckt?	10.11.2021, 11:28
	Jochen	Maria	Heute bist du zu spät!!	10.11.2021, 11:28
	Maria	Jochen	Oha was (Emoji)	10.11.2021, 11:28
	Maria	Jochen	Ich habs voll verpeilt	10.11.2021, 11:28
	Maria	Jochen	Ich lieg immer noch im Bett :/	10.11.2021, 11:28

	Jochen	Maria	Unfassbar	10.11.2021, 11:29
	Jochen	Maria	Aber du weißt was das heißt… der nächste Kaffee geht auf dich	10.11.2021, 11:29
	Maria	Jochen	Aber sowas von!	10.11.2021, 11:30
	Maria	Jochen	Tut mir echt leid	10.11.2021, 11:30
	Maria	Jochen	Ich beeile mich	10.11.2021, 11:30
	Maria	Jochen	Bekommst auch noch einen Cookie	10.11.2021, 11:31
	Jochen	Maria	Nagut	10.11.2021, 11:31
	Jochen	Maria	Ich warte dann am gewohnten Ort	10.11.2021, 11:31
	Jochen	Maria	Bis gleich	10.11.2021, 11:31
	Maria	Jochen	Okay, bin schon auf dem Sprung	10.11.2021, 11:32
	Jochen	Maria	(Daumen hoch emojis)	10.11.2021, 11:32

Tabelle 13: Experiment 1: Einzelchats Teil V

Experiment	Chatname	Sender/ Gerät	Medientyp	Dateiname(n) + kurze Inhaltsbeschreibung (oder Originaldatei)	Datum/ Uhrzeit
Medien Senden A-B	Jochen	SE (Nele)	Bild	IMG_0578 + Mops	09.11.21, 13:08
	Nele	S9 (Jochen)	Bild	Haselnuss-fruechte-iStock_78390065.jpg + Haselnusspflanze	09.11.21, 13:09
	Jochen	SE (Nele)	Video	IMG_0579 + Stuhl und Kaffee	09.11.21, 13:13
	Nele	S9 (Jochen)	Video	20211109_131152.mp4 + Kaffee umrühren	09.11.21, 13:14
	Jochen	SE (Nele)	Dokument	DE102015101895A1.pdf + Patent Rückenkratzer	09.11.21, 13:16
	Nele	S9 (Jochen)	Dokument	Q1_FY19_Consolidated_Financial_Statements.pdf	09.11.21, 13:16
	Jochen	SE (Nele)	Standort	Funktioniert nicht	
	Nele	S9 (Jochen)	Standort	Jiraskuv most, 15000 Prag, Tschechische Republik	09.11.21, 13:18
	Nele	S9 (Jochen)	GIF	200w.gif + laufende Katze	09.11.21, 13:21

	Jochen	SE (Nele)	GIF	IMG_0580 + aus der Decke kommende Katze	09.11.21, 13:22
	Nele	S9 (Jochen)	Sprachnachricht	Ich bin gleich da, ich ruf dich dann an	09.11.21, 13:23
	Jochen	SE (Nele)	Sprachnachricht	Besser ist das, ich frier mir hier nämlich den Arsch ab	09.11.21, 13:24
-----	------	-----	---------	------------------------------	---------
Medien Senden B-C	Nele	8 (Maria)	Bild	IMG_0413 + Zuckerturm	09.11.21, 13:26
	Maria	SE (Nele)	Bild	IMG_0581 + Spots	09.11.21, 13:27
	Nele	8 (Maria)	Video	IMG_0428 + fallende Kekstüte	09.11.21, 13:28
	Maria	SE (Nele)	Video	IMG_0582 + Zuckertüten	09.11.21, 13:29
	Nele	8 (Maria)	Dokument	DB_IG_IC_Linie_17_Fahrplantabelle_Mai2020-data.pdf	09.11.21, 13:31
	Maria	SE (Nele)	Dokument	Anleitung_Krawatten_binden.pdf	09.11.21, 13:31
	Nele	8 (Maria)	Standort	Louvre Museum Rue de Rivoli, 75058 Paris	09.11.21, 13:32

	Maria	SE (Nele	Standort	Funktioniert nicht	
	Nele	8 (Maria)	GIF	IMG_0429 + Hund fällt in Pool	09.11.21, 13:34
	Maria	SE (Nele)	GIF	IMG_0583 + Pinguin vs. Pinguin	09.11.21, 13:34
	Nele	8 (Maria)	Sprachnachricht	Mach mal bitte dir Tür auf, es ist kalt	09.11.21, 13:36
	Maria	SE (Nele)	Sprachnachricht	Du könntest auch einfach mal an deinen Schlüssel denken, ist echt nicht so schwer. Aber ja, ich komm.	09.11.21, 13:36
-----	------	-----	----------	----------	----------
Medien Senden A-C	Maria	S9 (Jochen)	Bild	Taxi-rostock-vito.jpg + Taxi	09.11.21, 13:38
	Jochen	8 (Maria)	Bild	IMG_0430 + Löffel	09.11.21, 13:40
	Maria	S9 (Jochen)	Video	20211109_134000.mp4 + drehende Kaffeetasse	09.11.21, 13:41
	Jochen	8 (Maria)	Video	IMG_0431 + Handyhaufen	09.11.21, 13:42
	Maria	S9 (Jochen)	Dokument	2021-11-09-de.pdf	09.11.21, 13:45

	Jochen	8 (Maria)	Dokument	Chocolate-Chip-Cookies.pdf	09.11.21, 13:44
	Maria	S9 (Jochen)	Standort	Nordkapp/North Cape	09.11.21, 13:47
	Jochen	8 (Maria)	Standort	Boulevarden 5, Boulevarden 5, 9000 Aalborg	09.11.21, 13:48
	Maria	S9 (Jochen)	GIF	200.gif + Katze isst Melone	09.11.21, 13:48
	Jochen	8 (Maria)	GIF	IMG_0433 + tanzender Kermit	09.11.21, 13:52
	Maria	S9 (Jochen)	Sprachnachricht	Die Kekse schmecken echt lecker	09.11.21, 13:52
	Jochen	8 (Maria)	Sprachnachricht	Bist du jetzt zum Krümelmonster geworden oder was?	09.11.21, 13:53

Tabelle 14: Experiment 1: Einzelchats Teil VI

Experiment	Chatname	Sender/Gerät	Ergebnis (angenommen, abgelehnt, verpasst)	Beginn Datum/Uhrzeit	Ende Datum/Uhrzeit
Sprachanruf	Nele	S9 (Jochen)	Angenommen	09.11.21, 13:56	09.11.21, 13:57

	Nele	S9 (Jochen)	Abgelehnt	09.11.21, 13:57	09.11.21, 13:57
	Nele	S9 (Jochen)	Verpasst	09.11.21, 13:57	09.11.21, 13:58
	Jochen	SE (Nele)	Angenommen	09.11.21, 13:59	09.11.21, 14:00
	Jochen	SE (Nele)	Abgelehnt	09.11.21, 14:00	09.11.21, 14:00
	Jochen	SE (Nele)	Verpasst	09.11.21, 14:00	09.11.21, 14:01
	Nele	8 (Maria)	Angenommen	09.11.21, 14:04	09.11.21, 14:05
	Nele	8 (Maria)	Abgelehnt	09.11.21, 14:04	09.11.21, 14:04
	Nele	8 (Maria)	Verpasst	09.11.21, 14:02	09.11.21, 14:03
	Maria	SE (Nele)	Angenommen	09.11.21, 14:05	09.11.21, 14:06
	Maria	SE (Nele)	Abgelehnt	09.11.21, 14:06	09.11.21, 14:07
	Maria	SE (Nele)	Verpasst	09.11.21, 14:07	09.11.21, 14:08

	Maria	S9 (Jochen)	Angenommen	09.11.21, 14:08	09.11.21, 14:09
	Maria	S9 (Jochen)	Abgelehnt	09.11.21, 14:10	09.11.21, 14:10
	Maria	S9 (Jochen)	Verpasst	09.11.21, 14:10	09.11.21, 14:11
	Jochen	8 (Maria)	Angenommen	09.11.21, 14:12	09.11.21, 14:13
	Jochen	8 (Maria)	Abgelehnt	09.11.21, 14:13	09.11.21, 14:13
	Jochen	8 (Maria)	Verpasst	09.11.21, 14:13	09.11.21, 14:14
Videoanruf	Nele	S9 (Jochen)	Angenommen	09.11.21, 14:14	09.11.21, 14:15
Videoanruf sieht in Der App ge-nauso Aus wie Sprachan-ruf					

Tabelle 15: Experiment 2: Gruppenchat Teil I

Experiment	Gruppenname	Sender/Gerät	Hinzugefügt (Datum/Uhrzeit)	Chat gestartet (Datum/Uhrzeit)
Gruppe anlegen	A	S9 (Jochen)	09.11.21, 14:17	09.11.21, 14:17
	B	SE (Nele)	09.11.21, 14:18	09.11.21, 14:18
	C	8 (Maria)	09.11.21, 14:19	09.11.21, 14:19

Tabelle 16: Experiment 2: Gruppenchat Teil II

Experiment	Gruppenname	Sender/Gerät	Dateiname(n) + kurze Inhaltsbeschreibung (oder Originaldatei)	Datum/Uhrzeit
Profilbild festlegen	A	S9 (Jochen)	latest.png + Kummer (aus Alles steht Kopf)	09.11.21, 14:20
	B	SE (Nele)	IMG_0584 + schwarzes Loch	09.11.21, 14:21
	C	8 (Maria)	IMG_0434 + Pizza	09.11.21, 14:22

Tabelle 17: Experiment 2: Gruppenchat Teil III

Experiment	Chatname	Sender/Gerät	Nachricht	Datum/Uhrzeit
Nachrichtenaustausch Gruppe A	A	Jochen	Howdy	09.11.21, 14:17
		Maria	Hallo	09.11.21, 14:28
		Nele	Wurde aber auch lang-sam mal Zeit, dass wir ne Gruppe haben	09.11.21, 14:29
		Jochen	Hättest ja auch mal eine erstellen können	09.11.21, 14:30
		Jochen	Aber egal, jetzt haben wir eine	09.11.21, 14:30
		Nele	True	09.11.21, 14:31
		Maria	Mal ne Frage, brauchen wir jetzt noch was?	09.11.21, 14:31
		Maria	Ich hab schonmal Teig und Käse geholt	09.11.21, 14:31
		Nele	Nice	09.11.21, 14:32
		Nele	Ich hab noch Ananas da	09.11.21, 14:32

		Jochen	Hm okay	09.11.21, 14:32
		Jochen	Ich würde noch Mais oder so holen	09.11.21, 14:32
		Maria	Ja das hört sich gut an	09.11.21, 14:33
		Maria	Und vielleicht Salami	09.11.21, 14:33
		Nele	Sehr gut, ich glaube damit können wir arbeiten	09.11.21, 14:34
		Nele	Was hast du für (Käse Emoji)	09.11.21, 14:35
		Maria	Naja so klassischen Reibekäse	09.11.21, 14:35
		Maria	Der ganz vorne im Regal liegt	09.11.21, 14:35
		Jochen	Wenn ich eh einkaufen gehe, soll ich dann speziellen mitbringen?	09.11.21, 14:35
		Nele	So ne Kugel Mozarella wäre cool	09.11.21, 14:36
		Nele	Also mega lieb, wenn du den mitbringst	09.11.21, 14:36

		Jochen	Ja kein Problem	09.11.21, 14:37
		Jochen	Uhrzeit bleibt die selbe?	09.11.21, 14:37
		Maria	Ja so wie immer	09.11.21, 14:37
		Jochen	Ok dann bis später (Daumen hoch Emoji)	09.11.21, 14:37
		Nele	Bis dann	09.11.21, 14:38
---	---	---	---	---
Nachrichten Gruppe B	B	Nele	Joooooo	09.11.21, 14:18
		Nele	Lasst hören, ich will coole wissenschaftliche Facts	09.11.21, 14:39
		Jochen	So aus dem Nichts? Da bin ich überfragt	09.11.21, 14:39
		Maria	Fledermäuse machen knapp 20% aller bekannten Säugetierspezien aus	09.11.21, 14:41
		Jochen	War klar, du weißt sowas natürlich wieder	09.11.21, 14:41

		Nele	Hahaha oha wie krass	09.11.21, 14:42
		Nele	Man kann den Umfang von einem Kreis nie zu 100% genau berechnen	09.11.21, 14:42
		Nele	Weil Pi unendlich ist	09.11.21, 14:42
		Jochen	Was seid ihr bloß für Nerds (Emoji)	09.11.21, 14:43
		Maria	Wir beschäftigen uns halt mit sowas	09.11.21, 14:44
		Maria	Du bist halt einfach ein Langweiler (Emoji)	09.11.21, 14:44
		Jochen	Pass auf..	09.11.21, 14:46
		Jochen	Sonnenuntergänge auf dem Mars erscheinen blau	09.11.21, 14:46
		Jochen	Siehst du ich kann das auch	09.11.21, 14:46
		Nele	Sehr schön. Würde das gerne mal sehen (Emoji)	09.11.21, 14:47

		Maria	Da kannst du wohl leider lange drauf warten (Emoji)	09.11.21, 14:48
		Maria	Aber wenn es soweit ist, nehm mich unbedingt mit	09.11.21, 14:48
----------	-------	----------	----------	----------
Nachrichten Gruppe C	C	Maria	Heyho	09.11.21, 14:19
		Jochen	Hi :-)	09.11.21, 14:49
		Nele	Ah schön, meine Moral Support Gruppe	09.11.21, 14:50
		Nele	Was liegt euch auf dem Herzen, Kinderlein?	09.11.21, 14:51
		Jochen	Ne Selbsthilfegruppe? Finde ich super	09.11.21, 14:51
		Jochen	Also Hallo erstmal, ich bin der Jochen und habe aktuell extrem viel Stress	09.11.21, 14:51
		Jochen	Dadurch kann ich abends schlecht einschlafen. Was kann ich dagegen machen?	09.11.21, 14:52

		Nele	Hallo Jochen	09.11.21, 14:52
		Maria	Hallo Jochen	09.11.21, 14:52
		Maria	Ich kenn das nur zu gut	09.11.21, 14:53
		Maria	Hast du schonmal versucht abends zu meditieren oder warm zu duschen?	09.11.21, 14:53
		Jochen	Ja aber das hat bisher wenig geholfen	09.11.21, 14:53
		Jochen	Ich bin langsam echt überfragt, was ich noch machen kann	09.11.21, 14:54
		Nele	Baldrian kann ich empfehlen	09.11.21, 14:56
		Nele	Das ist eigentlich ne sehr simple Option	09.11.21, 14:56
		Jochen	Nagt dann Probier ich das mal. Ich danke euch	09.11.21, 14:57
		Nele	Mach das :) gibt’s auch im Supermarkt als Tablette	09.11.21, 14:58

| --- | --- | --- | --- | --- |
Nachrichten Gruppe A	A	Nele	Ich hab was bei dir liegen lassen, Maria	10.11.2021, 10:58
		Maria	Ja nicht schlimm	10.11.2021, 10:58
		Maria	Wollte fragen, ob wir heute Abend Restever-wertung machen	10.11.2021, 10:59
		Jochen	Oh jaa	10.11.2021, 10:59
		Jochen	Da bin ich dabei :)	10.11.2021, 10:59
		Nele	Klingt gut	10.11.2021, 10:59
		Nele	Dann kann ich auch gleich meinen Beutel noch mitnehmen	10.11.2021, 11:00
		Maria	Ja der liegt aktuell bei mir neben dem Schrank	10.11.2021, 11:00
		Jochen	Ab wannn können wir kommen?	10.11.2021, 11:00
		Jochen	Wie wäre es ab 19.30?	10.11.2021, 11:00

		Maria	Ja wäre für mich soweit in Ordnung	10.11.2021, 11:01
		Maria	Passt dir das auch Nele?	10.11.2021, 11:01
		Nele	Ich hab noch einen Tme-rin um 19:00 :(	10.11.2021, 11:02
		Nele	Ich würde dann nach kommen	10.11.2021, 11:02
		Nele	Je nachdem wie lange das geht	10.11.2021, 11:02
--------	-------	---------	----------	----------
Nachrichten Gruppe B	B	Nele	Wusstet ihr, dass Maden durch ihr Gesäß atmen	10.11.2021, 11:04
		Nele	Genau wie Schildkröten auch	10.11.2021, 11:04
		Jochen	Oh man jetzt geht das schon wieder los	10.11.2021, 11:04
		Jochen	Was ist bloß los bei euch	10.11.2021, 11:04
		Maria	Lass uns doch	10.11.2021, 11:05
		Maria	Wir sind halt so	10.11.2021, 11:05

		Nele	Man Jochen :(	10.11.2021, 11:06
		Jochen	Ne sorry aber wofür braucht man das??	10.11.2021, 11:06
		Maria	Genau für solche Chats	10.11.2021, 11:06
		Maria	Kannst ja gehen	10.11.2021, 11:06
		Nele	Ist nicht Cleopatra näher an unserer Zeit jetzt dran, als am Bau der Pyramiden?	10.11.2021, 11:06
		Maria	O da habe ich noch nie drüber nachgedacht	10.11.2021, 11:07
		Jochen	…	10.11.2021, 11:07
		Jochen	Alles klar, dann fachsimpelt ihr mal weiter	10.11.2021, 11:07
		Jochen	Ich geh die Sonne genießen (Sonnenbrillen Emoji)	10.11.2021, 11:08
		Nele	Aber immer schön Sonnencreme benutzen	10.11.2021, 11:09

		Nele	Schon ab 5 Sonnenbränden ist das Hautkrebsrisiko um 50% erhöht	10.11.2021, 11:09
----------	----------	----------	----------	----------
Nachrichten Gruppe C	C	Jochen	Leute!!	10.11.2021, 11:10
		Jochen	Ihr werdet es nicht glauben, aber es hat funktioniert	10.11.2021, 11:10
		Maria	Was genau meinst du?	10.11.2021, 11:11
		Jochen	Meine Schlafstörungen sind vorbei	10.11.2021, 11:11
		Nele	Oha wirklich (Emoji)	10.11.2021, 11:11
		Nele	Du hast die Tabletten also ausprobiert?	10.11.2021, 11:12
		Nele	Und es hat direkt geklappt?	10.11.2021, 11:12
		Jochen	Naja so halb würde ich sagen	10.11.2021, 11:12

		Jochen	Könnte aber auch an der Flasche Rotwein gelegen haben (Emoji)	10.11.2021, 11:12
		Maria	Das ist jetzt nicht dein Ernst oder?	10.11.2021, 11:13
		Maria	Wir haben dir doch so viele Tipps gegeben	10.11.2021, 11:14
		Nele	Wenn’s funktioniert (Emoji)	10.11.2021, 11:14
		Nele	Nur nicht zum Alkoholiker werden	10.11.2021, 11:14
		Jochen	Ne eine Flasche am Abend geht schon fit	10.11.2021, 11:15
		Maria	Das glaube ich nicht	10.11.2021, 11:15
		Maria	Überlege dir das bitte nochmal (Emoji)	10.11.2021, 11:15
		Nele	Das ist definitiv zu viel und geht ganz und gar nicht fit	10.11.2021, 11:16
		Jochen	Ihr habt ja keine Ahnung	10.11.2021, 11:16

Tabelle 18: Experiment 2: Gruppenchat Teil IV

Experiment	Gruppenname	Sender/ Gerät	Medientyp	Dateiname(n) + kurze Inhaltsbeschreibung (oder Originaldatei)	Datum/ Uhrzeit
Medien Gruppe A	A	Jochen	Bild	Wide__450x253__mobile__scale_2.jpg + Nordlichter	09.11.21, 15:02
		Maria	Bild	IMG_0435 + Cosmo und Wanda	09.11.21, 15:03
		Nele	Bild	IMG_0585 + Pizza	09.11.21, 15:04
		Jochen	Video	20211109_150535.mp4 + tippen	09.11.21, 15:07
		Maria	Video	IMG_0436 + Kaffeetassen	09.11.21, 15:08
		Nele	Video	IMG_0587 + Fenster Zoom	09.11.21, 15:08
		Jochen	Dokument	Beispiel.pdf	09.11.21, 15:10
		Maria	Dokument	Die_besten_IN_FORM_Salat-Rezepte.pdf	09.11.21, 15:11
		Nele	Dokument	Pizza.pdf	09.11.21, 15:10

		Jochen	Standort	Berliner Straße 1A, 99091 Erfurt, Deutschland	09.11.21, 15:12
		Maria	Standort	Rügen	09.11.21, 15:13
		Nele	Standort	Funktioniert nicht	
		Jochen	GIF	Funny-cat-2020-7.gif + fallende Katze	09.11.21, 15:15
		Maria	GIF	IMG_0437 + Auf dem Rücken liegender Hund	09.11.21, 15:15
		Nele	GIF	IMG_0588 + sitzender Hund	09.11.21, 15:15
		Jochen	Sprachnachricht	Die Katze finde ich am besten	09.11.21, 15:16
		Maria	Sprachnachricht	Also ich persönlich finde den Hund besser	09.11.21, 15:16
		Nele	Sprachnachricht	Welchen Hund? Da sind zwei. Ich find meinen auch sehr gut. Aber der der wiggelt…	09.11.21, 15:17
---	---	---	---	---	---
Medien Gruppe B	B	Jochen	Bild	Squirrel_posing.jpg + Eichhörnchen	09.11.21, 15:20

		Maria	Bild	IMG_0439 + Nüsse in Schale	09.11.21, 15:20
		Nele	Bild	IMG_0590 + Fraktale	09.11.21, 15:21
		Jo-chen	Video	20212209_152312.mp4 + Zuckerpäck-chen	09.11.21, 15:24
		Maria	Video	Zuerst versehentlich zwei Fotos IMG_0442 + Fallender Keks	09.11.21, 15:25
		Nele	Video	IMG_0591 + Kaffee umrühren	09.11.21, 15:22
		Jo-chen	Dokument	Pandas.pdf	09.11.21, 15:26
		Maria	Dokument	Bambus.pdf	09.11.21, 15:27
		Nele	Dokument	Fraktale.pdf	09.11.21, 15:26
		Jo-chen	Standort	Kölnberg 1, 84171 Baierbach, Deutsch-land	09.11.21, 15:27
		Maria	Standort	Spiekeroog Spieekeroog	09.11.21, 15:28
		Nele	Standort	Funktioniert nicht	

		Jo-chen	GIF	Chipmunk-nuts.gif + Streifenhörnchen isst Nuss	09.11.21, 15:28
		Maria	GIF	IMG_0438 + Hund im Raumschiff	09.11.21, 15:29
		Nele	GIF	IMG_0589 + Hund weckt Herrchen	09.11.21, 15:29
		Jo-chen	Sprachnach-richt	War der Hund wirklich im Weltall?	09.11.21, 15:31
		Maria	Sprachnach-richt	Nein, ist alles gefotoshoppt	09.11.21, 15:31
		Nele	Sprachnach-richt	Das ist bestimmt so ne Simulation gewe-sen	09.11.21, 15:32
------	---------- --	-------	----------	----------	----------
Me-dien Gruppe C	C	Jo-chen	Bild	20211110_102221.jpg + Bücher	10.11.21, 10:26
		Maria	Bild	IMG_0443 + Buchrücken	10.11.21, 10:26
		Nele	Bild	IMG_0592 + Treppe in der Hochschulbibli-othek	10.11.21, 10:24

		Jo-chen	Video	20211110_102224.mp4 + Bücher	10.11.21, 10:37
		Maria	Video	IMG_0444 + Video von Büchern	10.11.21, 10:32
		Nele	Video	IMG_0593 + Video von Büchern	10.11.21, 10:30
		Jo-chen	Dokument	2017_Umgang_mit_Fachliteratur_web-site.pdf	10.11.21, 10:38
		Maria	Dokument	Dmb_wohnungsvermietung.pdf	10.11.21, 10:38
		Nele	Dokument	Geschichte_Stadtbibliothek1.pdf	10.11.21, 10:38
		Jo-chen	Standort	Thistedvej 671, 9690 Fjerritslev Dänemark	10.11.21, 10:39
		Maria	Standort	Hiddensee, Hiddensee	10.11.21, 10:40
		Nele	Standort	Funktioniert nicht	
		Jo-chen	GIF	Cute-cat.gif + süße Katze	10.11.21, 10:42
		Maria	GIF	IMG_0446 + Dicke Tiere jagen sich	10.11.21, 10:41
		Nele	GIF	IMG_0594 + lesender Hund	10.11.21, 10:40

		Jo-chen	Sprachnach-richt	JO, der Gepard ist ja mal richtig fett	10.11.21, 10:43
		Maria	Sprachnach-richt	Leute, ich kann mir die Sprachnachrichten erst nachher anhören	10.11.21, 10:44
		Nele	Sprachnach-richt	Das Video ist schon so alt	10.11.21, 10:43

Tabelle 19: Experiment 2: Gruppenchat Teil V

Experi-ment	Gruppen-name	Sender/Gerät	Typ (Bild m. Text)	Dateiname(n) + kurze Inhaltsbeschreibung (oder Originaldatei)	Datum/Uhrzeit
	A	Jochen	Bild mit Text	20211110_104506.jpg + Bücher Wo sind die anderen Bücher?	10.11.2021, 10:48
	B	Jochen		20211110_104507.jpg + Bücherregal Das sortieren ist sicher anstrengend	10.11.2021, 10:51
	C	Jochen		20211110_104509.jpg + Raum Die Sonne lacht (Son-nenbrillen Emoji)	10.11.2021, 10:55

	A	Maria		IMG_0448 + Lampen Da ist ne Lampe kaputt	10.11.2021, 10:49
	B	Maria		IMG_0449 + Bücher (verschwommen) Soo viele Bücher wtf	10.11.2021, 10:52
	C	Maria		IMG_0450 + Bücher Kann ich nur empfehlen (Emoji)	10.11.2021, 10:54
	A	Nele		IMG_0595 + Ekel aus Alles steht Kopf Ist ja peinlich	10.11.2021, 10:50
	B	Nele		IMG_0596 + Wut aus Alles steht Kopf Ich. Will. KEKSE	10.11.2021, 10:51
	C	Nele		IMG_0597 + Angst aus Alles steht Kopf Ich hab Angst, Leute	10.11.2021, 10:54

Tabelle 20: Experiment 2: Gruppenchat Teil VI

Experiment	Gruppenname	Sender/Gerät	Titel/Thema, Auswahlmöglichkeiten & Ergebnis	Datum/Uhrzeit
Umfrage	A	Jochen	Welches ist dein Lieblings Char ? Kummer, Wut, Ekel, Freunde, Angst & 1*Kummer, 2*Wut	09.11.21, 15:32
	B	Nele	Bestes Pizza Topping, Ananas, Nichts, mehr Ananas, 1*Ananas, 1*Nichts, 1*mehr Ananas	09.11.21, 15:37
	C	Maria	Wo gehen wir essen? Hier, da, dort 1*Hier, 1*Da, 1*Dort	09.11.21, 15:38

Selbständigkeitserklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbständig und nur unter Verwendung der angegebenen Literatur und Hilfsmittel angefertigt habe.

Stellen, die wörtlich oder sinngemäß aus Quellen entnommen wurden, sind als solche kenntlich gemacht.

Diese Arbeit wurde in gleicher oder ähnlicher Form noch keiner anderen Prüfungsbehörde vorgelegt.

Mittweida, den 4. Oktober 2023