FAST DETECT
SACHVERSTÄNDIGENBÜRO
FÜR IT-FORENSIK

HOCHSCHULE
MITTWEIDA
University of Applied Sciences

BACHELORARBEIT

Frau
Yasmin Scheithauer

Der soziale Netzwerkdienst Threads im Kontext der forensischen Analyse von Android-Geräten

Mittweida, Januar 2024

Fakultät **Angewandte Computer- und Biowissenschaften**

BACHELORARBEIT

Der soziale Netzwerkdienst Threads im Kontext der forensischen Analyse von Android-Geräten

Autorin:
Yasmin Scheithauer

Studiengang:
Allgemeine und Digitale Forensik

Seminargruppe:
FO20w5-B

Erstprüfer:
Prof. Ronny Bodach

Zweitprüfer:
Paul Prade, M.Sc.

Einreichung:
Mittweida, 07.01.2024

Verteidigung/Bewertung:
Mittweida, 2024

Faculty of **Applied Computer Sciences and Biosciences**

BACHELOR THESIS

The Threads social networking service in the context of Android device forensic analysis

Author:
Yasmin Scheithauer

Course of Study:
General and Digital Forensics

Seminar Group:
FO20w5-B

First Examiner:
Prof. Ronny Bodach

Second Examiner:
Paul Prade, M.Sc.

Submission:
Mittweida, 07.01.2024

Defense/Evaluation:
Mittweida, 2024

Bibliografische Beschreibung:

Scheithauer, Yasmin:
Der soziale Netzwerkdienst Threads im Kontext der forensischen Analyse von Android-Geräten. – 2024. – 52 S.
Mittweida, Hochschule Mittweida – University of Applied Sciences, Fakultät Angewandte Computer- und Biowissenschaften, Bachelorarbeit, 2024.

Referat:

Ziel dieser Arbeit ist es, die Ablagestruktur des sozialen Netzwerkdienstes Threads durch forensische Analysen an Android-Geräten zu untersuchen. Die Testdaten werden mit Hilfe von zwei Android-Smartphones generiert. Auf einem der Mobilgeräte werden Root-Rechte aktiviert, um Zugriff auf die Anwendungsdaten von Threads zu erhalten. Die Root-Rechte ermöglichen einen permanenten Zugriff auf Anwendungsdaten, wodurch ein mehrmaliges Auslesen der Anwendungsdaten ohne hohen Zeitaufwand möglich und somit eine detailreiche Analyse realisierbar ist. Das zweite Mobilgerät wird einer Informationstechnologie (IT)-forensischen Extraktion mittels UFED Touch2 unterzogen. Aus dieser Extraktion wird anschließend ein UFED-Bericht generiert, welcher Informationen zu Anwendungen beinhaltet, die auf dem Gerät verwendet wurden. Aus der Analyse soll hervorgehen, welche Anwendungsdaten von Threads in den UFED-Bericht einfließen. Die Literaturrecherche zeigte, dass bisher keine wissenschaftlichen Arbeiten zur Anwendung Threads veröffentlicht wurden. Infolgedessen soll der Fokus der Analysen auf Ablagestruktur und Informationen zum Nutzerkonto sowie Aktionen, wie das Teilen von Beiträgen oder Verfassen von Kommentaren, liegen.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

AOSP . . . . . Android Open Source Project

DB . . . . . Database

DBMS . . . . . Database Management System

DNS . . . . . Domain Name System

DSGVO . . . . . Datenschutzgrundverordnung

EU . . . . . Europäische Union

FTP . . . . . File Transfer Protocol

Gzip . . . . . GNU Zip

HTTP . . . . . Hypertext Transfer Protocol

ID . . . . . Identifier

IT . . . . . Informationstechnologie

JFIF . . . . . JPEG File Interchange Format

JPEG . . . . . Joint Photographic Experts Group

JSON . . . . . JavaScript Object Notation

LAN . . . . . Local Area Network

MPEG . . . . . Moving Picture Experts Group

OpenGL / **ES** . . . . . Open Graphics Library for Embedded Systems

PC . . . . . Personal Computer

PNG . . . . . Portable Network Graphic

QR . . . . . Quick Response

SFTP . . . . . sicheres Dateiübertragungsprotokoll

SHM . . . . . Shared Memory

SMS . . . . . Short Message Service

SQL . . . . . Structured Query Language

SSH . . . . . Secure Shell

TV . . . . . Television

UFDR . . . . . UFED Physical Analyzer Report Package

UFED . . . . . Universal Forensics Extraction Device

URL . . . . . Uniform Resource Locator

USB . . . . . Universal Serial Bus

VPN . . . . . Virtual Private Network

WAL . . . . . Write Ahead Log

WLAN . . . . . Wireless Local Area Network

XML . . . . . Extensible Markup Language

1 Einleitung

Die digitale Welt ist für viele Menschen mittlerweile zu einem festen Bestandteil des Lebens geworden - egal ob im Berufsalltag oder bei Freizeitaktivitäten. Insbesondere die Verwendung von sozialen Netzwerken ist verbreitet [1]. Soziale Netzwerke werden bevorzugt zum Erstellen, Teilen oder Kommentieren und Bewerten von Beiträgen verwendet [2]. Derartige Plattformen gibt es in unterschiedlichen Ausführungen, die verschiedenen Zwecken dienen. Die gängigste Funktion, welche ein Großteil der sozialen Plattformen anbietet, ist der Austausch von Texten, Bildern und Videos. In welchem Rahmen Funktionen angeboten werden, hängt vom zu erfüllenden Zweck der Plattform ab. Sehr beliebte soziale Plattformen z.B. Instant Messenger (Dienste für den sofortigen Nachrichtenversand), wie WhatsApp, Signal oder Telegram [3]. Aber auch Microblogging-Dienste, wie X (ursprünglich Twitter), sollten nicht vernachlässigt werden [4]. Der Begriff Microblogging wird in Abschnitt 2.1.1 näher erläutert.

1.1 Beschreibung der Problematik

Aus dem Bundeslagebild des Bundeskriminalamtes aus dem Jahr 2022 geht hervor, dass rund 30 Prozent der registrierten Straftaten, die im Internet begangen wurden, aufgeklärt werden konnten [5]. Für die Ermittlungsbehörden sind bei der Fallaufklärung jedoch nicht nur Spuren relevant, welche unmittelbar durch das Begehen der Straftat entstehen. Auch die Spuren, aus denen hervorgeht, wie, wo und durch wen eine Straftat geplant wurde, können maßgeblich zur Aufklärung beitragen. Für die Planung einer Straftat können insbesondere Text-, Bild- und Videoübermittlungsfunktionen verschiedener Anwendungen missbräuchlich verwendet werden. Aus diesem Grund kann es für den Ermittlungsverlauf hilfreich sein, wenn Mitwirkende, wie Informationstechnologie (IT)-Analysten, bereits im Voraus Kenntnisse über die Speicherstrukturen einer Anwendung besitzen.

Threads ist eine seit Juli 2023 veröffentlichte Plattform, zu der bisher keine wissenschaftlichen Arbeiten existieren. Bereits kurz nach Veröffentlichung soll Threads eine große Anzahl an Nutzern aufgewiesen haben. Verschiedene Quellen berichten von ca. 70 Millionen registrierten Nutzern in 48 Stunden. [6–8]

Obwohl Threads als X / Twitter-Konkurrent bezeichnet wird, können die Nutzerzahlen bisher nicht an die von X heranreichen. Im Juli 2023 lag die Anzahl der täglich aktiven Threads-Nutzer bei knapp 13 Millionen, die X-Nutzer hingegen bei fast 106 Millionen [9]. Die Plattform Threads wurde innerhalb der Europäischen Union (EU) auf Grund von Verstößen gegen die Datenschutzgrundverordnung (DSGVO) lange Zeit nicht zugelassen. Dies gilt auch für den Zeitraum, in dem die Testdaten erhoben wurden. Die Freigabe der Anwendung im EU-Inland erfolgte am 14.12.2023 und könnte einen weiteren Anstieg der Nutzerzahlen bewirken. [10–12]

Zudem wurden Entwicklungen weiterer Threads-Funktionen, wie eine erweiterte Suchfunktion oder die Einführung des Erwähnens anderer Nutzerkonten in einem Bild- oder Video-Beitrag, angekündigt. Auch dies ist eine Möglichkeit, durch die Threads Aufmerksamkeit und somit höhere Nutzerzahlen generieren könnte. [13]

1.2 Motivation und wissenschaftliche Relevanz

Die Datenmengen, welche IT-Analysten nach dem Erfüllen eines Straftatbestandes im digitalen Rahmen auswerten, können mehrere Terabyte umfassen. Auf Grund dieser Menge an Daten wurde das Konzept zur Priorisierung der Datenauswertung entwickelt. Dieses gibt vor, in welcher Reihenfolge Daten sinnvoll gesichert und ausgewertet werden. Das Ziel besteht darin, die Daten im Vorfeld auf eine priorisiert auszuwertende Datenmenge zu beschränken. Die Wahrscheinlichkeiten, die beschreiben, wo vermehrt bzw. kaum relevante Daten zu erwarten sind, werden als Basis zur Bestimmung der Prioritäten-Liste verwendet. Die Formulierung allgemeingültiger Kriterien, nach welcher eine Priorisierung stattfindet, stellt sich auf Grund der individuellen Fälle jedoch als diffizil heraus. [14]

Die aus dieser Arbeit hervorgehenden Ergebnisse können bei der Erstellung einer solchen Prioritätenliste unterstützend wirken. Die zu erwartenden Nutzerdaten von Threads könnten folglich besser eingeordnet werden.

1.3 Zielstellung

Die Betrachtung des aktuellen Forschungsstandes ergab, dass bis zum momentanen Zeitpunkt keine wissenschaftlichen Arbeiten zum sozialen Netzwerkdienst Threads veröffentlicht wurden. Im Zuge dessen soll diese Arbeit eine Grundlage für mögliche weitere Forschungen zum Thema Threads bieten. Um als Grundlage dienen zu können, werden Threads-Testdaten an Mobilgeräten mit dem Betriebssystem Android generiert, da Android ein weit verbreitetes Betriebssystem ist. 2019 hatte Android einen globalen Marktanteil von fast 75 Prozent der Smartphone-Betriebssysteme [15]. Die Testdaten sollen anschließend extrahiert und einer IT-forensischen Analyse unterzogen werden.

Im Fokus der Testdaten-Analyse sollen Datenbanken, XML-Dateien, Cache-Dateien und die allgemeine Ablagestruktur der Threads-Daten stehen, um einen Überblick der durch Threads hinterlegten Daten zu generieren. Folgende Informationen und Erkenntnisse sollen aus dieser Arbeit hervorgehen:

- Angaben zum Nutzerkonto
- individuelle Einstellungen des Nutzerkontos
- Aktivitäten des Nutzerprofils
- Interaktionen mit anderen Nutzerprofilen
- Verknüpfung von Bildern / Videos mit Nutzerprofilen

Des Weiteren wird eine forensische Extraktion eines Smartphones erfolgen, um die Analyse eines automatisiert generierten UFED-Berichtes durchführen zu können. Daraus soll hervorgehen, inwiefern und in welchem Umfang Anwendungsdaten der Anwendung Threads erkannt und interpretiert werden.

1.4 Literaturübersicht des aktuellen Forschungsstandes

Auf Grund der Tatsache, dass Threads zum aktuellen Zeitpunkt erst wenige Monate verfügbar ist, steht bisher nur wenig Literatur zur Verfügung. Wissenschaftliche Arbeiten bzgl. Nutzungsspuren (Artefakten), die bei der Verwendung von Threads durch den Nutzer entstehen, wurden in der Ver-

gangenheit nicht veröffentlicht. Da Threads jedoch aus der Anwendung Instagram hervorgeht und beide Anwendungen durch denselben Konzern Meta Platforms, Inc. entwickelt werden [16], wäre es möglich, dass die Speicherstrukturen von Threads auf denen von Instagram basieren und dementsprechend ähnlich sein könnten.

Informationen zur Instagram-Speicherstruktur finden sich in mehreren Arbeiten. Das Kapitel '*Investigating Instagram Privacy Through Memory Forensics*' (Untersuchung der Instagram-Privatsphäre durch Speicher-Forensik) aus dem Buch '*Intelligent Computing*' (Intelligente Datenverarbeitung) von Kohei Arai beschäftigt sich mit Instagram-Artefakten durch die Nutzung von Instagram im Webbrowser. Es erfolgte eine Speicherauswertung, aus der Informationen zum Nutzerkonto und dessen Instagram-Aktivitäten hervorgingen. [17]

Der Artikel '*Forensic Analysis of Instagram on Android*' (Forensische Analyse von Instagram auf Android) beinhaltet Informationen von Instagram-Artefakten im Speicher von Android-Geräten. Dabei wird auf Verzeichnisstrukturen und deren Inhalte eingegangen. [18]

Quellen zum Thema Threads selbst beinhalten zum Großteil ähnliche Informationen. Darin werden meist Funktionen der Anwendung beschrieben. Des Weiteren wird darauf eingegangen, welche Funktionen in Zukunft hinzukommen werden. Der Artikel '*Prospect of Threads in Contrast to Twitter as an Online Social Network Tool for Conflict Resolution*' (Die Perspektive von Threads im Vergleich zu Twitter als soziales Online-Netzwerk-Tool zur Konfliktlösung) bspw. enthält allgemeine Informationen über die Anwendung Threads sowie Funktionserläuterungen. Zudem werden die Funktionen von X und Threads gegenübergestellt. [19]

In verschiedenen Quellen wird außerdem diskutiert, inwiefern Threads zum X-Konkurrenten werden könnte. Die Medien erwähnen in dieser Hinsicht vermehrt die Übernahme der X-Plattform durch Elon Musk und den damit einhergehenden Veränderungen, welche verstärkt negative Reaktionen hervorriefen. Infolgedessen erhoffe sich der Meta-Konzern mit Threads eine Alternative zur Verfügung zu stellen, an der unzufriedenen X-Nutzer Interesse finden. [20–22]

Threads in der hier beschriebenen Form gibt es seit Juli 2023. Jedoch existierte die Anwendung bereits vor einigen Jahren in einer anderen Ausführung. Ebenfalls durch Meta entwickelt, existierte Threads bis 2021 als eine Art Messenger Service (Nachrichten-Dienst). Die damalige Anwendung fungierte ähnlich wie Facebook Messenger. Direkt-Nachrichten aus Instagram konnten in Threads gesendet und empfangen werden. Da die Funktionen von Instagram, WhatsApp und Facebook Messenger jedoch immer ähnlicher wurden und somit das Angebot einer weiteren Anwendung dieser Form nicht sinnvoll erschien, entschied sich der Konzern im Jahr 2021 die Nutzung von Threads einzustellen. Daraufhin erfolgte eine Umgestaltung der Anwendung. Auch zum Threads-Vorgänger gingen keine wissenschaftlichen Erkenntnisse aus der Literaturrecherche hervor. [23]

2 Technische Grundlagen

Das Kapitel ‘Technische Grundlagen‘ befasst sich mit dem nötigen Hintergrundwissen, auf dem die weitere Auswertung basiert. Dabei wird zuerst auf die betrachtete Anwendung Threads und deren Funktionen eingegangen. Es folgt eine Erläuterung von virtuellen privaten Netzwerken (VPN), welche zur Nutzung der Anwendung nötig sind. Auf auszuwertende Dateiformate sowie das verwendete Betriebssystem Android wird anschließend eingegangen. Zuletzt folgt eine Erläuterung möglicher Methoden zur IT-forensischen Datensicherung der Mobilgeräte.

2.1 Threads

Die Anwendung Threads vom US-amerikanischen Internetkonzern Meta Platforms, Inc., veröffentlicht am 05.07.2023 durch Mark Zuckerberg, ist ein soziales Netzwerk zum Teilen von Texten, Bildern oder Videos. Die Anwendung wird für iOS- und Android-Betriebssysteme sowie als Weboberfläche entwickelt. Ausgelegt wurde die Plattform für die öffentliche Kommunikation und Diskussion vielfältiger Themen. Im Folgenden wird die Plattform näher betrachtet. [24, 25]

2.1.1 Microblogging

Threads fungiert wie ein Mikro-Blog, d.h. es werden Textbeiträge von geringem Umfang, Bilder, Links oder auch Videos in einem chronologisch geordneten Blog dargestellt. Die Veröffentlichung von kurzen, eher informellen Nachrichten dient dazu, schnell und ohne großen Aufwand Inhalte mit anderen Threads-Nutzern zu teilen. Das Erstellen von Mikro-Blogs, auch Microblogging genannt, eignet sich vor allem für mobile Endgeräte. [26, S. 37]

2.1.2 Funktionen

Threads erleichtert den Austausch verschiedener Inhalte mit Freunden oder Familie. Die Plattform bietet jedoch auch die Möglichkeit, sich mit Personen weltweit zu vernetzen, welche z.B. die gleiche Meinung teilen oder ähnliche Interessen besitzen. Im Folgenden wird auf die Funktionsmöglichkeiten der Anwendung Threads eingegangen. Ein Großteil der Informationen dieses Abschnittes wurde erhoben, indem die Plattform installiert und durch Testen genauer betrachtet wurde. Anzumerken ist hierbei, dass Threads, im Gegensatz zu ähnlichen Anwendungen, keine Möglichkeit zum Austausch von Direkt-Nachrichten bietet. Threads steht als reine Microblogging-Plattform zur Verfügung.

2.1.2.1 Aufbau der Oberfläche

Die Nutzeroberfläche von Threads besteht aus fünf Hauptseiten, zwischen denen mit einem Klick auf das entsprechende Symbol aus Abbildung 2.1 gewechselt werden kann. Die Symbolleiste ist am unteren Bildschirmrand der Anwendung zu finden. Wie die Hauptseiten aufgebaut sind, zeigt Abbildung 2.2.

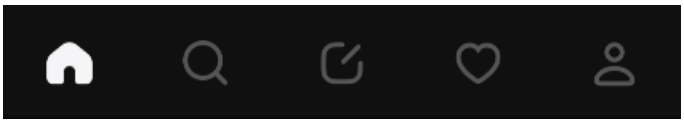

Abbildung 2.1: Threads-Symbolleiste

Haus

Mittels Klick auf das Haus-Symbol öffnen sich die »Für dich«- und die »Gefolgt«-Seite. Auf diesen Seiten werden Beiträge von anderen Nutzern angezeigt. Die »Für dich«-Seite gibt Inhalte wieder, die dem Nutzer gefallen könnten. Die »Gefolgt«-Seite beinhaltet empfohlene Beiträge von Nutzerkonten, denen der Nutzer folgt [27]. Nach welchen spezifischen Kriterien der Algorithmus Inhalte empfiehlt, ist nicht ersichtlich.

Lupe

Das Lupen-Symbol steht stellvertretend für die Suchfunktion, mit welcher nach Nutzernamen oder spezifischen Inhalten gesucht werden kann. Werden nach Eingabe eines Suchbegriffs ein oder mehrere Treffer angezeigt, gelangt man durch einen Klick auf den Treffer zum jeweiligen Profil bzw. Beitrag.

Notizzettel mit Stift

Durch das Notizzettel-Symbol öffnet sich eine Vorlage, um einen neuen Threads-Beitrag zu erstellen.

Herz

Die mit dem Herz-Symbol gekennzeichnete Seite beinhaltet Informationen zu Aktivitäten. Darunter zählen Anfragen, Antworten, Erwähnungen, Zitate und Reposts. Unter einem Repost wird das Teilen bzw. das erneute Hochladen eines bereits existierenden Threads verstanden.

Person

Durch das Person-Symbol sind Informationen zum eigenen Profil, wie der vollständige Name, der Nutzername oder die Anzahl der Personen, die dem eigenen Profil folgen, aufrufbar. Auch der Thread-Verlauf (chronologischer Verlauf der Beiträge), Antworten und Reposts (erneutes Teilen von Beiträgen anderer Nutzerkonten) des eigenen Nutzerkontos sind auf dieser Seite gelistet. [28]

2.1.2.2 Verfasser eines Beitrags

Ein Beitrag, in diesem Kontext auch Thread genannt, kann aus Text, Bildern, Videos oder einer Kombination daraus bestehen. Zudem können bereits existierende Threads / Beiträge zitiert, Threads-Konten erwähnt oder Links einem Beitrag beigefügt werden. [27]

2.1.2.3 Einstellungen eines verfassten Beitrags

Als Verfasser eines Beitrags kann die Anzahl der »Gefällt mir«-Angaben verborgen werden. Außerdem kann bestimmt werden, wer auf den Thread antworten darf: jede Person, gefolgten Personen oder erwähnte Personen. [27]

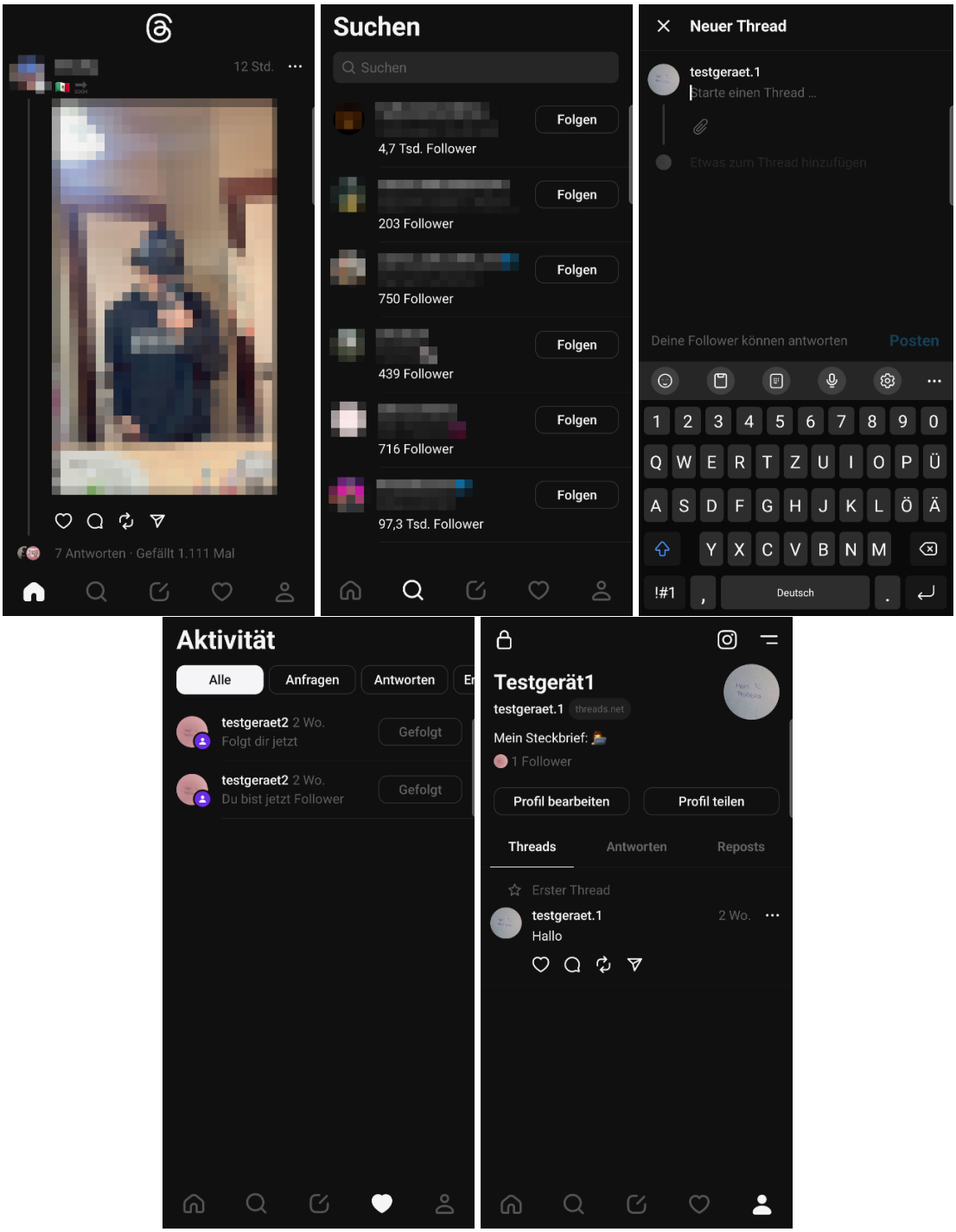

Abbildung 2.2: Hauptseiten von Threads

2.1.2.4 Einstellungen zum Nutzerkonto

Ein Profil besteht aus Profilbild, Steckbrief und Verlinkung. Diese Angaben können individuell gestaltet und jederzeit geändert werden. Ein Nutzerkonto kann privat oder öffentlich geführt werden. Der Unterschied besteht darin, dass bei einem privaten Konto erst eine Bestätigung der Follow (Folge)-Anfrage erfolgen muss, bevor der andere Threads-Nutzer die Inhalte des eigenen (privaten) Threads-Kontos sehen kann. Bei öffentlichen Nutzerprofilen können Beiträge ohne Bestätigung aufgerufen werden. Die Anzahl der »Gefällt mir«-Angaben können global für das eigene Nutzerkonto verborgen werden. Diese Option ist jedoch mit dem Instagram-Konto verknüpft, wodurch bei Deaktivierung der Funktion die »Gefällt mir«-Angaben weder auf Threads noch auf Instagram zu sehen sind. Des Weiteren besteht die Möglichkeit, die bereits auf Instagram gefolgten Nutzer zu importieren, sodass auf Threads denselben Nutzern wie auch auf Instagram gefolgt wird. Personen, welche die Anwendung Threads nicht nutzen, können via Instagram, SMS (Short Message Service) oder E-Mail (elektronische Post) aufgefordert werden, Threads beizutreten. Des Weiteren kann festgelegt werden, welche Nutzer das eigene Nutzerkonto erwähnen dürfen: niemand, jeder oder ausschließlich Nutzer, denen man selbst folgt. Außerdem kann eine Standard- oder individuelle Liste mit Worten angelegt und aktiviert werden, um Kommentare bzw. Antworten, die Worte dieser Liste enthalten, für Nutzer die dem eigenen Nutzerkonto nicht folgen auszublenden. Diese Liste kann aus Beleidigungen oder anderen unerwünschten Begriffen bestehen. Optional sind auch Benachrichtigungseinstellungen individuell wählbar, welche jedoch entsprechend den Standard-Einstellungen unverändert bleiben, da das Testen dieser Funktionen für diese Arbeit nicht notwendig ist. [27, 29]

2.1.2.5 Betrachter eines Threads

Der Betrachter kann durch eine »Gefällt mir«-Angabe den Beitrag als positiv bewerten oder eine individuelle Antwort bzw. Kommentar verfassen. Auch das Antworten auf einen Kommentar ist möglich, wodurch eine Antwort-Hierarchie entsteht. Antworten, die auf einen Beitrag verweisen entsprechen somit der Antwort-Ebene 1 und Antworten, die auf Kommentare der Ebene 1 verweisen entsprechen der Antwort-Ebene 2. Außerdem besteht die Option, einen Beitrag zu melden, wenn der Inhalt bspw. gegen die Nutzungsrichtlinien verstößt. Ein Beitrag kann zudem erneut geteilt werden. Die Plattformen Threads und Instagram sind miteinander verknüpft, weshalb Beträge von Threads auf verschiedene Weisen auch auf Instagram geteilt werden können. Bspw. kann ein Thread als Instagram Direct Message (dt.: Direktnachricht) versendet, als Instagram-Beitrag oder als Instagram-Story hochgeladen werden. [27]

2.1.2.6 Andere Nutzerkonten

Andere Nutzerkonten können stummgeschaltet, eingeschränkt oder blockiert werden. Zudem besteht die Möglichkeit, anderen Nutzern zu folgen. Inhalte, ausgehend von den gefolgten Nutzerkonten, können dann auf der »Gefolgt«-Seite erscheinen. [27, 29]

2.1.2.7 Löschen und Zurücksetzen von Aktionen

Nach dem Erstellen bzw. Hochladen eines Threads kann dieser auch gelöscht werden. Eine ‘Gefällt mir‘-Angabe kann zurückgezogen werden. Auch die Blockierung, Stummschaltung oder Einschränkung eines Nutzerkontos können aufgehoben werden. Eigene Antworten oder Reposts können ebenfalls gelöscht werden. [27]

2.2 Virtual Private Network

Mit Hilfe eines VPN, ist es möglich verschlüsselte Datenpakete über ein öffentliches bzw. nicht privates Netzwerk zu transportieren. Dafür wird ein Tunneling-Protokoll verwendet, mit dessen Hilfe die verschlüsselten Datenpakte über das öffentliche Netzwerk übertragen werden können. Ein Vorteil einer VPN-Verbindung ist, dass der Netzwerkverkehr verschlüsselt ist und die übertragenen Daten dem Internetanbieter somit verborgen bleiben. Zusätzlich erschwert die Verschlüsselung des Datenverkehrs das Ausspähen von Daten durch Hackerangriffe. [30, S. 79–80]

Zum Erheben der Testdaten wurde eine VPN-Verbindung verwendet, um den tatsächlichen Geräte-Standort zu verbergen, da eine Nutzung von Threads zum Zeitpunkt der Testdatengenerierung innerhalb der EU nicht freigegeben und die Anwendung daher nicht vollumfänglich zur Verfügung stand. [11, 31]

2.3 Spuren im digitalen Kontext

Edmond Locard, ein französischer Arzt und Kriminologe, galt als Pionier der forensischen Wissenschaft und formulierte das Locard‘sche Austauschprinzip, welches besagt, dass ein Kontakt zwischen Objekten nicht ohne Kontamination stattfinden könne [32]. Diese Formulierung bezieht sich auf die physische Spurenwelt, gilt jedoch auch gewissermaßen an einem digitalen Tatort. Digitale Spuren werden dabei als Daten definiert, welche in Computersystemen gespeichert oder übertragen wurden. Der Entstehungsprozess von digitalen Spuren findet nicht, wie es bei Begehung einer Straftat in der realen Welt üblich ist, an einem lokalen, sondern an mehreren Orten statt.

An der Datenentstehung, -übermittlung und -speicherung sind drei zusammenhängenden Komponenten beteiligt, anhand derer digitale Spuren aufzufinden sind. Zu den drei Komponenten gehören das Internet, LAN (Local Area Network) oder WLAN (Wireless Local Area Network) und das Kerngerät. Kerngeräte können u.a. PCs, Tablets oder, wie in dieser Ausarbeitung, die verwendeten Mobiltelefone sein. Die Analyse bezieht sich in diesem Rahmen ausschließlich auf die Daten der Kerngeräte. [33, S. 114–118]

2.3.1 Datenbanken

Die folgenden Abschnitte beschäftigen sich mit der Thematik Datenbanken. Dabei wird auf die Definition und verschiedene Datenbank-Modelle eingegangen. Anschließend wird das Datenbank-Format, welches für die vorliegende Ausarbeitung relevant ist, erläutert.

2.3.1.1 Definition von Datenbanken

Eine Datenbank beinhaltet eine Menge an Daten, die in einem logischen Zusammenhang stehen. Die Verwaltung einer Datenbank übernimmt ein Datenbankverwaltungssystem (engl.: Database Management System (DBMS)). Ein Datenbank-Managementsystem ist eine Software, die Zugriff auf Datenbanken verwaltet. Der Nutzer kann dadurch Datenbanken erstellen, lesen, ändern oder löschen sowie Daten einpflegen. [34, S. 3]

2.3.1.2 Datenbankmodelle

Datenbanken können sich in ihrem Aufbau voneinander unterscheiden und werden daher in verschiedene Modelle unterteilt. Dazu gehören bspw. das relationale, das Netzwerk- oder das hierarchische Datenbank-Modell. [35, S. 115–156]

Im Zuge dieser Analysen weisen ausschließlich relationale Datenbanken eine wesentliche Relevanz auf, weshalb dieses Datenbank-Modell im Folgenden näher betrachtet wird. Durch ein relationales Datenbank-Modell können Daten in Form von Relationen organisiert werden. Eine Relation ist eine zweidimensionale Tabelle mit einer konstanten Anzahl an Spalten und beliebig vielen Zeilen, in der sich alle Entitätstypen darstellen lassen. Dabei entspricht eine Zeile einer Tabelle einem Datensatz. Die Spalten enthalten Attribute, welche sich auf Eigenschaften und Merkmale von Entitäten beziehen. Die Identifizierung eines Datensatzes erfolgt über den Primärschlüssel, welcher sich aus einem oder mehreren Attributen zusammensetzt. Ein Primärschlüssel bleibt unverändert und sollte minimal sein, d.h. aus so vielen Attributen wie nötig und so wenigen Attributen wie möglich bestehen, um die eindeutige Identifikation zu ermöglichen. Durch Fremdschlüssel können Datensätze verschiedener Tabellen vereint werden, die miteinander in Verbindung stehen. Der Fremdschlüssel ist dabei eine Art Verweis auf den Primärschlüssel der anderen Tabelle. [36, S. 30–32]

2.3.1.3 SQLite

SQLite ist eine Programmbibliothek, über die relationale Datenbanksysteme realisiert werden können. SQLite gilt als Standardlösung für Android- und iOS-Betriebssysteme. SQL (Structured Query Language; dt.: strukturierte Abfragesprache) ist in SQLite implementiert und ermöglicht es schnell und effizient, Daten aus der Datenmenge zu filtern. SQLite speichert alle Relationen, also Tabellen einer Datenbank, in nur einer Datei. Um mit einer in SQLite existierenden Datenbank arbeiten zu können, bedingt es keinen zwischengeschalteten Serverprozess. Die Datenbank kann unmittelbar in einer Anwendung installiert werden. [37, S. 129–132]

2.3.2 XML-Dateien

Ein Beispiel für die Ablage von Daten im XML-Format sind die sog. ‘Shared Preferences‘ unter Android. Bei diesen handelt es sich um Einstellungen, Benutzervorlieben oder andere Daten, welche als Schlüssel-Wert-Paar gespeichert werden. Durch den Schlüssel, bspw. die Nutzer-ID, kann der zugehörige Wert abgerufen werden. [38]

Die Extensible Markup Language (dt.: erweiterte Auszeichnungssprache) ist eine weit verbreitete Computersprache, wodurch Daten strukturiert in einer Textdatei dargestellt werden. Vorteil der Sprache ist, dass sowohl Menschen als auch Maschinen diese interpretieren können. Eine XML-Datei beinhaltet sogenannte Tags, welche Elemente und die zugehörige Hierarchie definieren. In Elementen können wiederum Text bzw. Daten gespeichert werden. Die XML-Sprache kann für unterschiedliche Zwecke verwendet werden. Bspw. dient sie zur Konfiguration von Software, dem Austausch von Daten zwischen Computersystemen oder der Speicherung von Daten. [39, S. 11–20]

2.3.3 Cache-Speicher

Ein Cache-Speicher dient dem effizienten und schnellen Zugriff auf Speicherinhalte. Im Hardware-Cache sind Kopien von Daten des Hauptspeichers zu finden, wodurch beim Aufruf dieser Daten über den Cache auf einen zeitintensiveren Hauptspeicher-Zugriff verzichtet werden kann. Anwendungen wie Threads hingegen verwenden Software-Caches. Dies dient ebenfalls einem schnelleren Zugriff auf häufig genutzte Daten, unterscheidet sich jedoch in einigen Punkten vom Hardware-Caching. Ein Software-Cache ist im Gegensatz zum Hardware-Cache virtuell und bewirkt keinen schnelleren Zugriff auf den Speicher. Der Software-Cache speichert aus dem Internet bezogene Daten, welche durch das lokale Speichern im Cache nicht erneut aus dem Internet heruntergeladen werden müssen, wenn es zum wiederholten Aufruf der Inhalte kommt. [40, S. 190–191] [41]

2.3.4 JSON-Dokumente

Die JavaScript-Objekt-Notation (engl.: JavaScript Object Notation (JSON)) ist ein Datenaustauschformat, welches von den gängigen Programmiersprachen, wie Java, Python oder C#, interpretiert werden kann. Die Daten eines JSON-Dokumentes sind auf Grund des simplen Aufbauformats auch für Menschen nachvollziehbar. JSON-Dokumente bestehen aus Objekten, welche durch Name-Wert-Paaren näher beschrieben werden. Werte können unterschiedlichen Datentypen, wie weitere Objekte, Arrays (Liste von Werten), Zeichenketten, Zahlen, boolesche Werte oder Null (entspricht einem fehlenden oder keinem Wert) entsprechen. [42, S. 21–34]

2.4 Betriebssystem Android

Das Android-Betriebssystem ist ein Open-Source-Betriebssystem, welches durch Google entwickelt wird. Ursprünglich wurde Android für Smartphones und Tablets entwickelt. Mittlerweile wird das Betriebssystem auch für TVs oder Digital-Kameras verwendet.

Wie in Abbildung 2.3 [43, S. 168] dargestellt, besteht das Android-Betriebssystem aus vier Schichten. Die Basis bildet ein **Linux-Kernel**. Die darüber liegende Schicht besteht zum einen aus verschiedenen **Bibliotheken** und zum anderen aus der **Android-Laufzeitumgebung**. Zu den Bibliotheken zählen u.a. folgende:

- Open Graphics Library for Embedded Systems (OpenGL / ES; dt.: Offene Grafikbibliothek für eingebettete Systeme) dient zur Darstellung von Grafiken.
- MPEG wird für das Speichern von Videos verwendet.

- SQLite ist ein relationales Datenbankmanagementsystem, welches zur Informationsspeicherung verwendet wird.
- WebKit bildet die Grundlage für die Open-Source-Suchmaschine.

Das darüber liegende **Anwendungs-Framework** bietet Entwicklern die Möglichkeit, auf Geräteeigenschaften zuzugreifen. Darüber hinaus gibt es die **Anwendungsschicht**, welche durch verschiedene Anwendungen eine Benutzeroberfläche zum Bedienen des Gerätes bilden. [43, S. 167–168] [44, S. 308–309]

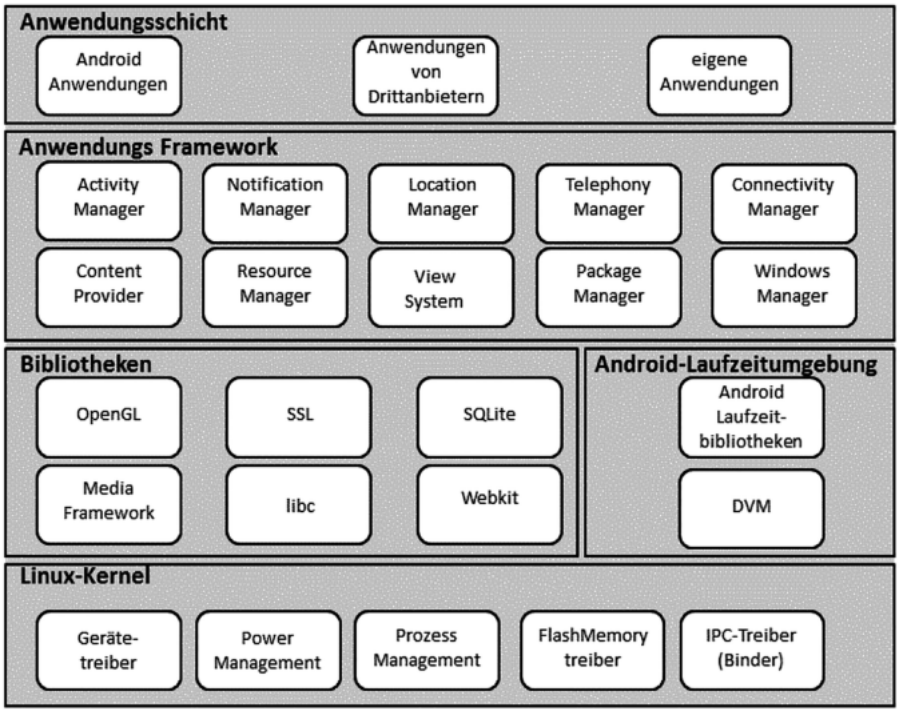

Abbildung 2.3: Schichten des Android-Betriebssystems

2.5 Auslesemethoden

Die Daten der Mobilgeräte, die im Rahmen der Ausarbeitung genutzt wurden, wurden auf unterschiedliche Arten ausgelesen. Die folgenden Abschnitte erläutern die theoretischen Grundlagen.

2.5.1 Testgerät 1 - Datenextraktion mittels SFTP

Der Nutzer des Testgerätes 1 verfügte über einen Root-Zugriff. Die Datenextraktion erfolgte über eine SFTP (vgl. Abschnitt 2.5.1.2), was im Folgenden erläutert wird.

2.5.1.1 Root-Zugriff

Der Geräte-Nutzer besitzt im Normalfall keine Root-Rechte bzw. Administratorrechte, sondern eingeschränkte Rechte, mit denen, anders als mit Root-Rechten, nicht auf alle Dateien des Gerätes zugegriffen werden kann. Eingeschränkte Rechte sind notwendig, um dauerhafte Veränderungen

der Kernfunktionen des Android-Betriebssystems durch den Nutzer, sei es bewusst oder unbewusst, zu vermeiden. Durch Veränderungen des Betriebssystems kann keine Garantie für eine fehlerfreie Funktionalität des Gerätes gewährleistet werden. Ungewollte Folgen kann ein uneingeschränkter Zugriff auch dann haben, wenn bspw. Schadsoftware das Gerät infiziert und mit den Root-Rechten des Nutzers Veränderungen an sensiblen Daten vornimmt. Hierbei ist anzumerken, dass das Sicherheitsmodell von Android sogenanntes 'Sandboxing' (dt. Sandkastenprinzip) vornimmt, um der Verbreitung von Schadsoftware entgegenzuwirken. Unter Verwendung von Zugangskontrollen werden dabei Anwendungs- sowie Systemprozesse voneinander isoliert, was die Ausbreitung von Schadsoftware erschwert. [43, S. 179–181] [45]

Vorteilhaft an der Nutzung von uneingeschränkten Rechten ist u.a. jedoch, dass auch ohne vollständige forensische Dateisystem-Extraktion Anwendungsdaten betrachtet werden können. Dieser Vorteil wurde im Rahmen der vorliegenden Arbeit genutzt, um erzeugte Testdaten unmittelbar nach einer Nutzeraktion einsehen und somit eine detailreiche Auswertung der Daten des Testgerätes 1 durchführen zu können.

2.5.1.2 Datentransfer

Die Secure File Transfer Protocol (SFTP)-Verbindung (dt.: Sicheres Dateiübertragungsprotokoll) basiert auf dem File Transfer Protocol (FTP; dt: Dateiübertragungsprotokoll). Mit Hilfe dieses Protokolls ist es möglich, einen Datentransfer zwischen einem FTP-Client und einem Web-Server zu generieren. Jedoch erfolgt der Datentransfer mit FTP über einen ungesicherten Kanal. Daher kommt die Secure Shell (SSH; dt.: sichere Hülle) zum Einsatz. Über das SSH-Protokoll kann ein Kommunikationskanal abgesichert werden, über den Daten verschlüsselt übertragen werden können. Bei SFTP handelt es sich somit um eine Datenübertragung mittels FTP, bei der die Vertraulichkeit der übertragenen Daten zusätzlich über das SSH-Protokoll abgesichert ist. [46]

2.5.2 Testgerät 2 - Datenextraktion mittels Spezial-Hardware

Die Daten von Testgerät 2 wurden mit Spezial-Hardware (dem forensischen Extraktionsgerät UFED Touch2 der Firma Cellebrite) ausgelesen. Für Android-Betriebssysteme gibt es verschiedene Extraktionsmethoden. Diese werden im Folgenden erläutert.

2.5.2.1 Manuelle Extraktion

Die manuelle Extraktion erfolgt über einen aktiven Zugriff auf des Gerät bzw. auf die Benutzeroberfläche. Einsehbar sind dadurch Daten, welche der gewöhnliche Nutzer / Besitzer des Gerätes einsehen kann. Eine manuelle Extraktion ist ein einfacher Weg, um u.a. Fotos, Videos, Browser- sowie Nachrichtenverläufe, etc. ohne Verwendung eines IT-forensischen Extraktionsgerätes, sichten und bspw. durch Bildschirmfotos extrahieren zu können. Ein Nachteil dieser Methode ist jedoch, dass durch einen aktiven Zugriff auf das Dateisystem Daten ungewollt gelöscht oder verändert werden können. Die manuelle Extraktion kann als zusätzliche Methode verwendet werden, um Daten sichten zu können, die aus anderen Extraktionsmethoden verschlüsselt hervorgehen. [47, S. 441–445]

2.5.2.2 Logische / Dateisystem Extraktion

Eine logische Extraktion beinhaltet Daten eines Dateisystems, wie Ordner und Dateien, auf die der Nutzer Zugriff hat. Die Extraktionsmethode ähnelt dabei einem Backup, also einer Datensicherung, die Datenverluste vorbeugen soll. Gelöschte Dateien können durch eine logische Extraktion jedoch nicht wiederhergestellt werden. Auch die Extraktion von Anwendungsdaten wird durch diese Methode nicht realisiert. [47, 48]

2.5.2.3 Logische / Vollständige Dateisystem Extraktion

Beim Auslesen des vollständigen Dateisystems werden neben den für Nutzer einsehbare Daten auch gelöschte, System-, Anwendungs- und Metadaten extrahiert, was einen umfangreicheren Einblick in die Geräte-Nutzung bieten kann. Gelöschte Daten beziehen sich hierbei auf Daten, die als gelöscht markiert, jedoch noch nicht physisch gelöscht bzw. überschrieben wurden. Da jedoch einige Betriebssystem-Versionen und Gerätemodelle keine vollständige Dateisystem-Extraktion zulassen, muss in solchen Fällen eine andere Extraktionsmethode gewählt werden. Auch wenn eine vollständige Dateisystem Extraktion manuell durch Root-Rechte durchführbar ist, ist die Verwendung eines IT-forensischen Extraktionsgerätes zu empfehlen, da durch die Extraktionen mittels Root-Rechten einige Daten verschlüsselt kopiert werden. Durch IT-forensische Extraktionsgeräte hingegen können Dateien entschlüsselt werden, sofern der entsprechende Schlüssel aus der Extraktion entnommen werden kann. [49]

2.5.2.4 Physische Extraktion

Durch eine physische Extraktion werden die Daten eines Gerätes auf Bit-Ebene kopiert. Mit Hilfe dieser Methode können, neben den Daten des Dateisystems, auch als gelöscht markierte Daten sowie der nicht zugewiesene Speicherbereich des Gerätes ausgelesen werden. Auch für die physische Extraktion ist ein IT-forensisches Extraktionsgerät nicht zwingend notwendig, wenn Root-Recht aktiviert sind. Jedoch besteht auch in diesem Fall das Problem, dass Daten verschlüsselt ausgelesen werden, was durch IT-forensische Extraktionsgeräte weitestgehend unterbunden werden kann. [47, 50, 51]

3 Methodisches Vorgehen

Im Folgenden werden die verwendeten Werkzeuge und Methoden erläutert, anhand derer die Testdaten generiert und ausgewertet wurden.

3.1 Vorbereitung

Die folgenden Abschnitte beschreiben die Eigenschaften der verwendeten Mobilgeräte sowie die Einrichtungsprozesse der nötigen Umgebungen, um die Testdaten generieren zu können. Darunter zählen die Installation von Instagram und Threads sowie die Einrichtung weiterer notwendiger Programme, um auf Threads vollumfänglich zugreifen zu können.

3.1.1 Mobilgeräte

Für die Generierung der Testdaten, wurden zwei Mobilgeräte mit dem Betriebssystem Android durch die FAST-DETECT GmbH zur Verfügung gestellt, welche Zugang zum Internet besitzen. Tabelle 3.1 beinhaltet eine Informationsübersicht zu den Mobilgeräten.

Tabelle 3.1: Informationen zu den Mobilgeräten

	Testgerät 1	**Testgerät 2**
Marke	Samsung	Xiaomi
Produktname	Galaxy S22	Redmi Note 10S
Modell	SM-S901B/DS	M2101K7BNY
Android-Version	13	11
Auslesemethode	Extraktion der Threads-Anwendungsdaten mittels Root-Zugriff	logisch (vollständiges Dateisystem)

Die Auslesemethoden werden in Abschnitt 3.3 erläutert.

3.1.2 Virtual Private Network Verbindung

Zur Verwendung einer VPN-Verbindung wurde die Anwendung Secure VPN installiert, welche es ermöglicht, eine VPN-Verbindung für den Datentransfer frei wählbarer Anwendungen zu erstellen. Dafür wurde ein VPN-Server-Standort außerhalb der EU gewählt. Für beide Mobilgeräte gelten folgende Punkte:

- Anwendungs-ID: com.fast.free.unblock.secure.vpn
- Version: 4.1.13
- Installationsdatum: 26.09.2023

3.1.3 Instagram-Installation

Auf beiden Mobilgeräten wurde die Anwendung Instagram über den Google Play Store installiert und anschließend je ein Instagram-Nutzerkonto eingerichtet, da die Registrierung bei Threads nur mittels Instagram-Konto erfolgen kann. Folgende Tabelle 3.2 gibt Informationen zu den Instagram-Nutzerkonten an.

Tabelle 3.2: Informationen zu den Instagram-Nutzerkonten

	Name	**Benutzername**
Testgerät 1	Testgerät1	testgeraet.1
Testgerät 2	Testgerät2	testgeraet2

Für beide Mobilgeräte gelten folgende Punkte:

- Anwendungs-ID: com.instagram.android
- Version: 301.1.0.33.110
- Installationsdatum: 26.09.2023

3.1.4 Threads-Installation

Nach der Einrichtung des Instagram-Kontos findet sich im Hauptmenü ein Link zum Google-Play-Store-Download von Threads (Schritte 1 und 2 aus Abbildung 3.1). Alle unter Abbildung 3.1 und Abbildung 3.2 abgedruckten Inhalte dienen lediglich zur Veranschaulichung der Anwendungsoberfläche.

Nach Installation der Threads-Anwendung wurde der Nutzer auf der Startseite aufgefordert, wie Schritt 3 aus Abbildung 3.1 zeigt, ein Instagram-Konto auszuwählen, mit welchem der Nutzer bei Threads angemeldet werden soll. Es folgte die Aufforderung zur Einrichtung des Threads-Profils (Schritt 1 aus Abbildung 3.2). Dafür können die Daten entweder von Instagram importiert oder individuell festgelegt werden. Zum Ende der Anmeldung musste entschieden werden, ob das Profil öffentlich oder privat (Schritt 2 Abbildung 3.2) geführt werden soll. Das Konto wurde auf privat gesetzt. Folglich erschien eine Beschreibung der Anwendung Threads, wie in Schritt 3 aus Abbildung 3.2, bevor die Weiterleitung zur Standard-Oberfläche erfolgte. Tabelle 3.3 gibt einen Überblick zu den angelegten Nutzerkonten wieder.

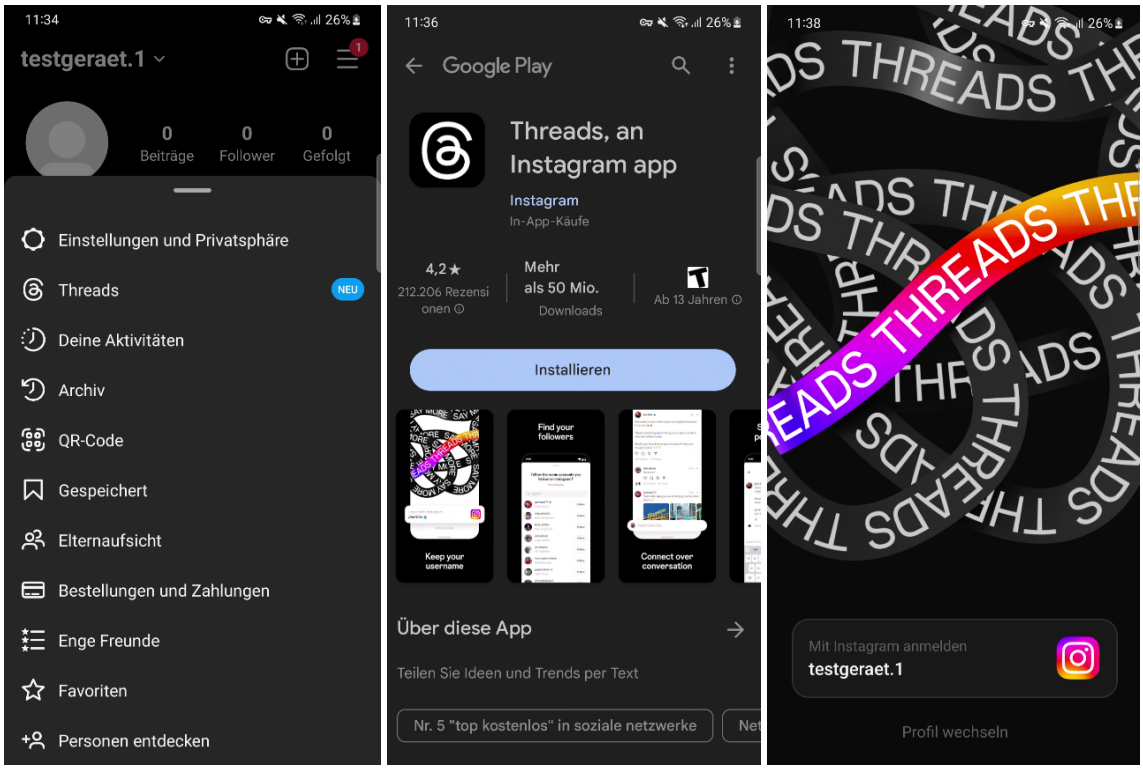

Abbildung 3.1: Threads-Installation Schritte 1-3

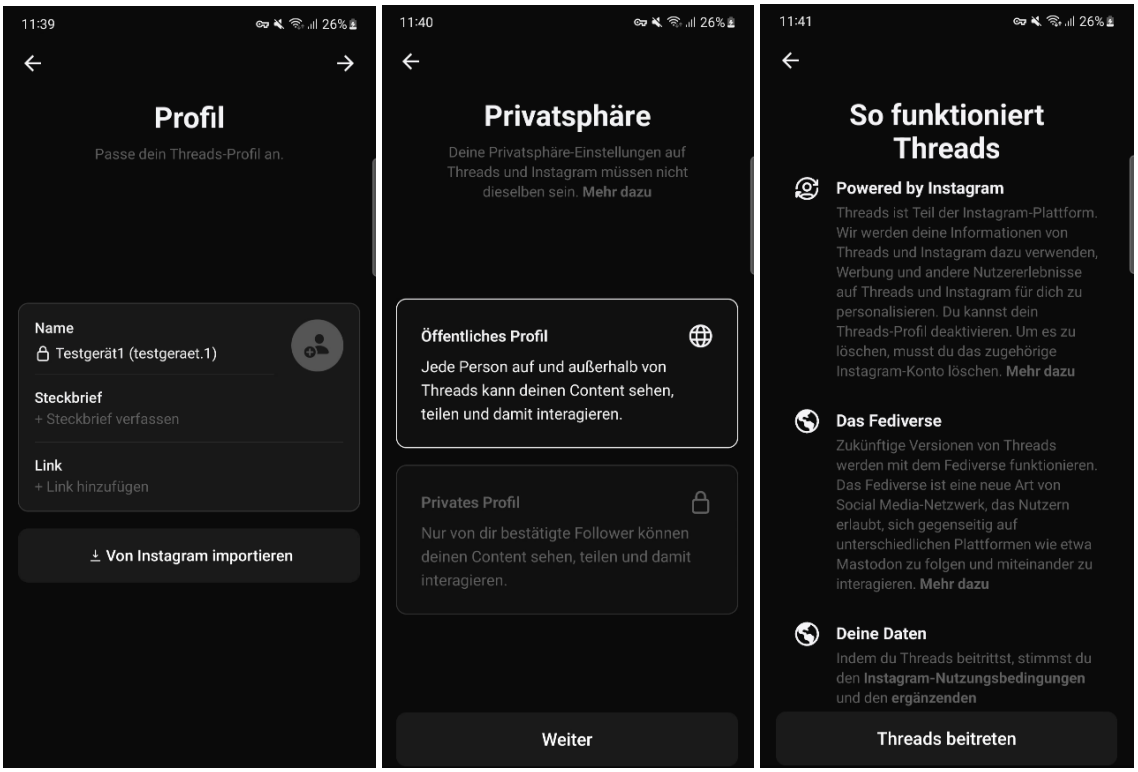

Abbildung 3.2: Threads-Installation Schritte 4-6

Tabelle 3.3: Informationen zu den Threads-Nutzerkonten

	Name	**Benutzername**
Testgerät 1	Testgerät1	testgeraet.1
Testgerät 2	Testgerät2	testgeraet2

Für beide Mobilgeräte gelten folgende Punkte:

- Anwendungs-ID: com.instagram.barcelona
- Version: 301.0.0.30.109
- Installationsdatum: 26.09.2023

3.2 Generierung der Testdaten

Nachdem auf jedem Mobilgerät ein privates Threads-Konto eingerichtet wurde, erfolgte, wie in den nächsten Abschnitten beschrieben, die Testdatengenerierung. Alle aufgeführten Aktionen wurden an beiden Mobilgeräten durchgeführt.

3.2.1 Voreinstellungen

Die Interaktion zwischen privaten Nutzerkonten erfordert zu Beginn eine gegenseitige Bestätigung der ‘Follow‘ (dt.: Folge)-Anfrage. Die Anfragen wurden jeweils bestätigt, sodass der Threads-Nutzer die Beiträge des anderen Nutzers einsehen konnte. Bei einem öffentlichen Nutzerprofil ist keine Anfrage-Bestätigung notwendig, um die Beiträge dieses Profils einsehen zu können.

Im weiteren Verlauf wurde ein Profilbild gesetzt sowie ein Steckbrief- bzw. Biografie-Text verfasst. Des Weiteren erfolgte das Anlegen einer Wortliste, deren Begriffe automatisiert innerhalb der Anwendung für Personen, die dem eigenen Nutzerkonto nicht folgen, verborgen werden (vgl. Abschnitt 2.1.2.4). Als zu filterndes Wort wurde ‘blöd‘ gewählt. Weitere gesetzte Voreinstellungen sind in Tabelle 3.4 aufgeführt. Unter dem Attribut ‘Einstellungen‘ sind alle Änderungsmöglichkeiten gelistet. Das Attribut ‘Optionen‘ beschreibt die Auswahlmöglichkeiten, wobei die gesetzte Option farbig gedruckt ist. Zu beachten ist, dass für Einstellungen einer Zeile, wie z.B. ‘Gefällt mir‘-Angaben und Antworten, die Option individuell wählbar ist, auf Grund von Gleichheit jedoch zu einer Tabellenzeile zusammengefasst wurde.

Tabelle 3.4: Voreinstellungen der Anwendung Threads

Beschreibung	Einstellungen	Optionen
Benachrichtigungen (Threads und Antworten)	‘Gefällt mir‘-Angaben; Antworten; Erwähnungen; Reposts; Zitate; erste Threads	von allen; von Personen, denen du folgst; deaktiviert
Benachrichtigungen (Gefolgt und Follower)	Follower-Anfragen; bestätigte Follower-Anfragen; Kontovorschläge; bereits gefolte Nutzer, die Threads beitreten	aktiviert; deaktiviert
Benachrichtigungen (von Threads)	tägliche Zusammenfassung; Erinnerungen; Produktankündigungen; Vorschläge zum Folgen	aktiviert; deaktiviert
Privatsphäre	Erwähnungen zulassen von	alle; Profile, denen du folgst; niemand
Nachrichten bzw. Kommentare verbergen	Standard-Wortfilter-Liste; personalisierte Wortfilter-Liste	aktiviert; deaktiviert
Beiträge auf anderen Plattformen vorschlagen	Vorschlagen eigener Beiträge: auf Instagram; auf Facebook	aktiviert; deaktiviert (kann nur für öffentliche Nutzerkonten aktiviert werden)

Um die Repost- und Zitierfunktion sowie das Teilen von Threadsbeiträgen über Instagramfunktionen (Instagram-Story, Beitrag und -Direkt-Nachricht) testen zu können, mussten die Threads-Profile von privater auf öffentliche Führung gesetzt werden. Alle anderen Voreinstellungen blieben jedoch unverändert während der Testdatengenerierung.

3.2.2 Verfassen von Beiträgen

Nach dem Setzen der Voreinstellungen aus Abschnitt 3.2.1 wurden durch die Autorin der vorliegenden Arbeit mehrere Beiträge mit unterschiedlichen Inhalten verfasst, welche im Folgenden aufgelistet sind:

- Beitrag mit Text
- Beitrag mit Bild
- Beitrag mit Video

- Beitrag mit Bild und Beschriftung
- Beitrag mit Video und Beschriftung
- Beitrag mit Bildreihe und Beschriftung
- Beitrag mit Videoreihe und Beschriftung
- Beitrag mit Bild- und Videoreihe mit Beschriftung
- Beitrag mit Erwähnung eines anderen Nutzerprofils
- Beitrag mit Zitierung eines anderen Beitrags

Anzumerken ist hierbei, dass Threads eine Anwendung ist, die das Teilen von Audiodateien nicht ermöglicht.

3.2.3 Beitrag-Reaktionen

Threads bietet verschiedene Möglichkeiten, auf Beiträge zu reagieren. Darunter zählen die Vergabe von ‘Gefällt mir‘-Angaben (engl.: Likes), das Verfassen von Antworten oder Reposts. Um möglichst realistische Testdaten zu generieren, wurden einige Beiträge mit sogenannten Likes versehen. Des Weiteren erfolgte das erneute Teilen von Beiträge mittels Repost-Funktion. Unter einigen Beiträgen wurden außerdem Konversationen in Form von Antworten nachgestellt. Im Folgenden wird aufgeführt, mit welchen Inhalten Antworten verfasst wurden:

- Antwort mit Text
- Antwort mit Bild
- Antwort mit Video
- Antwort mit Wort der benutzergenerierten Moderations-Wortliste

Des Weiteren wurden Threads-Beiträge über die Anwendung Instagram mittels Direkt-Nachrichten-Funktion weitergeleitet sowie als Instagram-Beitrag hochgeladen und in der Instagram-Story [1] (dt.: Geschichte) geteilt. Das

3.2.4 Test weiterer Funktionen

Die Suchfunktion wurde getestet, um nach Nutzerprofilen und themenspezifischen Inhalten zu filtern. Für einige Beiträge wurde die Anzahl der ‘Gefällt mir‘-Angaben durch das Verfasser-Profil verborgen, sodass sie für Threads-Nutzer nicht mehr sichtbar sind. Auch Antwortmöglichkeiten wurden eingeschränkt, sodass nur im Beitrag erwähnte Personen auf den Beitrag antworten konnten.

Beiträge von anderen Nutzerprofilen wurden verborgen, was bedeutet, dass diese Inhalte nicht mehr in den benutzerdefinierten Vorschlägen (‘Für dich‘ und ‘Gefolgt‘-Seite) erschienen. Threads-Nutzerprofile wurden außerdem stummgeschaltet (keine Anzeige von Beiträgen oder Antworten dieser Profile) oder eingeschränkt (keine Anzeige von Benachrichtigungen dieser Profile). Auch das Blockieren von Nutzerprofilen wurde getestet.

Abbildung 3.3 gibt einen Einblick in die generierten Testdaten der Anwendung Threads.

[1] https://help.instagram.com/1257341144298972/?cms_platform=android-app&helpref=platform_switcher

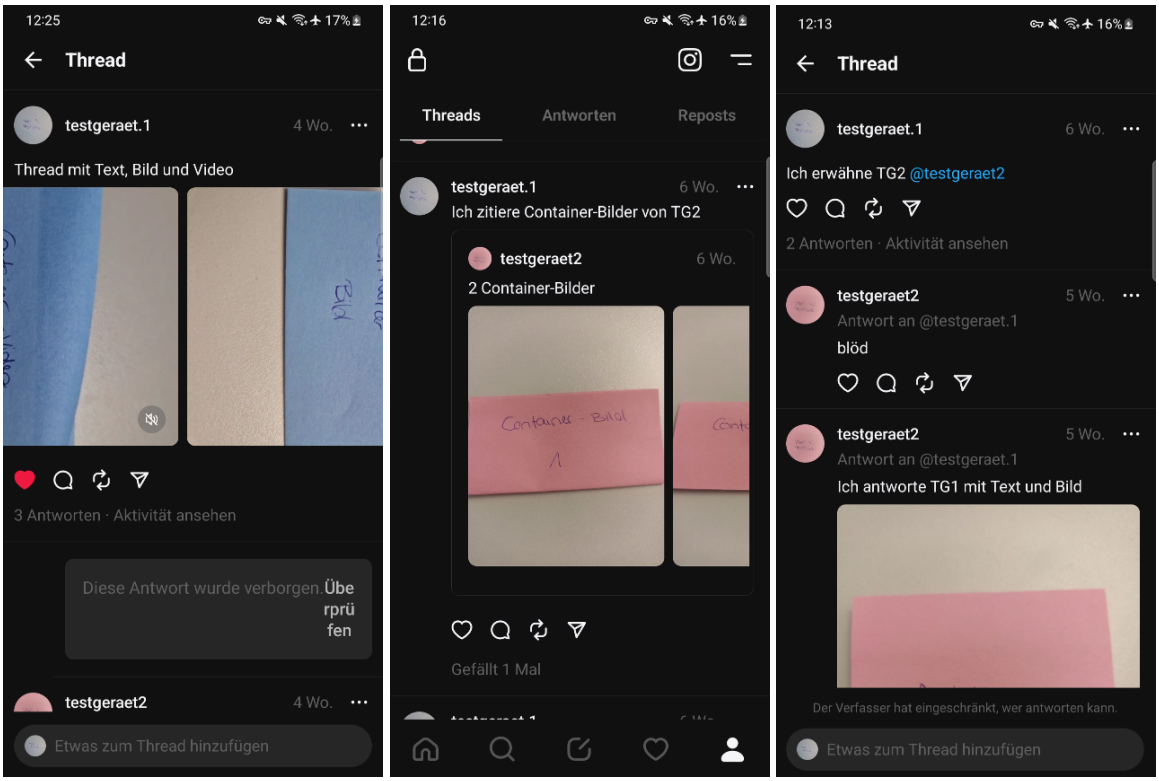

Abbildung 3.3: Ausschnitte der generierten Testdaten

3.3 Auslesen der Mobilgeräte

Bevor die Datenauswertung stattfinden kann, ist das Auslesen der Testdaten erforderlich. Dies erfolgte auf unterschiedliche Arten, um eine detailreiche Auswertung zu ermöglichen. Im folgenden wird darauf eingegangen, wie die Mobilgeräte ausgelesen wurden.

3.3.1 Testgerät 1

Für Testgerät 1 wurde vor dem Erzeugen der Testdaten ein Root-Zugriff generiert. Anschließend wurden die generierten Testdaten mittels SFTP-Verbindung ausgelesen. Der Vorgang wird im Folgenden erläutert.

Um Zugriff auf Administratorrechte zu erreichen, ist die Aktivierung der Entwickleroptionen sowie des Universal Serial Bus (USB)-Debuggings (dt.: Fehlersuche) notwendig. Aus einem Android Open Source Project (AOSP)-Image, welches der auf dem Testgerät 1 installierten Betriebssystemversion entspricht, wurde anschließend das Boot-Image extrahiert und mit Hilfe des Magisk Managers[2] modifiziert, sodass die Administratorrechte aktiviert sind. Magisk Manager ist ein Werkzeug, mit dessen Hilfe Android-Betriebssysteme gerootet oder modifiziert werden können. Im Anschluss wurde der Bootloader des Testgerätes 1 entsperrt und durch den modifizierten Bootloader ersetzt. [52]

[2] https://magiskmanager.com/

Der Datentransfer zwischen Test- und Auswertungsrechner erfolgte über den FTP-Client FileZilla. Auf dem Auswertungsrechner sind die unter Abschnitt 3.4 genannten Programme installiert, welche zur Auswertung der Testdaten dienen. Der Datentransfer erfolgte über ein sicheres Datentransport-Protokoll, wie in Abschnitt 2.5.1.2 beschrieben. [53]

Diese Methode hat den Vorteil, dass nicht das vollständige Abbild des Speichers extrahiert werden muss. Über den direkten Zugriff auf alle Dateien können daraus die Anwendungsdaten von Threads selektiert und somit ohne hohen Zeitaufwand extrahiert werden. Demzufolge können Anwendungsdaten nach jeder Aktion in Threads erneut ausgelesen werden, was eine detailreiche Auswertung ermöglicht.

3.3.2 Testgerät 2

Diese Arbeit entstand im Zuge der Zusammenarbeit mit dem Sachverständigenbüro für IT-Forensik FAST-DETECT GmbH. Daraus ging der Zugang zum benötigten Auslesegerät Universal Forensics Extraction Device (UFED) Touch2 für das Testgerät 2 hervor. Im Zuge dessen wurde eine vollständige Dateisystem-Extraktion vorgenommen.

Anhand der ausgelesenen Daten wurde ein UFED-Bericht generiert. Dieser enthält aufbereitete Daten, woraus z.B. Informationen zu Nutzerkonten, sozialen Medien oder Datenbanken hervorgehen, die auf dem Gerät installiert bzw. vermerkt wurden. Relevant für die vorliegende Arbeit ist, ob und in welchem Umfang Threads-Anwendungsdaten erkannt werden. [54]

3.4 Datenanalyse

Die folgenden Abschnitte erläutern, mit welchen Werkzeugen der Auswertungsprozess durchgeführt wurde. Aus den generierten Daten von Testgerät 1 geht die Auswertung von Ablagestruktur, Datenbanken, XML-Dateien und weiteren relevanten Daten hervor. Der UFED-Bericht von Testgerät 2 wurde nach Anwendungsdaten von Threads durchsucht, welche aus der Datenextraktion von Testgerät 1 hervorgingen.

3.4.1 Ablagestruktur im Speicher

Die Ablagestruktur der Threads-Anwendungsdaten wurde anhand von EnCase (Version 6.19.7.2) betrachtet[3]. EnCase ermöglicht eine strukturierte Analyse und übersichtliche Darstellung der Daten. Die Detektion des Stammverzeichnisses von Threads erfolgte durch die Datenbank ‘localappstate.db‘, welche die IDs der installierten Anwendungen des Android-Betriebssystems enthält und unter dem Verzeichnispfad ‘\data\data\com.android.vending\databases\‘ zu finden ist [55, S. 201–207].

Abbildung 3.4 zeigt einen Ausschnitt der Datenbank ‘localappstate.db‘. Der Ausschnitt beinhaltet die Einträge der Threads- (Eintrag 1) und der Instagram-Anwendung (Eintrag 2). Mit Hilfe des Paketnamens (Attribut package_name) können Anwendungen unter Android eindeutig identifiziert

[3] Die angegebene EnCase-Version wird standardmäßig durch die FAST-DETECT GmbH verwendet und wurde daher auch für Auswertungszwecke dieser Arbeit genutzt.

werden. Des Weiteren ist aus der Ansicht der erste Installationszeitpunkt der Anwendung im Unix-Milliseconds-Format sowie unter dem Attribut ‘Account‘ eine E-Mail-Adresse zu entnehmen, mit der die Nutzerkonten angelegt wurden.

	package_name	first_download_ms	account	title
1	com.instagram.android	1695713779868	[redacted]	NULL
2	com.instagram.barcelona	1695719623933		NULL

Abbildung 3.4: Ausschnitt der Datenbank ‘localappstate.db‘

3.4.2 SQLite-Datenbanken

Die Analyse der Datenbanken erfolgte mit Hilfe des DB Browser for SQLite (Version 3.12.1). Das Programm besitzt eine integrierte Filterfunktion und ermöglicht das Ausführen von SQL-Befehlen, was eine detailreiche Analyse zulässt.

3.4.3 XML-Dateien

XML-Dateien wurden durch den Text-Editor Sublime Text (Version Build 3114) betrachtet. Sublime Text erkennt den Aufbau von XML-Dateien und kann diese strukturiert darstellen. Die Verwendung der Funktion zur farblichen Hervorhebung der XML-Syntax führte zur Verbesserung der Lesbarkeit der untersuchten XML-Dateien.

3.4.4 Bild-, Audio- und Videodateien

Das Betrachten von Bildern geschah mit Hilfe des Bildbetrachtungsprogramms IrfanView (Version 4.56). Videos sowie Audios wurden durch das Videoabspielprogramm VLC Media Player (Version 3.0.6) betrachtet. Des Weiteren wurden fragmentierte Video-Abschnitte mit Hilfe des Hex-Editors HxD (Version 2.1.0.0) zusammengesetzt, um sie vollständig abspielen zu können. Die Metadaten konnten mit Hilfe des Programms ExifTool (Version 11.99) dargestellt werden.

3.4.5 Dekomprimierungsverfahren

Die Testdaten enthalten mittels Gzip komprimierte Dateien. Um die Inhalte zu dekomprimieren und anschließend einsehen zu können, wurde das Programm 7-Zip (Version 23.01) verwendet.

3.4.6 UFED-Bericht

Die extrahierten Gerätedaten wurden mittels der Software Physical Analyzer (Version 7.65.0.22) der Firma Cellebrite aufbereitet und in einer sog. (UFDR)-Datei hinterlegt. UFDR steht hierbei für UFED Physical Analyzer Report Package. Diese UFDR-Datei kann durch den Cellebrite Reader (Version 7.62.0.59) geöffnet werden. Der UFED-Bericht konnte anschließend im Cellebrite Reader mit nach relevanten Daten durchsucht werden. [54]

4 Ergebnisse

Die folgenden Abschnitte beschreiben Ergebnisse und Erkenntnisse, zu denen die Analyse führte. Darunter zählt u.a. die allgemeine Ablagestruktur der Anwendung Threads. Des Weiteren folgt eine Beschreibung, wie Bild- und Video-Dateien, welche über Threads geteilt wurden, mit Nutzerdaten in Verbindung gebracht werden können.

4.1 Ablagestruktur

Das Betrachten der Ablagestruktur zeigte, dass die Anwendungsdaten von Threads im Stammverzeichnis ‘\data\data\com.instagram.barcelona‘ abgelegt werden. Das Stammverzeichnis beinhaltet weitere Unterverzeichnisse, wovon nicht jedes verwertbare Daten aufwies. Die Auswertung beschränkte sich daher auf die Unterverzeichnisse ‘cache‘, ‘databases‘ und ‘shared_prefs‘. Diese Verzeichnisse enthalten Bilder und Videos, die über Threads geteilt wurden sowie Informationen zu Nutzerkonten und deren Aktivitäten. Die folgenden Abschnitte geben einen Überblick zu den Inhalten der Unterverzeichnisse ‘cache‘, ‘databases‘ und ‘shared_prefs‘. Abbildung 4.1 zeigt die Ablagestruktur der eben genannten Verzeichnisse im Stammverzeichnis ‘com.instagram.barcelona‘.

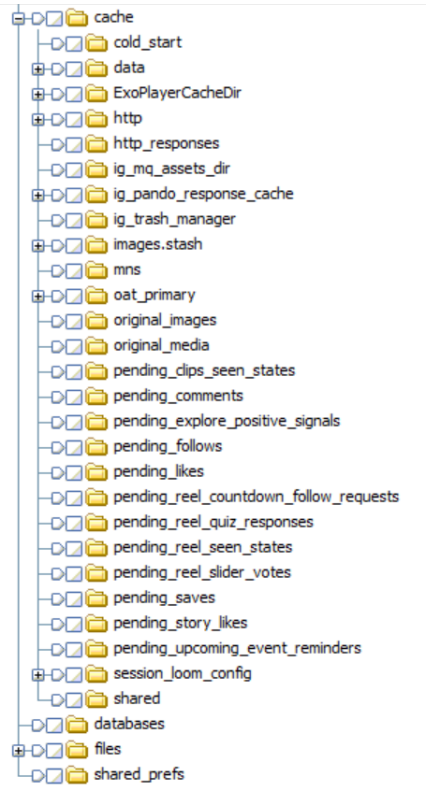

Abbildung 4.1: Ablagestruktur der Anwendungsdaten von Threads

4.1.1 Cache

Das Cache-Verzeichnis ist unter dem Pfad ‘\data\data\com.instagram.barcelona\cache\‘ vorzufinden. Die Inhalte des Cache-Ordners sind in Tabelle 4.1 aufgeführt.

Um die Tabellen übersichtlich zu halten, werden Ablageorte nicht als vollständige Verzeichnis-Pfade angegeben. Beispielsweise dient ‘<Cache-Verzeichnis>‘ als Platzhalter für das Hauptverzeichnis ‘\data\data\com.
instagram.barcelona\cache\‘. ‘<Nutzer-ID>‘ hingegen ist ein Platzhalter für die tatsächliche Threads-Nutzer-ID.

Tabelle 4.1: Inhalt des Cache-Ordners

Verzeichnispfad	**Inhalt**	**Beschreibung**
\data\data\com.instagram.barcelona\cache\	Ordner, Textdateien, Bilder, Videos, Audios	enthält weitere Ordner und Dateien; Erläuterung in Abschnitt 4.2.1
<Cache-Verzeichnis>\cold_start\	Textdatei (Dateiname entspricht der Nutzer-ID)	Informationen zu hochgeladenen Beiträgen, Erläuterung in Abschnitt 4.2.2
<Cache-Verzeichnis>\ExoPlayer CacheDir\videocache\	.exo-Dateien	Video-Beiträge des Nutzers und aus dem benutzerdefinierten Feed; Erläuterung in Abschnitt 4.2.3
<Cache-Verzeichnis>\http_responses\	komprimierte HTTP-Antworten	Informationen zu hochgeladenen Beiträgen und Kommentaren; Erläuterung in Abschnitt 4.2.4
<Cache-Verzeichnis>\ig_pando_response_cache\<Nutzer-ID>\	Textdatei mit standardisierten Content Filter-Listen	enthält gleiche Daten wie Content Filter-Datenbank (vgl. Abschnitt 4.3.2); Erläuterung in Abschnitt 4.2.5
<Cache-Verzeichnis>\mns\	Textdatei ‘dns‘	letzte Zugriffszeit auf DNS-Server
<Cache-Verzeichnis>\images.stash\clean\	.jfif-Dateien	Profilbilder, Bilder des benutzerdefinierten Feeds; Erläuterung in Abschnitt 4.2.6
<Cache-Verzeichnis>\original_images\	.jfif-Dateien	enthält durch den Nutzer zuletzt hochgeladene Bilder; Erläuterung in Abschnitt 4.2.7
<Cache-Verzeichnis>\shared\	.png-Dateien	über Instagram geteilte Threads-Beiträge; Erläuterung in Abschnitt 4.2.8

4.1.2 Datenbanken

Datenbanken, welche aus der Nutzung der Anwendung Threads hervorgingen, wurden unter dem Datenbank-Verzeichnispfad ‘\data\data\com.instagram.barcelona\databases\‘ abgelegt. In diesem Verzeichnis sind SQLite-Datenbanken hinterlegt, welche Informationen zu Aktivitäten und Einstellungen der Anwendung Threads enthalten. Tabelle 4.2 beinhaltet nähere Informationen zu den Datenbanken.

Tabelle 4.2: Inhalt der Datenbanken

Dateipfad	Inhalt
<Datenbank-Verzeichnis>\time_in_app_<Nutzer-ID>.db	Zeitstempel der letzten Protokollierung und der letzten Datenlöschung; Erläuterung in Abschnitt 4.3.1
<Datenbank-Verzeichnis>\content_filter_dictionary_db_<Nutzer-ID>	Content-Filter-Listen verschiedener Sprachen; Erläuterung in Abschnitt 4.3.2
<Datenbank-Verzeichnis>\barcelona_feed_items_room_db_<Nutzer-ID>	Informationen zu Threads aus dem benutzerdefinierten Feed; Erläuterung in Abschnitt 4.3.3

Aus den generierten Testdaten geht zu jeder Datenbank eine Shared Memory-Datei (SHM-Datei) sowie eine Write Ahead Log-Datei (WAL-Datei) hervor. Die SHM-Datei wird von verschiedenen Prozessen zur Koordinierung des Zugriffs verwendet. Die WAL-Datei hingegen speichert Transaktionen, welche noch nicht in der Hauptdatenbank hinterlegt wurden. Ausgenommen davon ist die Datenbank ‘time_in_app_<Nutzer-ID>‘, zu der eine ‘db.journal‘-Datei existiert, welche den aktuellsten vollständigen Datenbankinhalt speichert, um die Datenbank im Falle eines ungewollten Datenverlustes wiederherstellen zu können. [56, 57]

4.1.3 Shared Preferences

Der ‘Shared Preferences‘-Ordner beinhaltet Informationen und Einstellungen zum Nutzerkonto und wurde unter dem Ordnernamen ‘shared_prefs‘ hinterlegt. Die im ‘Shared Preferences‘-Ordner abgelegten XML-Dateien sind unter dem Verzeichnispfad ‘\data\data\com.instagram.barcelona\shared_prefs\‘ zu finden. Die folgende Tabelle 4.3 zeigt die Dateien und deren Inhalte.

Tabelle 4.3: Inhalt der Shared-Preferences-Dateien

Dateipfad	Dateiinhalt
<SharedPrefs-Verzeichnis>\ autobackupprefs.xml	Informationen zum Nutzerkonto (Nutzer-ID, Nutzername, Profilbild-URL)
<SharedPrefs-Verzeichnis>\ NOTIFICATION_CHANNELS.xml	Benachrichtigungseinstellungen; Erläuterung in Abschnitt 4.4.1
<SharedPrefs-Verzeichnis>\ig_cask_ metadata_store.xml	Informationen zur Löschung von Daten; Erläuterung in Abschnitt 4.4.2
<SharedPrefs-Verzeichnis>\devprefs.xml	Navigationskette der letzten Sitzung mit Zeitstempel; Erläuterung in Abschnitt 4.4.3
<SharedPrefs-Verzeichnis>\com.instagram. barcelona_preferences.xml	Angaben zum Nutzerkonto; Erläuterung in Abschnitt 4.4.4
<SharedPrefs-Verzeichnis>\<Nutzer-ID>_ USER_PREFERNCES.xml	Angaben zu Nutzerkonten, die mittels Suchfunktion detektiert wurden; Erläuterung in Abschnitt 4.4.5

4.1.4 Weitere Threads-Daten

Außerhalb des ‘com.instagram.barcelona‘-Verzeichnisses wurden weitere Threads-Daten unter dem Verzeichnispfad ‘\data\media\0\‘ hinterlegt. Darin befinden sich folgende, in Tabelle 4.4 dargestellte, weitere Verzeichnisse:

Tabelle 4.4: Inhalt des Media-Verzeichnisses

Verzeichnispfad	Inhalt	Beschreibung
Pictures\Threads\	.jpg-Dateien	Profilbild des Nutzerkontos
Pictures\.thumbnails\	.jpg-Dateien	durch Nutzerkonto hochgeladene Bilder
Movies\Threads\	.mp4-Dateien	durch Nutzer hochgeladene Videos
Movies\.thumbnails\	.jpg-Dateien	Vorschaubilder der Videos, welche durch das Nutzerkonto hochgeladen wurden

Nähere Erläuterungen der Daten aus Tabelle 4.4 sind in Abschnitt 4.5 zu finden.

4.2 Cachedaten-Analyse

In den folgenden Abschnitten werden die Daten des Cache-Ordners genauer betrachtet. Dafür werden insbesondere Metadaten der Bilder und Videos sowie Inhalte von Textdateien betrachtet. Die daraus resultierenden Erkenntnisse können wiederum mit Informationen aus Datenbanken oder XML-Dateien verknüpft werden.

4.2.1 Stammverzeichnis des Caches

Das Cache-Stammverzeichnis enthält Ordner, Textdateien sowie Bilder, Videos und Audiodateien. Die Bilder im Joint Photographic Experts Group (JPEG)-Format und Videos im MP4 (Abkürzung für MPEG4)-Format sind als kürzlich durch den Nutzer hochgeladene Medien identifizierbar. Die ebenfalls im MP4-Format hinterlegten Audiodateien gehören zu den Video-Dateien. Im Folgenden sind Beispiele für die Bezeichnung einer Video- und einer Audiodatei gelistet:

- segmentingMuxer_0_**1698148377**683_AUDIO72678378223368376 76.mp4
- segmentingMuxer_0_**1698148376**933_VIDEO8501420258956049005.mp4

Die farbig gedruckten Zahlenfolgen sind Zeitstempel im Unix-Milliseconds-Format und weisen auf den Zeitpunkt des Hochladens des Videos hin. Die in Fettschrift hervorgehobenen Abschnitte der Zeitstempel stimmen überein; die Zeitpunkte liegen somit in zeitlicher Nähe zueinander. Dies kann auf eine Zusammengehörigkeit der durch den Nutzer hochgeladenen Dateien zueinander hindeuten. Des Weiteren geht aus den Metadaten hervor, dass die Video- und Audiodatei eine ähnliche Abspieldauer, mit einer Abweichung von wenigen Millisekunden, besitzen. Verifizieren, ob Video- und Audiodatei zusammengehören, lässt sich jedoch nur anhand der Originaldatei, bei der Video und Audio nicht separiert wurden.

4.2.2 cold_start

Der Ordner ‘cold_start‘ enthält eine Textdatei, deren Dateiname der Nutzer-ID entspricht. In dieser Datei sind Threads-Aktionen aufgeführt, welche durch Attribut-Werte beschrieben werden. Der Dateiinhalt beginnt mit dem Attribut ‘num_results‘, welchem ein Integer-Wert zugeordnet ist. Der Integer-Wert entspricht der Anzahl der in der Datei aufgeführten Threads-Aktionen. Einer Aktion, also dem Hochladen eines Beitrags, sind Informationen zum Ersteller des Beitrags zugeordnet sowie Angaben zum Beitrag selbst. Abbildung 4.2 zeigt exmplarisch die ersten Zeilen der Datei des ‘cold_start‘-Verzeichnisses. Abbildung 4.3 bildet einen Ausschnitt von Informationen eines Beitrags aus dieser Datei ab. Tabelle 4.5 enthält relevante Attribute und deren Definitionsbereiche, welche sich auf den Beitrag beziehen. Die in Tabelle 4.6 aufgeführten Attribute betreffen den Ersteller des Beitrags.

```
{"num_results":8,"more_available":true,"auto_load_more_enabled":true,"is_direc
t_v2_enabled":true,"next_max_id":"KEEAITgD1BmVAS3kKQEx45IBLYevAC_XlgEth1-
ATDuWAS3rHDTU9t_ALO48gb2akwEtsQkBI8VgAS30LgFXkZQBLRa4wd32g2NGAhgPcHVsbF90b19yZ
WZyZXNoaLEBAIevAC_XlgEth1-ATDuWAS2I3TlkxebALAxWrse79bEsmCOtKeT0sSydya-
qGZBxLCE4A9QZlQEtsQkBI8VgAS2ydQBHA1sBLb1tOUDW67Es0YC4go8kpyxZfzsc-
OmxLOITO9O1Jacs5CkBMeOSAS3kQ7lUPiKnLGdEuOSjIacs6Z86XHAlpyzrHDTU9t_ALO48gb2akwE
tcAGCpuBbAS30LgFXkZQBLfT3uV2JIqcsAA==","view_state_version":"1701334200072-
b639a1380b234f15a1ec35e0447b5959","client_feed_changelist_applied":false,"requ
est_id":"110b1b0b39414df1981decc564b5348a","pull_to_refresh_window_ms":5000,"p
reload_distance":4,"status":"ok","pagination_source":"text_post_feed_following
","session_id":"dec04e51-
bcaf-445e-95b9-88610091f10f","hide_like_and_view_counts":0,"last_head_load_ms"
:1701334200371,"is_shell_response":false,"feed_items":[{"text_post_app_thread"
:{"thread_items":[{"post":{"pk":3243039057634176903,"id":"3243039057634176903_
```


Abbildung 4.2: Erste Zeilen der Datei des ‘cold_start‘-Verzeichnisses


```
:{"thread_items":[{"post":{"pk":3243039057634176903,"id":"3243039057634176903_
62074384035","taken_at":1700820403,"device_timestamp":853076314786001,"client_
cache_key":"MzI0MzAzOTA1NzYzNDE3NjkwMw==.2","filter_type":0,"like_and_view_cou
nts_disabled":true,"integrity_review_decision":"pending","caption_is_edited":f
alse,"strong_id__":"3243039057634176903_
62074384035","text_post_app_info":{"is_reply":false,"reply_control":"mentioned
_only","can_reply":true,"direct_reply_count":2,"hush_info":null,"is_first_post
":false,"is_parent_edited":false,"is_post_unavailable":false,"link_preview_att
achment":null,"mention_count":1,"post_preview_caption":"Ich erwähne TG1 😆
@testgeraet.1","quote_count":0,"reply_facepile_users":[],"reply_level":0,"repl
y_to_author":null,"repost_count":0,"self_thread_count":0,"share_info":{"can_qu
ote_post":true,"can_repost":true,"is_reposted_by_viewer":false,"quoted_post":n
ull,"quoted_post_caption":null,"repost_restricted_reason":null,"reposted_post"
:null},"will_add_author_to_mentioned_users":false},"caption":{"pk":"1787628369
2993873","user_id":62074384035,"user":{"pk":62074384035,"pk_id":"62074384035",
"full_name":"Testgerät2","is_private":false,"has_onboarded_to_text_post_app":t
rue,"strong_id__":"62074384035","fbid_v2":"17841461921069298","username":"test
geraet2","is_verified":false,"profile_pic_id":"3201675974412014225_
62074384035","profile_pic_url":"https://scontent-
lga3-2.cdninstagram.com/v/t51.2885-19/382940626_336878735406309_
2029451286640383094_n.jpg?stp=dst-jpg_s150x150\u0026_nc_ht=scontent-
lga3-2.cdninstagram.com\u0026_nc_cat=109\u0026_nc_ohc=rEuBHd5X4BUAX_ZfA0L
\u0026edm=AJ1VKAgBAAAA\u0026ccb=7-5\u0026oh=00
_AfA1YWcz-1dUhpXDDb0bJ4Cy2Pd9KXpQDnECszzB9aEVSQ\u0026oe=656C87EA\u0026_nc_sid=
69b717","transparency_product_enabled":false},"type":1,"text":"Ich erwähne TG1
```


Abbildung 4.3: Beitragsinformationen des ‘cold_start‘-Verzeichnisses

Tabelle 4.5: Relevante Beitrag-Attribute

Attribut	Wert	Beschreibung
created_at	numerische Zeichenfolge	Zeitstempel des Hochladens
is_reply	boolescher Wert	Beitrag ist eine / keine Antwort auf einen anderen Beitrag
reply_control	Follower; gefolgten Profilen; erwähnte Profile	Angabe, wer auf den Beitrag antworten kann
reply_level	Integer-Wert	Antwort-Ebene
is_first_post	boolescher Wert	Angabe, ob es der erste / nicht der erste Beitrag ist
mention_count	Integer-Wert	Anzahl der im Beitrag erwähnten Profile
quote_count	Integer-Wert	Anzahl der Zitate des Beitrags
repost_count	Integer-Wert	Anzahl, wie oft der Beitrag erneut hochgeladen wurde
can_repost	boolescher Wert	true = Repost bei öffentlichen Nutzerkonten möglich; false = Repost bei privaten Nutzerkonten nicht möglich
is_reposted_by_viewer	boolescher Wert	Angabe, ob der Beitrag über das eigene Nutzerkonto erneut geteilt wurde
quoted_post	null oder weitere Attribute zum Zitat	null = kein Zitat im Beitrag hinterlegt; Aufführung weiterer Attribute, wenn Zitat vorhanden
reposted_post	null oder weitere Attribute zum Repost	null = Beitrag ist kein Repost; Aufführung weiterer Attribute, wenn Beitrag ein Repost ist
did_report_as_spam	boolescher Wert	true = Beitrag wurde gemeldet; false = Beitrag wurde nicht gemeldet
content_type	Zeichenfolge	Art des Contents (z.B. Kommentar)
original_width	Integer-Wert	Breite des Bild- oder Video-Beitrags
original_height	Integer-Wert	Höhe des Bild- oder Video-Beitrags
like_count	Integer-Wert	Anzahl der ‘Gefällt mir‘-Angaben
has_liked	boolescher Wert	Angabe, ob Beitrag über eigenes Nutzerkonto geliket wurde
media_type	Integer-Wert	1 = Foto; 2 = Video; 8 = Bild / Video-Reihe; 18 = Repost; 19 = Text
product_type	Zeichenfolge	feed = Bild- oder Video-Beitrag; text_post = Textbeitrag; carousel_container = Bild- oder Videoreihe

Tabelle 4.6: Relevante Ersteller-Attribute

Attribut	Wert	Beschreibung
username	Zeichenfolge	Nutzername
user_id	numerische Zeichenfolge	elfstellige Nutzer-ID
full_name	Zeichenfolge	vollständig angegebener Name
is_private	boolescher Wert	Nutzerkonto ist (nicht) privat
is_verified	boolescher Wert	Nutzerkonto ist (nicht) verifiziert
profile_pic_id	Zeichenfolge	Profilbild-ID
profile_pic_url	Zeichenfolge	Profilbild-URL

Durch mehrmaliges Extrahieren dieser Datei, lies sich feststellen, dass der Inhalt regelmäßig erneuert wird und somit Informationen zu älteren Beiträgen in dieser Datei verloren gehen. In welchen Zeitabständen oder durch welche Ereignisse die Inhalte erneuern werden, konnte nicht nachvollzogen werden.

4.2.3 ExoPlayerCacheDir

Im Ordner ‘ExoPlayerCacheDir‘ befindet sich ein weiterer Ordner mit der Bezeichnung ‘videocache‘. Dieser beinhaltet Dateien im EXO-Format. Die EXO-Dateien sind fragmentierte MP4-Dateien, welche nach dem Zusammentragen der Fragmente, mit Hilfe des Hex-Editors HxD, vollständig abgespielt werden können. Darunter sind Videos, die durch die Nutzerkonten von Testgerät 1 und Testgerät 2 sowie weiteren unbekannten Nutzerkonten auf Threads hochgeladen wurden. Es folgen zwei Beispiele des Aufbaus der Video-Dateinamen:

- 3242979062804744820_**62219277051**.null.6764998386959721vd.-1.310511401_166415039847694_3605731805280984387_n.mp4.0.**1701670651213**.v2.exo
- 3242979062804744820_**62219277051**.null.6764998386959721vd.-1.310511401_166415039847694_3605731805280984387_n.mp4.554309.**1701439774192**.v2.exo

Die folgenden Punkte erläutern die Zusammenstellung des Dateinamens:

- Die farbig fett gedruckte numerische Zeichenfolge entspricht der Nutzer-ID des Nutzerkontos, durch welches das Video über Threads geteilt wurde.
- Der farbig gedruckte Teil ist bei jedem Fragment desselben Videos identisch.
- Nach dem farbigen Abschnitt folgt, wie im Beispiel, ‘0‘ oder eine andere Zahlenfolge, die den Zeitpunkt, in dem das Video-Fragment im vollständigen Video einsetzt, kennzeichnet.
- Das Fragment mit der Zeitmarke ‘0‘ (entspricht Sekunde 0) signalisiert demnach den Video-Start.

- Die schwarze fett gedruckte numerische Zeichenfolge entspricht einem Zeitstempel im Unix-Milliseconds-Format, welcher möglicherweise den Zeitpunkt des Speichervorgangs beschreibt, da der Zeitstempel nur näherungsweise dem Zeitpunkt des Hochladens entspricht.

Durch die Analyse der Datenbanken und XML-Dateien können die Videos mit weiteren Informationen verknüpft werden. Dieser Vorgang ist in Abschnitt 4.6 aufgeführt.

4.2.4 http_responses

Das Verzeichnis ‘http_responses‘ enthält mittels Gzip-Verfahren komprimierte Dateien im JSON-Format. Auffällig dabei ist die unspezifische Dateiendung ‘.clean‘. Aus dem Dateinamen (Bsp.: 3803cb1d-body_gzip.clean) und der hexadezimalen Ansicht des Datei-Headers geht jedoch hervor, dass die Datei Gzip-komprimiert ist. Der Datei-Header beginnt mit der Zeichenfolge ‘1F 8B‘, was der Signatur von Gzip-komprimierten Dateien entspricht.

Zu jeder ‘-body_gzip.clean‘-Datei existiert zudem eine ‘-resp_gzip.clean‘-Datei. ‘resp‘ steht vermutlich für ‘Response‘, was übersetzt ‘Antwort‘ bedeutet. Die ‘-resp_gzip.clean‘-Dateien enthalten u.a. Informationen zum Status der Anfrage. Die dekomprimierten ‘-body_gzip.clean‘-Dateien weisen ähnliche Daten zur Ereignis-Datei im ‘cold_start‘-Verzeichnis auf. In der Ereignis-Datei sind lediglich Informationen zu Beiträgen vorzufinden, jedoch keine zu Beitrag-Antworten. Dateien des ‘http_responses‘-Verzeichnisses enthalten sowohl Informationen zum Beitrag als auch zu dessen Antworten.

Die ‘-body_gzip.clean‘-Dateien beinhalten Schlüssel-Wert-Paare, wie in der Datei des ‘cold_start‘-Ordners, um Objekte näher zu beschreiben. Grundsätzlich werden in Bezug auf Antworten die gleichen Attribute aufgeführt, wie für Beiträge. Darunter zählen u.a. Attribute zu Erstellungsdatum, Erwähnungen, Zitierungen, Reposts, ‘Gefällt mir‘-Angaben, etc. In folgender Tabelle 4.7 sind Attribute aufgelistet, die relevante Daten über Antworten aufweisen.

Tabelle 4.7: Relevante Antwort-Attribute

Attribut	Wert	Beschreibung
is_reply	boolescher Wert	true = Antwort; false = Beitrag
post_preview_caption	Zeichenfolge	textueller Inhalt der Antwort
reply_level	Integer-Wert	Antwort-Ebene
reply_to_author	Element mit weiteren Attributen	Attribute zum Verfasser des Beitrags, auf den geantwortet wurde
candidates	Array	Höhe, Breite und URL zu Bildern / Videos (sofern in Antwort vorhanden)
reply_facepile_users	Array	Informationen zu Nutzerprofilen der Antwort-Autoren

Aus der Analyse ging außerdem hervor, dass die ‘http_responses‘-Dateien nicht gelöscht werden, sondern zumindest über den Zeitraum, in dem die Testdaten generiert wurden, erhalten bleiben. Die Testdaten-Generierung erstreckte sich über etwa zehn Wochen. Ob eine Löschung zu einem späteren Zeitpunkt stattfindet, konnte im Rahmen dieser Ausarbeitung nicht nachvollzogen werden.

4.2.5 ig_pando_response_cache

Im Ordner ‘ig_pando_response_cache‘ konnte ein Unterordner festgestellt werden, dessen Verzeichnisname der Nutzer-ID entspricht. In diesem Ordner ist eine Textdatei hinterlegt. Der Dateiname besteht aus einer nicht nachvollziehbaren Zeichenfolge. Der Inhalt der Datei weist eine Liste von Content-Filtern verschiedener Sprachen auf, welche automatisiert durch die Anwendung angelegt wurden. Da der Inhalt jedoch dem der wesentlich übersichtlicheren Datenbank ‘content_filter_dictionary_db_<Nutzer-ID>‘ gleicht, wird dieser anhand der Datenbank in Abschnitt 4.3.2 erläutert.

4.2.6 images.stash

Der Ordner ‘images.stash‘ enthält zwei weitere Ordner ‘clean‘ und ‘dirty‘, von denen nur ersterer Daten enthält. Im Ordner ‘clean‘ sind JPEG File Interchange Format (JFIF) und Portable Network Graphic (PNG) formatierte Dateien hinterlegt. Dateien im PNG-Format sind möglicherweise der Facebook-Anwendung zuzuordnen, da diese die Bezeichnung ‘facebook.com‘ im Dateinamen enthalten. Allerdings zeigen diese Dateien lediglich schwarze Bild-Inhalte und die Zuordnung zu spezifischen Nutzeraktionen ist nicht ersichtlich.

Die JFIF-Dateien hingegen können in zwei Kategorien eingeteilt werden: Profilbilder und Bilder des benutzerdefinierten Feeds. Die Kategorien sind anhand des Aufbaus der Dateinamen unterscheidbar. Im Folgenden sind beispielhaft zwei Dateinamen aufgelistet:

- Profilbild:
  https%3a%2f%2fcdninstagram.com%2fv%2ft51.2885-19%2f383840612_1551192028953998_7361247906864230808_n.jpg%3fstp=dst-jpg_s150x150&ccb=7-5_-1_-1
- Benutzerdefinierter Feed:
  MzIyMDYxMjQ2MDM4MTQzNzc4NQ==.2-ccb7-5_1080_1438

Die Dateinamen der Profilbilder entsprechen URLs, unter denen die Profilbilder aufzufinden sind. URLs können jedoch reservierte Zeichen beinhalten, die missverständlich bei der Internetübertragung oder als Dateipfad interpretiert werden würden. Daher wurde für die obige Dateibezeichnung die Prozent-Codierung verwendet, um reservierte Zeichen durch unmissverständliche Zeichen zu ersetzen.

Der farbig hinterlegte Teil der Dateibezeichnung des benutzerdefinierten Feeds ist eine mittels Base64 codierte Zahlenfolge.

Inwiefern die Bilder als Profilbild bzw. benutzerdefinierter Feed eingeordnet werden können, ist in Abschnitt 4.6 anhand weiterer Daten aufgeführt.

4.2.7 original_images

Aus dem Testszenario ging hervor, dass das Verzeichnis ‘original_images‘ Bilder enthält, die zuletzt durch den Nutzer hochgeladen wurden. Der Inhalt des Ordners wird regelmäßigen erneuert. In welchem Zeitraum oder durch welche Ereignisse die Aktualisierung ausgelöst wird, wurde nicht ersichtlich.

4.2.8 shared

Der Ordner ‘shared‘ beinhaltet die über Instagram geteilten Threads-Beiträge. Wird ein Video als Instagram-Beitrag oder Instagram-Story geteilt, wird lediglich ein Vorschaubild des Videos verwendet, welches auf Instagram angezeigt wird. Aus den Testdaten geht hervor, dass im ‘shared‘-Verzeichnis lediglich der aktuellste Beitrag und die zuletzt geteilte Story mit Threads-Inhalten hinterlegt werden. Die Story mit Threads-Inhalten wird im Verzeichnis unter ‘sticker.png‘ abgelegt und der Beitrag unter der Bezeichnung ‘feed_post.png‘. Des Weiteren besitzen auf Instagram geteilte Medien mit Threads-Inhalten einen spezifischen Hintergrund. Der Hintergrund dient vermutlich dem schnellen Erkennen von Threads-Inhalten auf Instagram. Die Vorlagen für die Hintergründe sind im ‘shared‘-Verzeichnis unter ‘feed_background_dark.png ‘ und ‘story_background_dark.png ‘hinterlegt.

4.3 Datenbankanalyse

Die folgenden Abschnitte beleuchten den Inhalt der Datenbanken und welche Informationen daraus zu ziehen sind. Aus den extrahierten Anwendungsdaten gehen mehrere Datenbanken hervor. Drei der aus den Testdaten hervorgegangenen Datenbanken enthalten befüllte Tabellen, welche relevante Daten aufweisen.

4.3.1 time_in_app_<Nutzer-ID>.db

Die ‘time_in_app_<Nutzer-ID>.db‘-Datenbank enthält u.a. die Tabelle ‘metadata‘, welche zwei Zeitstempeleinträge (last_logging_timestamp und last_eviction_timestamp) im Unix-Seconds-Format enthält. Beide Zeitstempel sind innerhalb dieses Testszenarios stets identisch. Möglicherweise könnten die Zeitstempel für den letzten Nutzungszeitpunkt der Anwendung und die letzte Bereinigung bzw. Entfernung von Anwendungsdaten stehen. Um welche Anwendungsdaten es sich dabei genau handelt, konnte im Rahmen dieser Ausarbeitung jedoch nicht nachvollzogen werden.

Des Weiteren existiert in dieser Datenbank die Tabelle ‘intervals‘. Diese weist die Attribute ‘start_event‘ und ‘end_event‘ auf. Die Testdaten enthalten für das Attribut ‘start_event‘ Integer-Werte von 1 oder 7. Als Attribut ‘end_event‘ ist ausschließlich der Integer-Wert 2 aufgeführt. Die Integer-Werte des Attributs ‘start_event‘ könnten für das Durchführen einer bestimmten Aktion stehen (z.B. das Öffnen der Anwendung oder das Hochladen eines Beitrags). Der Integer-Wert des Attributs ‘end_event‘ könnte anschließend auf die erfolgreiche oder fehlgeschlagene Durchführung der Aktion hinweisen. Die Theorie lässt sich anhand der Testdaten jedoch nicht verifizieren, da kein Szenario nachgestellt werden konnte, welches eine eindeutige Zuordnung von Integer-Wert zu Nutzeraktion zulässt.

Des Weiteren enthält die Tabelle die Attribute ‘start_walltime‘ und ‘end_walltime‘, welche Zeitstempel im Unix-Seconds-Format aufweisen. Diese Zeitstempel stehen möglicherweise für Start- und Endzeit einer Aktion. Weitere Zeitstempel weisen die Attribute ‘start_uptime‘ und ‘end_uptime‘auf. Diese Zeitstempel hingegen bestehen in den generierten Testdaten aus fünf bis sechs Ziffern, was auf ein proprietäres Zeitformat hinweisen könnte.

4.3.2 content_filter_dictionary_db_<Nutzer-ID>

Die ‘content_filter_dictionary_db_<Nutzer-ID>‘-Datenbank enthält u.a. die Tabelle ‘content_filter_-dictionary_metadata‘, welche Content Filter-Listen verschiedener Sprachen enthält, die automatisiert durch die Anwendung generiert wurden. Abbildung 4.4 zeigt einen Ausschnitt der Tabelle.

	dictionary_key	name	latestVersion		
1	972134933488349	igd_predefined_profanity_list_english_refresh	6e8aa57b	7adc9766	76f09ed8...
2	1169998560477470	igd_predefined_profanity_list_de_refresh	0a69e72a	59b7d2f0	b7887524...

Abbildung 4.4: Tabelle: content_filter_dictionary_metadata

Aus dem Attribut ‘name‘ ist zu entnehmen, welcher Sprache der Datenbank-Eintrag zuzuordnen ist. Das Attribut ‘latestVersion‘ enthält mehrere durch Tabulatoren getrennte Zeichenketten, möglicherweise Hashwerte, die auf Filter-Wortlisten verweisen könnten. Die als Hashwert vermuteten Zeichenketten konnten jedoch anhand der Anwendungsdaten nicht näher spezifiziert werden. Abbildung 4.4 zeigt einen Ausschnitt der Tabelle ‘content_filter_dictionary_metadata‘.

Des Weiteren ist in dieser Tabelle die benutzergenerierte Filter-Wortliste zu finden, welche den ‘dictionary_key‘ ‘user_custom_dictionary_key‘ besitzt. Den Attributen ‘name‘ und ‘latestVersion‘ sind keine Werte zugeordnet. Jeder Content-Filter-Liste ist jedoch eine ID zugeordnet. Diese ID findet sich unter dem Attribut ‘dictionary_id‘ der Tabelle ‘content_filter_dictionary_entries‘ wieder. In der Spalte ‘pattern‘, wie in Abbildung 4.5 zu sehen, ist die benutzergenerierte Filter-Liste im Klartext hinterlegt.

	dictionary_id	pattern
1	25	blöd

Abbildung 4.5: Tabelle: content_filter_dictionary_entries

4.3.3 barcelona_feed_items_room_db_<Nutzer-ID>

Die Tabelle ‘barcelona_user_feed_items‘ der ‘barcelona_feed_items_room_db_<Nutzer-ID>‘-Datenbank beinhaltet Informationen zu benutzergenerierten Inhalten der ‘Gefällt mir‘- und der ‘Gefolgt‘-Seite. In Abbildung 4.6 ist ein Ausschnitt der Tabelle mit einer Auswahl von Attributen zu sehen.

	id	data	media_age
1	3224453471294269300	{"id":"3224453471294269300","show_create_reply_cta"...	1698604829
2	3224603613225880705	{"id":"3224603613225880705","show_create_reply_cta"...	1698622727
3	3224643617708262437	{"id":"3224643617708262437","show_create_reply_cta"...	1698627496

Abbildung 4.6: Tabelle: barcelona_feed_items_room_db_<Nutzer-ID>

Dem Attribut ‘data‘ sind JSON-Dokumente zugeordnet. Aus diesen gehen nähere Informationen zum Beitrag sowie dem Verfasser des Beitrages hervor. Außerdem ist den Daten zu entnehmen, inwiefern das eigene Nutzerprofil und das Verfasserprofil zueinander stehen. Folgende Tabelle 4.8 und Tabelle 4.9 weisen Informationen zum Beitrag und dessen Verfasser in Form von Attributen und deren Wertzuweisungen auf.

Tabelle 4.8: Informationen zum Beitrag

Attribut	**Wert**	**Beschreibung**
created_at_utc	numerische Zeichenfolge	Zeitstempel des Hochladens des Beitrags im Unix-Seconds-Format
did_report_as_spam	boolescher Wert	true = Beitrag wurde gemeldet; false = Beitrag wurde nicht gemeldet
text	alphanumerische Zeichenfolge	Text, der dem Beitrag zugefügt wurde
carousel_media_count	Integer-Wert	Anzahl der Bilder / Vidoes, die der Beitrag enthält
like_and_view_counts_disabled	boolescher Wert	De- / Aktivierung der Betrachter- und ‘Gefällt mir‘-Anzahl-Anzeige
like_count	Integer-Wert	Anzahl der ‘Gefällt mir‘-Angaben
media_type	Integer-Wert	1 = Foto; 2 = Video; 8= Bild / Video-Reihe; 18 = Repost 19 = Text
original_height	Integer-Wert	Höhe des Bild- oder Video-Beitrags
original_width	Integer-Wert	Breite des Bild- oder Video-Beitrags
product_type	Zeichenfolge	feed = Bild / Video; text_post = Text; carousel_container = Bild / Video-Reihe
direct_reply_count	Integer-Wert	Anzahl der direkten Antworten (Antworten mit Antwort-Ebene 1)

Tabelle 4.9: Informationen zum Verfasser des Beitrags

Attribut	Wert	Beschreibung
is_private	boolescher Wert	true = Nutzerprofil ist privat; false = Nutzerprofil ist öffentlich
is_verified	boolescher Wert	true = Nutzerprofil ist verifiziert; false = Nutzerprofil ist nicht verifiziert
user_id	numerische Zeichenfolge	elfstellige Nutzer-ID
full_name	Zeichenfolge	vollständiger Name
profile_pic_url	Zeichenfolge	Profibild-URL
username	Zeichenfolge	Nutzername

Tabelle 4.10 enthält Attribute, welche den Freundschaftsstatus zwischen Nutzer- und Verfasserprofil näher beschreiben.

Tabelle 4.10: Freundschaftsstatus zwischen Nutzer- und Verfasserprofil

Attribut	Wert	Beschreibung
followed_by	boolescher Wert	true = Verfasser folgt dem Nutzerprofil; false = Verfasser folgt dem Nutzerprofil nicht
following	boolescher Wert	true = Nutzerprofil folgt dem Verfasserprofil; false = Nutzerprofil folgt dem Verfasserprofil nicht
is_bestie	boolescher Wert	true = Verfasser gehört zu ‘engen Freunden‘; false = Verfasser gehört nicht zu ‘engen Freunden‘
is_restricted	boolescher Wert	true = Verfasserprofil wurde eingeschränkt; false = Verfasserprofil wurde nicht eingeschränkt
outgoing_request	boolescher Wert	true = Folge-Anfrage wurde gestellt; false = Folge-Anfrage wurde nicht gestellt

Alle Attribute der Tabelle 4.8, Tabelle 4.9 sowie Tabelle 4.10 gehen aus einem JSON-Dokument hervor. Für einen besseren Überblick wurden die Attribute unterteilt und tabellarisch aufbereitet dargestellt.

Die mehrmalige Extraktion der Datenbank-Tabelle zeigte, dass die Tabellen-Einträge regelmäßig erneuert bzw. ersetzt werden, wodurch Daten zu älteren Beiträgen nicht mehr in der Datenbank auffindbar sind. In welchen Zeitabständen die Daten erneuert werden oder welche Aktionen die Aktualisierung auslösen, konnte nicht nachvollzogen werden.

4.4 XML-Datenanalyse

Die folgenden Abschnitte beschäftigen sich mit relevanten XML-Dateien, welche im Ordner ‘shared_prefs‘ des Stammverzeichnisses hinterlegt sind. Einige der Dateien weisen jedoch lediglich eine Deklaration auf, durch welche ein XML-Dokument eingeleitet wird. Andere weisen neben der Deklaration wenige grundlegende Informationen, wie Einstellungen des Nutzerprofils, auf, die jedoch in relevanteren Dateien erneut aufgegriffen werden. Auf Grund dessen werden in den folgenden Abschnitten die als relevant erachteten XML-Dokumente näher beleuchtet.

4.4.1 NOTIFICATION_CHANNELS.xml

Die XML-Datei ‘NOTIFICATION_CHANNELS.xml‘ enthält keine spezifischen Eigenschaften des Nutzerkontos. Der Inhalt entspricht einer Listung von Benachrichtigungseinstellungen, welche die untersuchte Anwendung betreffen. Darunter zählen bspw. Vibrationseinstellungen, Einstellungen der Benachrichtigungstöne, Priorisierung der Benachrichtigungsart oder Einschränkungen von Benachrichtigungen.

4.4.2 ig_cask_metadata_store.xml

Angaben zur automatisierten Löschung oder Entfernung von Daten werden in der XML-Datei ig_cask_metadata_store.xml festgehalten. Einige in dieser Datei angegebenen Verzeichnispfade existieren innerhalb der Testdaten nicht. Grund dafür könnte sein, dass diese Pfade bereits automatisch durch die Anwendung gelöscht wurden.

4.4.3 devprefs.xml

Die Datei ‘devprefs.xml‘ beinhaltet Informationen zu Nutzeraktivitäten. Vermerkt sind der Zeitpunkt der letzten Hintergrundaktivität der Anwendung (last_app_background_timestamp) sowie der Zeitstempel der letzten Navigation innerhalb der Anwendung (last_navigation_timestamp) im Unix-Milliseconds-Format. Des Weiteren ist in der Datei eine Navigationshistorie (last_navigation_history) hinterlegt. Aus der Historie ist u.a. zu entnehmen, in welcher Reihenfolge die Hauptseiten der Anwendung Threads besucht wurden.

Zudem ist in der Datei eine Navigationskette aufgeführt. Auch diese bezieht sich augenscheinlich auf kürzlich durchgeführte Aktionen unter Angabe von Zeitstempeln. Die Datei weist weitere Attribute mit entsprechenden Werten auf, wie das letzte Navigationsziel, welche die jüngsten Aktivitäten der Anwendung darstellen.

4.4.4 com.instagram.barcelona_preferences.xml

‘com.instagram.barcelona_preferences.xml‘ ist eine Datei, die Informationen zum Nutzerkonto enthält. Auch hierbei sind verschiedene Zeitstempel aufgeführt. Außerdem ist eine Google Advertising ID, also eine Werbe-ID, aufgeführt, die für personalisierte Werbezwecke genutzt wird. Der Kernteil der Datei besteht aus drei Elementen mit den Bezeichnungen ‘account_linking_family_map_data‘,

‘current‘ und ‘user_access_map‘. Das Element ‘account_linking_family_map_data‘ weist Daten zum Nutzerkonto auf. Im Folgenden sind ausgewählte Punkte des Elements aufgeführt. Da jedes dieser Attribute bereits in anderen Tabellen, wie Tabelle 4.6, erläutert wurde, folgt hier lediglich eine Aufzählung:

- Nutzer-ID (user_id)
- vollständiger Name (full_name)
- Nutzername (username)
- Verifizierungsstatus (is_verified)
- Profilbild-URL (profile_pic_url)

Das Element ‘user_access_map‘ weist Wiederholungen des ‘account_linking_family_map_data‘ Elements auf, welche nicht erneut erwähnt werden. In Tabelle 4.11 sind einige Attribute des ‘user_access_map‘-Elements aufgeführt. Alle Daten beziehen sich weiterhin auf das betrachtete Nutzerkonto.

Tabelle 4.11: Element ‘user_access_map‘

besties_count	**Integer-Wert**	**Anzahl der besten Freunde**
biography	Zeichenkette	Inhalt der Biografie
follower_count	Integer-Wert	Anzahl der Personen, die dem Threadskonto folgen
following_count	Integer-Wert	Anzahl der Personen, denen auf Threads gefolgt wird
hd_profile_pic_info	Element mit weiteren Attributen	URL, Breite und Höhe des Profilbildes
media_count	Integer-Wert	Anzahl der geteilten Beiträge

Das Element ‘current‘ enthält neben einigen bereits erwähnten Attributen aus ‘account_linking_family_map_data‘ spezifischere Daten zur Art des Nutzerkontos. Insbesondere wird auf Berechtigungen und Einschränkungen in Bezug auf Sonderfunktionen eingegangen. Unter anderem sind daraus folgende Informationen, welche in Tabelle 4.12 gelistet sind, zu entnehmen. Wiederholungen aus dem Element ‘account_linking_family_map_data‘ werden nicht erneut aufgeführt.

Tabelle 4.12: Element ‘current‘

Attribut	Wert	Beschreibung
account_type	Integer-Wert	1 = persönliches Konto liegt (vermutlich) vor[4]; Integer-Werte anderer Kontotypen anhand der Testdaten nicht nachvollziehbar
can_be_tagged_as_sponsor	boolescher Wert	true = Nutzerkonto kann als Sponsor[5] markiert werden; false = Nutzerkonto kann nicht als Sponsor markiert werden
can_boost_post	boolescher Wert	true = Einblenden von Werbung erlaubt; false = Einblenden von Werbung nicht erlaubt
can_see_organic_insights	boolescher Wert	true = Zugriffsberechtigung auf Daten und Statistiken von sozialen Medien; false = keine derartige Zugriffsberechtigung
can_generate_nametag	boolescher Wert	true = Berechtigung zur Generierung eines Quick Response (QR)-Codes; false = keine derartige Berechtigung
wa_addressable	boolescher Wert	true = weist möglicherweise auf ein WhatsApp-Konto hin; false = kein WhatsApp-Konto vorhanden
is_muted_words_custom_enabled	boolescher Wert	true = Aktivierung des Wortfilters; false = Deaktivierung des Wortfilters (benutzerdefinierte Wortliste)
is_muted_words_spamscam_enabled	boolescher Wert	true = Aktivierung des Wortfilters; false = Deaktivierung des Wortfilters (standartisierte Wortliste)
supervision_info	Element mit weiteren Attributen	Element enthält Informationen zu täglichen Zeitlimits, Altersangabe, Ruhefunktion, Pausenzeiten, etc.

Einige der Attribut-Beschreibungen des Elements ‘current‘, können lediglich vermutet werden. Die Testdaten wurden anhand von persönlichen Konten generiert, durch welche das Testen von einigen Sonderfunktionen nicht möglich ist.

[4] Das Threadskonto basiert auf dem Instagramkonto. Instagram bietet verschiedene Kontotypen, wie persönliche, Geschäfts- und Künstlerkonten, an.

[5] https://help.instagram.com/544284327840525/?helpref=search&query=sponsor&search_session_-id=d8231abf3fe4cbcda63ebefd1e20b9c2&sr=3

4.4.5 <Nutzer-ID>_USER_PREFERENCES.xml

Die Datei ‘<Nutzer-ID>_USER_PREFERENCES.xml‘ listet verschiedene Threads-Ereignisse unter Angabe von Zeitstempeln im Unix-Milliseconds-Format sowie aktuelle Einstellungen oder Benachrichtigungsangaben. In der folgenden Tabelle 4.13 sind einige Attribute der Datei mit Erläuterung aufgeführt.

Tabelle 4.13: Inhalt der <Nutzer-ID>_USER_PREFERENCES.xml-Datei

Attribut	Wert	Beschreibung
linked_fb_page_id	numerische Zeichenfolge	verlinkte Facebook-Nutzer-ID (durch Anwendung automatisch erkannt)
feed_last_server_ xposting_turn_on_ time_in_second	numerische Zeichenfolge	Zeitpunkt, zu dem ein Beitrag auf einer weiteren verknüpften Plattform geteilt wurde
HAS_NEW_ NOTIFICATION	boolescher Wert	true = Hinweis auf neue Benachrichtigung(en); false = keine Benachrichtigungen
casper_target_ event_timestamps	numerische Zeichenfolgen	Sammlung von Zeitstempeln, die Aktivitäten auf Threads kennzeichnen
recent_user_ searches_with_ts	Element mit weiteren Attributen	Attribute, die Informationen zu gesuchten Nutzerprofilen aufführen

4.5 Media-Verzeichnis-Analyse

Abbildung 4.7 zeigt die Ablagestruktur der Verzeichnisse ‘Movies‘ und ‘Pictures ‘ des Media-Verzeichnisses. Aus den generierten Testdaten geht hervor, dass im Verzeichnis ‘Pictures\Threads \‘ das Profilbild des betrachteten Nutzerkontos hinterlegt ist. Im Verzeichnis ‘Pictures\.thumbnails \‘ sind alle über Threads hochgeladenen Bild-Dateien sowie das Profilbild und Bildschirmfotos, die Inhalte der Anwendung Threads zeigen, als Vorschaubild hinterlegt. Auch das über Instagram hochgeladene Bild ist in diesem Verzeichnis gespeichert. Denkbar ist demnach, dass Bilder verschiedener Anwendungen unter diesem Pfad hinterlegt werden, wenn mehrere Anwendungen in aktiver Benutzung sind.

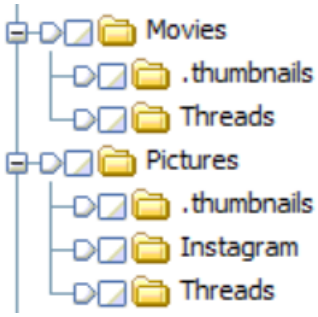

Abbildung 4.7: Media-Verzeichnis

Im Verzeichnis ‘Movies\Threads\‘ sind alle Videos hinterlegt, welche über Threads geteilt wurden. Das Verzeichnis ‘Movies\.thumbnails\‘ weist Vorschaubilder der geteilten Videos auf. Auch hier ist denkbar, dass weitere Videos und Vorschaubilder in diesen Verzeichnissen hinterlegt werden, wenn mehrere Anwendungen in aktiver Verwendung sind.

4.6 Verknüpfung der Daten

Die folgenden Abschnitte sollen eine Verbindung zwischen Bildern und Videos des Cache-Verzeichnisses und den Nutzerkonten, von denen die Medien geteilt wurden, aufweisen. Dafür werden folgende Daten herangezogen:

- die Tabelle ‘barcelona_user_feed_items‘ der Datenbank ‘barclona_feed_items_room_db_<Nutzer-ID>‘
- die Datei ‘cold_start\<Nutzer-ID>‘ aus dem Cache-Verzeichnis
- Dateien aus dem Ordner ‘http_responses‘ des Cache-Verzeichnisses
- Daten des Media-Verzeichnisses ‘\data\media\0\‘

Die folgenden Erläuterungen beziehen sich lediglich auf die Tabelle ‘barcelona_user_feed_items ‘ der eben genannten Datenbank, welche in diesem und folgenden Abschnitten als User Feed-Tabelle bezeichnet wird. Die eben genannte Datei aus dem Cache-Verzeichnis enthält eine Auflistung von Ereignissen, weshalb sie im Folgenden als Ereignis-Datei bezeichnet wird.

Jedes Ereignis der Ereignis-Datei führt Informationen eines geteilten Beitrags auf. Der Beginn eines Ereignisses ist an folgendem Aufbau zu erkennen:

{"text_post_app_thread":{"thread_items":[{"post":{"pk":

Dem Attribut ‘pk‘ ist eine 19-stellige numerische Zeichenfolge zugeordnet, welche dem Eintrag der Spalte ‘id‘ der User Feed-Tabelle, wie in Abbildung 4.6, entspricht. ‘pk‘ könnte für Primary Key (dt.: Primärschlüssel) stehen, da das Attribut ‘id‘ den Primärschlüssel der Tabelle darstellt. Das Attribut ‘data‘ weist teilweise identische Daten zum entsprechenden Ereignis der Ereignis-Datei auf. Nicht zu jedem Ereignis-Eintrag existiert ein entsprechender Eintrag in der User Feed-Tabelle und umgekehrt, weshalb in den weiterführenden Abschnitten die Zusammenhänge anhand beider Einträge beschrieben werden. Die Inhalte der Dateien des ‘http_responses‘-Verzeichnisses und der Ereignis-Datei sind identisch strukturiert, weshalb die Daten auf gleiche Weise miteinander verknüpft werden können. Die weiterführende Erläuterung erfolgt anhand der Ereignis-Datei.

4.6.1 Bilder des benutzerdefinierten Feeds

Die folgende Aufzählung enthält Attribute, mit dessen Hilfe Bilder des ‘images.stash\clean\‘-Verzeichnisses (vgl. Abschnitt 4.2.6) einem Nutzerkonto zugeordnet werden können:

- Das Attribut ‘media_type‘ verrät, welche Art von Beitrag (Text, Bild, Video, etc.) geteilt wurde (vgl. Tabelle 4.5). Es können auch mehrere Medien-Typen in einem Beitrag geteilt worden sein.

- Falls ein Bild- oder Video-Beitrag geteilt wurde, enthalten die Attribute ‘width‘ und ‘height‘ die Breite und die Höhe des Bildes oder Videos. Allerdings ist bei Höhe- und Breite-Attributen darauf zu achten, ob sie sich auf den Inhalt des Beitrags oder das Profilbild des Nutzerkontos beziehen.
- Aus den Informationen der Ereignis-Datei geht außerdem ein ‘client_cache_key‘ hervor, welcher auch in der Spalte ‘data‘ der User Feed-Tabelle im entsprechenden URL-Attribut des Bildes zu finden ist und unmittelbar nach der Zeichenfolge ‘ig_cache_key‘ folgt.
- Attribute, die sich auf ein Bild oder Video beziehen, werden eingeleitet durch: "image_versions2":{"candidates":[{

Der Wert des Attributs ‘client_cache_key‘ entspricht dem 19-stelligen numerischen Wert des Attributs ‘id‘in Base64-codierter Form. Der Base64-codierte ‘client_cache_key‘ ist zudem im Dateinamen des Bildes aus dem ‘images.stash\clean\‘-Verzeichnis enthalten. Folgende Punkte erläutern den Zusammenhang:

- Beispiel des Bild-Dateinamens: MzIyMDYxMjQ2MDM4MTQzNzc4NQ==.2-ccb7-5_1080_1438
- Der orange gefärbte Teil zeigt den Base64-codierten ‘client_cache_key‘, welcher decodiert der ID ‘3220612460381437785‘ entspricht.
- Demnach ist es möglich nach dem ‘client_cache_key‘ in den Dateinamen des ‘images.stash\clean\‘-Verzeichnisses zu filtern, um das entsprechende Bild zu ermitteln.
- Umgekehrt besteht die Möglichkeit, den orange gedruckten Teil zu decodieren und nach der daraus resultierenden ID in der Spalte ‘id‘ der User Feed-Tabelle zu filtern, um nähere Informationen zum Bild zu erhalten.
- Die blau gefärbten Teile sind identisch zu den Werten der Breiten- und Höhe-Attribute.

Nicht für jedes Bild im Cache-Verzeichnis ist ein entsprechender Eintrag in der Datenbank-Tabelle oder der Ereignis-Datei vorhanden. Teilweise sind auch für Einträge der Tabelle oder der Ereignis-Datei keine zugehörigen Bilder im Cache-Verzeichnis hinterlegt.

4.6.2 Profilbilder

Profilbilder wurden ebenfalls im Verzeichnis ‘images.stash\clean\‘ hinterlegt, weisen als Dateiname jedoch eine URL auf (vgl. Abschnitt 4.2.6). Um Profilbilder mit Informationen aus der Ereignis-Datei und der User Feed-Tabelle zu verbinden, sind die URLs der Profilbilder von Bedeutung. Die Profilbild-URL ist in der Ereignis-Datei unter dem Attribut ‘profile_pic_url‘ zu finden. In der User Feed-Tabelle hingegen werden Informationen zum Profil mit der Zeichenfolge » "hd_profile_pic_url_info":{ « eingeleitet. Daraufhin folgen die Attribute ‘width‘, ‘height‘ sowie ‘url‘.

Sofern jede der eben erwähnten URLs derselben Aktion zugehörig sind, weist jede der URLs einen identischen Abschnitt auf, welcher aus drei durch Unterstriche getrennte numerischen Zeichenfolgen besteht. Dieser kann beispielhaft folgendermaßen aussehen:

382940626_336878735406309_2029451286640383094

Mit Hilfe der identischen Abschnitte ist die Verknüpfung von Profilbildern und Nutzer-Informationen möglich. Hierbei anzumerken ist, dass nicht zu jedem Profilbild ein Datenbank- oder Ereignis-Eintrag vorhanden sein muss. Wie sich der identische Abschnitt zusammensetzt, kann durch die in diesem Rahmen durchgeführten Analysen nicht nachvollzogen werden. Keine der drei durch Unterstriche voneinander getrennten Zahlenfolgen tritt in einem anderen analysierten Zusammenhang auf.

4.6.3 Videos des benutzerdefinierten Feeds

Die betrachteten Videos sind im ‘ExoPlayerCacheDir‘-Verzeichnis, wie in Abschnitt 4.2.3 beschrieben, hinterlegt. Das folgende Beispiel zeigt den Aufbau des Video-Dateinamens, anhand dessen Informationen zum Video identifiziert werden können.

3217578432157841396_62219277051.null.865644161440947vd.-1.316256721_983162959446655_7544603757201016007_n.mp4.0.1698149166759.v2.exo

Der orange gedruckte Abschnitt entspricht dem Eintrag des ‘id‘-Attributs, also dem Primärschlüssel der User Feed-Tabelle. In der Datenbank-Tabelle kann somit nach der orange gefärbten ID gefiltert werden, um an mögliche Informationen zur Video-Datei zu gelangen. Auch hier ist anzumerken, dass nicht zu jedem Video ein Datenbank- oder Ereignis-Eintrag vorhanden sein muss. Es können auch Datenbank- oder Ereignis-Eintrage existieren, die auf Videos hinweisen, welche in den Anwendungsdaten nicht wiederzufinden sind.

Ein Grund für keinen identischen Treffer in der User Feed-Tabelle könnte jedoch auch der geteilte Medien-Typ sein, welcher in Tabelle 4.5 unter dem Attribut ‘media_type‘ näher erläutert wird. Bspw. wird einer Repost-Aktion, also dem erneuten Teilen eines Beitrags, eine ID zugewiesen, die nicht identisch zu der des ursprünglichen Beitrags ist. Die ID des ursprünglichen Beitrags wäre jedoch bei einem vorhandenen Eintrag in der Spalte ‘data‘ vorzufinden. Durch die Analyse weiterer Attribute des ‘data‘-Eintrags, wie dem Medien-Typ, kann die Verwendung des Videos näher spezifiziert bzw. eingeordnet werden.

Eine weitere Möglichkeit besteht darin, nach dem blau gedruckten Teil des Dateinamens in der Spalte ‘data‘ zu filtern. Auch dadurch können zugehörige Daten detektiert werden. Die Ereignis-Datei kann nach beiden farbig gedruckten Zeichenketten durchsucht werden, um Informationen zum Video zu lokalisieren, falls diese vorhanden sind.

Handelt es sich um eine Video-Reihe, was heißt, dass mehrere Videos gleichzeitig in einem Beitrag geteilt wurden, dann enthalten alle Video-Dateinamen einer Reihe eine identische ID (im Beispiel orange gefärbt). Unterscheiden lassen sich Videos einer Reihe anhand des blau gefärbten Abschnittes, welcher für jedes Video individuell ist.

4.6.4 Media-Verzeichnis

Die im Media-Verzeichnis gespeicherten Bilder und Videos, welche im Zusammenhang mit Threads stehen, weisen keine Dateinamen auf, die innerhalb der Threads-Anwendungsdaten erneut auftreten. Die Dateien der ‘.thumbnails‘-Verzeichnisse weisen fortlaufend nummerierte Dateinamen auf. Dies

erfolgt vermutlich in der Reihenfolge, in der die Daten abgelegt werden. Threads hingegen verwendet andere Vorgehensweisen zur Dateibezeichnung, weshalb mit Hilfe der Dateinamen keine Verbindung ersichtlich wird. Auch die über ExifTool aufgerufenen Metadaten weisen keine Verbindung auf. Lediglich der direkte Vergleich der Bilder und Videos mit den über Threads geteilten Medien ermöglicht eine Verknüpfung.

Auch die Dateien der beiden Verzeichnisse mit der Bezeichnung ‘Threads‘ weisen Dateinamen auf, die nicht sinnvoll mit den Anwendungsdaten in Verbindung gebracht werden können. Weitere Metadaten lassen ebenfalls keine Verknüpfung zu. Als Verbindung können für diese Daten lediglich der Verzeichnisname ‘Threads‘ oder der direkte Vergleich der Bild- bzw. Video-Inhalte dienen.

4.7 Aufbereitung der Daten als UFED-Bericht

Der UFED-Bericht beinhaltet Informationen zu installierten Anwendungen, zugehörige Nutzerprofile sowie Chatverläufe und weitere Daten, welche übersichtlich in Kategorien unterteilt und in tabellarischer Form aufgelistet sind. Die weiterführenden Unterabschnitte gehen auf Informationen zu Threads ein, welche aus dem UFED-Bericht hervorgingen. Dies soll einen Einblick geben, inwiefern und wie tiefgreifend Daten bezüglich der noch wenig erforschten Anwendung erkannt werden.

4.7.1 Installierte Anwendungen

Unter der Auflistung der auf dem jeweiligen Mobilgerät installierten Anwendungen, wie in Abbildung 4.8 zu entnehmen, erscheint u.a. ein Tabelleneintrag, welcher der Anwendung Threads anhand der Anwendungsidentifikation ‘com.instagram.
barcelona‘ zugeordnet werden kann. Des Weiteren geht aus dem Eintrag das Installationsdatum und die Version des Threads-Dienstes hervor. Ein (Anwendungs-) ‘Name‘ konnte dem Eintrag jedoch nicht zugeordnet werden. Auch die Einordnung als sozialer Netzwerkdienst oder Microblogging-Plattform unter ‘Categories‘ ist laut diesem Eintrag nicht zu erkennen.

Name	Version	Categories	Description	Identifier	Purchase Date
	309.0.0.39.109	App may not be from store		com.instagram.barcelona	26.09.2023 11:13:45(UTC+2)

Abbildung 4.8: Threads-Eintrag unter den installierten Anwendungen

4.7.2 Nutzerkonten

Zur installierten Anwendung Threads konnte ein entsprechendes Threads-Nutzerkonto ermittelt werden, welches in Abbildung 4.9 zu sehen ist. Als ‘Quelle‘ ist hierbei die Bezeichnung ‘Threads‘ aufgeführt. Zum Nutzerkonto kann des Weiteren der Nutzername (Attribut ‘Username‘) und der vollständig angegebene Name (Attribut ‘Name‘) extrahiert werden. Unter ‘Additional Info‘ ist der festgelegte Steckbrief angegeben und aus ‘Notes‘ geht die Anzahl der gefolgten und folgenden

Threads-Profilen hervor. Außerdem ist angegeben, ob ein Profil- bzw. Kontaktbild gesetzt ist. Im vorliegenden Szenario existiert ein Profilbild, dessen URL unter dem Punkt ‘Other Entries‘ gelistet ist. Neben der Profilbild-URL sind zudem die Threads- und Facebook-Nutzer-ID ergänzt.

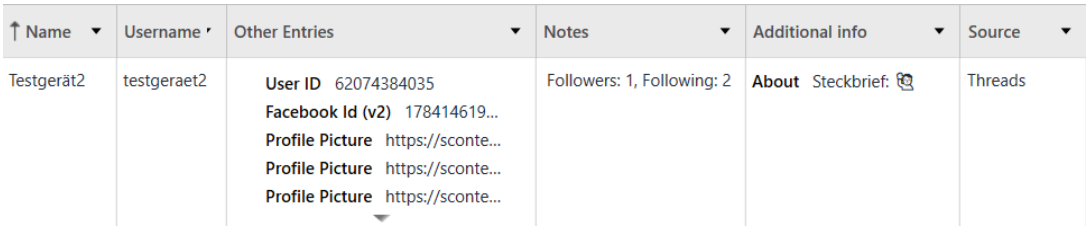

Abbildung 4.9: Threads-Nutzerkonto im UFED-Bericht

Der UFED-Bericht gibt zudem an, aus welchen Dateien die Informationen entnommen wurden. Im Falle des Threads-Nutzerkontos wurden die Informationen aus den Dateien des ‘http_responses‘-Verzeichnisses extrahiert, welches in Abschnitt 4.2.4 erläutert ist.

4.7.3 Kontakte

Ähnlich wie bei Nutzerkonten ist es möglich unter ‘Sources‘ nach ‘Threads‘ zu filtern, um entsprechende Kontakt-Einträge zu detektieren. Zu Threads-Kontakten ist der (vollständige) ‘Name‘ sowie unter ‘Other Entries‘, falls gesetzt, eine Profilbild-URL, die Threads- und Facebook-Nutzer-ID und der Threads-Nutzername aufgeführt. Zudem werden die Anzahl der gefolgten und folgenden Threads-Profile angegeben und unter dem Punkt ‘Interaction Statuses‘ ist der gegenseitige Folge-Status notiert. Als ‘Additional Info‘ ist der Biografie- bzw. Steckbrief-Eintrag angegeben. Im Falle mehrerer existierender Threads-Konten ist unter ‘Account‘ die ID des Nutzerprofils angegeben, von welchem der Kontakt ausgeht. Abbildung 4.10 zeigt einen Kontakt-Eintrag am Beispiel des Kontakts von Testgerät 1.

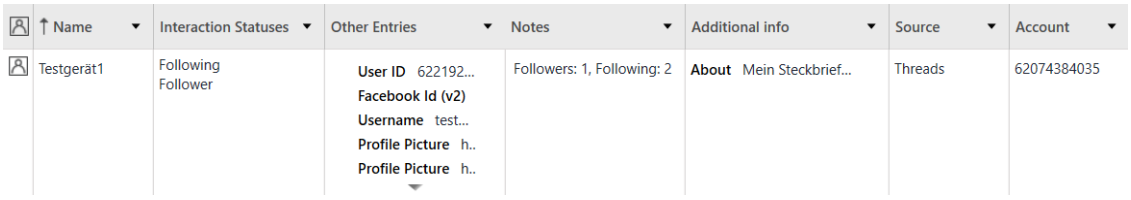

Abbildung 4.10: Auszug der Kontaktenliste des UFED-Berichtes

In Bezug auf die als Threads-Kontakt aufgeführten Nutzerprofile ist zu erwähnen, dass nicht zu jedem Profil eine aktive Verbindung besteht. Einige der aufgeführten Threads-Kontakte wurden lediglich in der benutzerdefinierten ‘Gefolgt‘-Seite vorgeschlagen, ohne dass eine aktive Interaktion erfolgte.

Auch die Informationen zu Threads-Kontakten wurden aus den Daten des ‘http_responses‘-Verzeichnisses extrahiert.

4.7.4 Beiträge

Im UFED-Bericht wird die Kategorie ‘Social Media‘ aufgeführt, welche Informationen über Threads-Beiträge enthält. In der Spalte ‘Source‘ kann nach dem Begriff ‘Threads‘ gefiltert werden, um relevante Einträge herauszufiltern. Folgende Informationen eines Beitrags werden dabei aufgeführt:

- Autor in Form von Nutzer-ID und vollständiger Nutzername
- textueller Inhalt
- Zeitpunkt des Hochladens
- Typ (Post = Beitrag oder Antwort; Share = Zitat)
- Quelle (z.B. Threads oder andere Plattformen)
- Reaktionen (Anzahl der ‘Gefällt mir‘-Angaben)
- Kommentare (Anzahl der Antworten)
- Account (Nutzer- ID des Kontos, auf welchem die Aktion festgestellt wurde (im Falle mehrerer Threads-Konten))
- Privatsphäre (Antwort- / Kommentar-Erlaubnis)

Die Informationen zu Threads-Beiträgen entnimmt der UFED-Bericht den Dateien des ‘http_responses‘-Verzeichnisses. Allein anhand der Daten des Berichtes lassen sich die aufgeführten Aktionen nicht in Antwort und Beitrag unterscheiden. Dementsprechend ist eine Zuordnung von Kommentaren bzw. Antworten zu bestimmten Beiträgen nicht möglich. Außerdem gehen aus der Auflistung der Beiträge und Antworten auch Inhalte der ‘Für dich‘-Seite hervor, die der Threads-Nutzer nicht aktiv wahrgenommen haben könnte.

4.7.5 Chats

Da Threads keine Direkt-Nachrichten-Funktion besitzt, konnten entsprechend keine Nachrichtenverläufe extrahiert werden. Jedoch wurden Instagram-Nachrichtenverläufe extrahiert, woraus die über Instagram ausgetauschten Threads-Beiträge hervorgehen. Die Threads-Beiträge sind zudem als ‘weitergeleitet‘ markiert. Aus den Informationen sind des Weiteren Nutzer- sowie vollständige Namen der Chatteilnehmer zu entnehmen.

4.7.6 Datenbanken

Dem UFED-Bericht des Testgerätes 2 können Threads-Datenbanken entnommen werden, die auch aus der Analyse des Testgerätes 1 hervorgingen. Das Stammverzeichnis der Datenbanken ist wie bei Testgerät 1 unter dem Ablageort ‘data\data\com.instagram.barcelona\databases\‘ zu finden. Es geht eine Datenbank mit der Bezeichnung ‘igtv_<Nutzer-ID> ‘ aus dem UFED-Bericht hervor, die unter den Anwendungsdaten von Testgerät 1 nicht existiert. Der Inhalt besteht aus vier Tabellen, aus denen ein Identitäts-Hashwert und die Lokalisierung sowie Spracheinstellung des Gerätes hervorgehen. Der Gerätestandort und die verwendete Sprache geht aus der Tabelle ‘android_metadata‘ hervor, welche in jeder der analysierten Datenbanken vorhanden ist. Da diese Tabelle in jeder Datenbank mit gleichem Inhalt existiert, ist davon auszugehen, dass diese Daten automatisch durch Android generiert werden. Die Datenbank ‘igtv_<Nutzer-ID> ‘ enthält somit keine zusätzlichen Informationen.

4.8 Rekonstruktion des Thread-Verlaufs

Als Thread-Verlauf ist die chronologische Reihenfolge der hochgeladenen Threads-Beiträge gemeint. Zu jedem Beitrag kann es potenzielle Antworten geben, welche ebenfalls in die Rekonstruktion einbezogen werden können.

Wie in Abschnitt 4.7.4 beschrieben, werden im UFED-Bericht die Aktionen nicht in Beitrag und Antwort unterschieden, wodurch auch keine Verbindung zwischen Beitrag und Antwort anhand dieser Daten hergestellt werden kann. Als Datenquelle werden jedoch die Dateien des ‘http_responses‘-Verzeichnisses angegeben, dessen Inhalte in Abschnitt 4.2.4 erläutert sind.

Ein weiterer Ansatz, um Thread-Verläufe zu rekonstruieren, könnten Datenbank-Einträge sein. Die Tabelle ‘barcelona_feed_items_room_db_Nutzer-ID‘ beinhaltet Informationen zu Beiträgen. Jedoch stellte sich im Zuge der Auswertung heraus, dass die Datenbank-Einträge regelmäßig gelöscht bzw. ersetzt werden, wodurch eine vollständige Rekonstruktion durch eine einmalige Extraktion der Testdaten nicht möglich wäre. Des Weiteren fiel auf, dass in der Datenbank-Tabelle kaum Beitragsinformationen zu eigens erstellten Beiträgen vorhanden sind, was eine Rekonstruktion der Beiträge des betrachteten Nutzerkontos zusätzlich erschwert. Zudem könnten anhand der Datenbank-Einträge lediglich Beiträge, nicht aber Antworten rekonstruiert werden, da keinerlei Hinweise auf die Inhalte von Antworten in den Datenbanken enthalten sind.

Ähnliche Probleme treten bei der Ereignis-Datei des ‘cold_start‘-Verzeichnisses auf. Vorteil ist dabei zwar, dass mehr Informationen zu eigens erstellten Testdaten vorhanden sind, jedoch wird auch diese Datei regelmäßig erneuert, sodass Informationen zu älteren Beiträgen verloren gehen, wenn die Daten einer einmaligen Extraktion entnommen werden. Zudem liefert auch diese Datei keine Informationen zu Antworten bzw. Kommentaren.

Die Dateien des ‘http_responses‘-Verzeichnisses, welche auch im Rahmen des UFED-Berichtes aufbereitet wurden, eigenen sich vermutlich besser, um den Thread-Verlauf zu rekonstruieren. Die Daten enthalten zum einen Informationen zu Antworten bzw. Kommentaren. Zum anderen werden die Daten, zumindest über einen längeren Zeitraum, nicht gelöscht, wodurch keine Informationen zu älteren Beiträgen verloren gehen.

Für die Rekonstruktion der Verläufe eignet sich vermutlich eine Programmbibliothek, die Daten im JSON-Format in eine für Menschen besser lesbare Form umwandeln kann. Jeder Beitrag und dessen Antworten werden in einer separaten Datei gespeichert. Daher kann es sinnvoll sein, jeden Beitrag einzeln zu rekonstruieren, bevor ein vollständiger chronologischer Verlauf entsteht.

Zur Rekonstruktion eines Beitrags könnte damit begonnen werden, die Objekte des JSON-Dokuments als Beitrag oder Antwort zu identifizieren. Dafür bietet sich das Attribut ‘is_reply‘ an, welches mit den Werten ‘wahr‘ oder ‘falsch‘ angibt, ob eine Antwort oder ein Beitrag vorliegt. Ist der Beitrag identifiziert, können anschließend Informationen, wie Nutzername und Inhalt des Beitrags detektiert werden. Entspricht der Nutzername oder die Nutzer-ID nicht den Daten des Nutzerkontos, dessen Thread-Verlauf rekonstruiert werden soll, muss die Datei nicht weiter gelesen und kann ignoriert werden.

Ist der Beitrag von Relevanz, können anschließend Informationen aus den Antwort-Objekten entnommen werden. Kommentare bzw. Antworten können unterschiedliche Antwort-Ebenen besitzen, welche durch das Attribut ‘reply_level‘ ermittelt werden können. Dies ermöglicht es, die Hierarchie der Objekte zu bestimmen. Anschließend muss jede Antwort der nächst höheren Ebene, also der entsprechenden Antwort oder dem Beitrag, zugeordnet werden. Anhand des Erstellungszeitstempels können die Antworten außerdem in die richtige Reihenfolge gebracht werden. Wurde dieser Prozess für jede Datei durchgeführt, können abschließend die Beiträge mittels Erstellungszeitstempel chronologisch geordnet werden.

5 Fazit und Ausblick

Das Ziel dieser Arbeit war es, anhand einer forensischen Analyse die Ablagestruktur der Anwendungsdaten des sozialen Netzwerkdienstes Threads näher zu beleuchten. Dafür wurden Threads-Anwendungsdaten mittels Root-Zugriff auf ein Mobilgerät im Laufe der Testdatengenrierung mehrere Male extrahiert und analysiert.

Außerdem sollte anhand generierter Threads-Testdaten eines weiteren Mobilgerätes ein UFED-Bericht betrachtet werden, welcher aus einer forensischen vollständigen Dateisystem-Extraktion hervorging. Durch den UFED-Bericht konnten zudem einige Erkenntnisse, die aus den analysierten Testdaten hervorgingen, gestützt werden.

Die Recherche des aktuellen Forschungsstandes ergab, dass bis zum aktuellen Zeitpunkt keine öffentlichen wissenschaftlichen Arbeiten bezüglich Threads-Anwendungsdaten existieren. Auf Grund des daraus resultierenden großen Auswertungsbereichs konnte in dieser Ausarbeitung lediglich eine allgemein gehaltene Analyse der Daten durchgeführt werden. Die Arbeit konzentriert sich zudem auf die Auswertung von Android-Geräten. In dieser Hinsicht sind beispielsweise Analysen von Threads-Daten auf weitere Betriebssysteme, wie iOS, erweiterbar. Denkbar wäre auch eine intensivere Betrachtung der Attribute aus XML-Dateien oder Datenbaken, deren Bedeutungen innerhalb dieser Ausarbeitung nicht eindeutig definiert werden konnten.

Durch die mehrmalige Extraktion von Testdaten fiel zudem eine große Menge an auszuwertenden Daten an, was eine vollumfängliche Analyse der Daten aufgrund des limitierten Zeitumfangs erschwerte. In weiteren Arbeiten zum Thema Threads-Daten könnten statistische Analysen durchgeführt werden, die eine intensivere und / oder umfangreichere Betrachtung der Daten ermöglichen.

Die Testdaten basierten des Weiteren auf Nutzerdaten eines Benutzerkontos. Dies war in dieser Hinsicht sinnvoll, um nachvollziehen zu können, wie sich Threads-Daten innerhalb der Ablagestruktur grundlegend verhalten. In weiteren Forschungen wären diese Erkenntnisse durch eine Betrachtung des Verhaltens von Testdaten mehrerer Threads-Konten lokalisiert auf einem Gerät erweiterbar.

Zur Erstellung der Testdaten wurden zwei Mobilgeräte mit je einem Threads-Nutzerkonto verwendet. Mit Hilfe weiterer Nutzerkonten von zusätzlichen Geräten wäre eine Betrachtung von Threads-Daten eines passiven Nutzers möglich. Zudem wäre die Generierung von Testdaten öffentlicher und privater Konten besser umsetzbar. Des Weiteren könnten Testdaten mit Hilfe von anderen Konto-Typen (z.B. Geschäftskonten) generiert werden, um nachvollziehen zu können, wie sich unterschiedliche Konto-Typen auf die Anwendungsdaten auswirken.

Im Zuge der Auswertung fiel außerdem auf, dass die Daten der Datenbank ‘barcelona_feed_items_-room_db_<Nutzer-ID>‘ und der Datei im Verzeichnis ‘cold_start‘ regelmäßig gelöscht bzw. erneuert werden. Die Datenbank enthält weiterhin deutlich mehr Informationen zu empfohlenen Inhalten der ‘Für dich‘-Seite als zu Beiträgen des eigenen Nutzerkontos. Die Datei des ‘cold_start‘- Verzeichnisses hingegen, weist mehr Informationen zu durch das Test-Nutzerkonto generierten bzw. kommentierten Beiträgen auf. In welchen Abständen und weshalb die Daten erneuert werden, konnte im Rahmen

dieser Analyse nicht evaluiert werden. Ein Prinzip, nach welchem die Daten abgelegt werden, konnte ebenfalls nicht nachvollzogen werden. Weitere Tests könnten den Fokus auf Speichereigenschaften legen, um das Verhalten von Threads-Anwendungsdaten nachvollziehen zu können.

5.1 Umsetzung der Zielstellung

Im Vorfeld wurden einige Ziele formuliert, die im Zuge dieser Tests bearbeitet werden sollten. Im Folgenden wird darauf eingegangen, inwiefern diese Ziele erreicht wurden.

5.1.1 Angaben zum Nutzerkonto und dessen Einstellungen

Zum Ermitteln von Nutzerkonto-Informationen können verschiedene Dateien herangezogen werden. Einen Großteil der Profildaten geben XML-Dateien des ‘shared_prefs‘-Verzeichnisses preis. Die Nutzer-ID ist zudem Bestandteil der Namen einiger Anwendungsdateien. Vermutlich sind anhand der Nuter-IDs in Dateinamen die Daten unterschiedlicher Threads-Konten unterscheidbar, wenn mehrere Threads-Konten auf demselben Gerät verwendet wurden.

Auch Einstellungen des Nutzerkontos können über XML-Dateien ermittelt werden, wie bspw. Benachrichtigungseinstellungen. Des Weiteren enthalten Datenbank-Einträge Informationen zu Content-Filter-Einstellungen.

Anhand von Informationen zu Threads-Beiträgen, welche u.a. in Datenbanken oder HTTP-Antwort-Dateien zu finden sind, können zudem Einstellungen zur Kommentar- bzw. Antwortregelung individueller Beiträge ermittelt werden.

5.1.2 Aktivitäten des Nutzerprofils

Zu Aktivitäten des Nutzerprofils zählen zum Beispiel das Hochladen von Beiträgen. Aus den Testdaten ging hervor, dass Beitragsinformationen aus der Datenbank ‘barcelona_feed_items_room_db_-<Nutzer-ID>‘ sowie aus HTTP-Antworten und der Datei des ‘cold_start‘-Verzeichnisses zu entnehmen sind. Auffällig in diesem Testszenario war, dass in der Datei des ‘cold_start‘-Verzeichnisses vermehrt Einträge zu generierten Beiträgen des Test-Nutzerkontos zu finden sind. In der Datenbank hingegen sind vor allem Informationen zu Beiträgen des benutzerdefinierten Feeds der ‘Für dich‘-Seite enthalten.

Die HTTP-Antwort-Dateien enthalten außerdem Inhalte von Kommentaren bzw. Antworten, wohingegen die Datenbank und die Datei des ‘cold_start‘-Verzeichnisses lediglich Antwort- / Kommentarregelungen und die Anzahl der Direkt-Antworten aufführen.

5.1.3 Interaktionen mit anderen Nutzerprofilen

Durch die Datenbank-Einträge des benutzerdefinierten Feeds geht hervor, welche Beiträge der Nutzer bevorzugt. Jedoch sind daraus keine aktiven Interaktionen, wie ‘Gefällt mir‘-Angaben oder Kommentare bzw. Antworten des betrachteten Nutzerkontos zu entnehmen. Zusätzlich ist zu beach-

ten, dass der Algorithmus, welcher den benutzerdefinierten Feed generiert, durch Ansehen und Liken von Beiträgen entwickelt wird. Der Algorithmus muss also erst eine gewisse Menge an Interaktionen des Nutzers sammeln, um einen für den Benutzer adäquaten Feed generieren zu können.

Interaktionen in Form von Antworten sind aus den HTTP-Antwort-Dateien zu entnehmen. Daraus geht hervor, welche Profile unter den generierten Test-Beiträgen kommentiert / geantwortet haben oder auf welche Beiträge das betrachtete Profil reagiert hat.

5.1.4 Verknüpfung von Bildern / Videos mit Nutzerprofilen

Die in den Cache-Anwendungsdaten hinterlegten Bilder und Videos können anhand des Dateinamens spezifischen Aktionen zugeordnet werden. Allerdings kann es vorkommen, dass nicht zu jedem Bild oder Video Informationen zu Herkunft und Verwendung aufzufinden sind. Auch Beitragsinformationen können Hinweise auf Bilder und Videos geben, welche letztendlich jedoch nicht im Cache- oder anderen Verzeichnissen vorzufinden sind. Dies kann bspw. am regelmäßigen Löschen bzw. Entfernen von Daten liegen.

Des Weiteren werden durch das System Bilder und Videos bzw. Vorschaubilder im Media-Verzeichnis, außerhalb der Threads-Anwendungsdaten, hinterlegt. Mit Hilfe von Metadaten konnte jedoch kein Zusammenhang zwischen den Media-Verzeichnis-Daten und den Informationen aus den Anwendungsdaten gefunden werden. Lediglich die Bild- bzw. Video-Inhalte lassen einen Rückschluss auf die generierten Testdaten zu.

5.1.5 Aufbereitung der Daten als UFED-Bericht

Anhand des UFED-Berichtes können einige Erkenntnisse, die aus der Analyse der Testdaten von Testgerät 1 gewonnen wurden, nachvollzogen werden. Jedoch weisen die Inhalte des UFED-Berichtes teilweise abweichende Daten auf, was möglicherweise auf die unterschiedlichen Betriebssystem-Versionen zurückzuführen ist. Unter Verwendung unterschiedlicher Betriebssysteme kann die Abweichung entsprechend größer ausfallen.

Trotz der Tatsache, dass Threads eine bisher wenig untersuchte Anwendung ist, weist der UFED-Bericht einige Informationen zu den generierten Testdaten auf. Threads konnte als Anwendung identifiziert werden, jedoch ist der Anwendungs-ID ‘com.instagram.barcelona‘ keine Anwendungs-Bezeichnung zugeschrieben. Allerdings kann dem Bericht der Nutzername und die Nutzer-ID sowie weitere Eckdaten zum erstellten Nutzerkonto entnommen werden, welche eindeutig der Quelle ‘Threads‘ zugeschrieben werden.

Des Weiteren stehen unter der Kategorie ‘Kontakte‘ Nutzerkonten gelistet, zu denen das Threads-Nutzerkonto des Mobilgerätes augenscheinlich Kontakt hatte. Darunter sind jedoch einige Nutzerkonten, dessen Beiträge lediglich in der benutzerdefinierten ‘Für dich‘-Seite eingeblendet wurden und somit keinen direkten Kontakt zum Test-Nutzerkonto aufweisen.

Auch Informationen zu Beiträgen und Kommentaren können aus dem UFED-Bericht entnommen werden. Daraus geht u.a. hervor, von welchem Nutzerkonto der Beitrag oder Kommentar ausgeht. Jedoch unterscheidet der UFED-Bericht nicht zwischen Beitrag und Kommentar bzw. Antwort. Dementsprechend kann anhand dieser Daten keine Zuordnung zwischen Kommentaren und Beiträgen erfolgen.

Aus der Analyse lässt sich schließen, dass durch den UFED-Bericht Nutzeraktionen aufbereitet dargestellt, jedoch teilweise nur schwierig in einen Kontext eingeordnet werden können. Beispielsweise unterscheidet die Aufbereitung nicht zwischen Beitrag und Antwort. Außerdem werden Nutzerkonten als Kontakte gelistet, da ein Algorithmus Beiträge fremder Nutzerkonten automatisch auf der ‘Für dich‘-Seite einblendet, obwohl zuvor keine Kontaktaufnahme erfolgte.

5.2 Zukünftige Analysen

Die Ergebnisse dieser Arbeit zeigen, dass die Ziele nicht vollumfänglich erreicht und Zusammenhänge nur teilweise nachvollzogen werden konnten. Zukünftige Analysen können demnach weitere Erkenntnisse in Bezug auf Anwendungsdaten von Threads auf Android-Geräten aufdecken. Da Threads grundsätzlich ein bisher kaum wissenschaftlich betrachtetes Gebiet ist, bleibt für weitere Analysen mit ähnlichen oder vollkommen anderen Schwerpunkten viel Forschungsraum.

Ein anderer Ansatzpunkt könnte den Datenaustausch zwischen Instagram und Threads thematisieren, da Threads eine Anwendung ist, dessen Nutzerkonto auf dem von Instagram basiert. Aus der Analyse der Testdaten ging bereits hervor, dass sich beide Plattformen Nutzerdaten, wie Nutzername und -ID, teilen. In dieser Hinsicht kann der Fokus auf Daten gelegt werden, welche durch beide Plattformen verarbeitet werden.

Im Rahmen dieser Arbeit konnten, auf Grund des begrenzten Bearbeitungszeitraumes, nicht alle aus den Testdaten hervorgegangenen Dateien näher beleuchtet werden. Auch der Inhalt von betrachteten Dateien konnte teilweise nicht eindeutig einer Funktion oder Bedeutung zugeordnet werden, was ebenfalls Raum für weitere Analysen bietet können.

Wie sich gelöschte Threads-Daten im Speicher verhalten, wurde im Zuge dieser Arbeit ebenfalls nicht überprüft, was jedoch für forensische Analysen durchaus eine wichtige Rolle spielen kann.

Des Weiteren wurde in der Einführung zum Thema Threads eine Ankündigung der Funktionserweiterung erwähnt, was eine Ergänzung der Anwendungsdaten zur Folge haben kann. Da Anwendungen permanent entwickelt und verbessert werden, erscheinen regelmäßig aktualisierte Versionen, welche weitere Untersuchungsmöglichkeiten bieten.

Das Veranlassen weiterer Analysen ist oftmals eine Frage der Kosten-Nutzen-Abwägung. In diesem Zusammenhang ist vor Augen zu führen, dass die Anwendung Threads zum momentanen Zeitpunkt erst seit wenigen Wochen in der EU zugelassen ist. Infolgedessen können die Nutzerzahlen stark zunehmen. Mit hoher Nutzeranzahl kann die Anzahl der Straftaten steigen, welche über oder mit Hilfe von Threads begangen werden könnten. Weitere Analysen im Bereich Threads würden demnach nicht unbegründet bleiben.

Literaturverzeichnis

[1] ARD/ZDF-Forschungskommission. „Social-Media-Nutzung 2019 bis 2022: Nutzung von Social Media allgemein 2021 und 2022 – mindestens einmal wöchentlich genutzt“. (2023), Adresse: https://www.ard-zdf-onlinestudie.de/tabellen-onlinenutzung/social-media-und-messenger/social-media/ (besucht am 11. 10. 2023).

[2] J.-H. Schmidt und M. Taddicken, Hrsg., *Handbuch soziale Medien* (Springer Reference Sozialwissenschaften). Wiesbaden: Springer VS, 2017, ISBN: 978-3-658-03765-9.

[3] ARD/ZDF-Forschungskommission. „Nutzung von Messengern: Nutzung von Messengern 2019 bis 2022 - täglich genutzt“. (2023), Adresse: https://www.ard-zdf-onlinestudie.de/tabellen-onlinenutzung/social-media-und-messenger/messenger/ (besucht am 11. 10. 2023).

[4] ARD/ZDF-Forschungskommission. „Social-Media-Nutzung 2019 bis 2022: Nutzung von Social-Media-Plattformen 2019 bis 2022 – mindestens einmal wöchentlich genutzt“. (), Adresse: https://www.ard-zdf-onlinestudie.de/tabellen-onlinenutzung/social-media-und-messenger/social-media/ (besucht am 11. 10. 2023).

[5] Bundeskriminalamt, *Cybercrime Bundeslagebild: Bundeslagebild 2022*, Wiesbaden, 2023.

[6] N. Dampz. „70 Millionen Nutzer: Traumstart für Twitter-Konkurrent Threads von Meta“. (2023), Adresse: https://www1.wdr.de/nachrichten/threads-twitter-konkurrenz-100.html (besucht am 10. 10. 2023).

[7] A. Heath. „Threads already has over 95 million posts“. (2023), Adresse: https://www.theverge.com/2023/7/6/23786108/threads-internal-activity-data-exclusive-instagram-meta (besucht am 10. 10. 2023).

[8] chartr. „Threads: Meta’s latest launch was a smash hit“. (2023), Adresse: https://www.chartr.co/stories/2023-07-10-1-instagram-springboarded-threads-to-100-million-users-in-record-time (besucht am 10. 10. 2023).

[9] L. Ceci. (2023), Adresse: https://www.statista.com/statistics/1401310/twitter-threads-app-daily-opens-engagement/ (besucht am 10. 10. 2023).

[10] ZDFheute. „Facebook-Konzern veröffentlicht Threads-App“. (2023), Adresse: https://www.zdf.de/nachrichten/wirtschaft/facebook-meta-threads-twitter-100.html (besucht am 10. 10. 2023).

[11] Haufe Online Redaktion. „Threads könnte doch bald in der EU verfügbar sein“. (2023), Adresse: https://www.haufe.de/compliance/recht-politik/dsgvo-und-digital-markets-act-threads-in-der-eu_230132_604256.html (besucht am 10. 10. 2023).

[12] C. Kainz, „Threads in der EU gestartet: Alles was ihr wissen müsst“, *futurezone.at*, 2023.

[13] Qatar News Agency. „Instagram stellt neue Funktionen für die Threads-Anwendung vor“. (2023), Adresse: https://www.qna.org.qa/de-DE/News-Area/News/2023-07/08/instagram-stellt-neue-funktionen-f%C3%BCr-die-threads-anwendung-vor (besucht am 11. 10. 2023).

[14] M. Bäcker, A. Dewald, F. C. Freiling und S. Schmitt, „Kriterien für die Priorisierung bei der Sicherung und Analyse digitaler Spuren“, *Datenschutz und Datensicherheit - DuD*, Jg. 36, Nr. 8, S. 597–602, 2012.

[15] J. Krokoszinski, „iPhone vs. Android: Wer hat die größeren Marktanteile?“, 2019.

[16] Instagram. „Instagram Threads | Instagram“. (2023), Adresse: https://about.instagram.com/de-de/threads (besucht am 17. 10. 2023).

[17] A. Ghafarian und J. Fredy, „Investigating Instagram Privacy Through Memory Forensics“, in *Intelligent Computing*, Ser. Lecture Notes in Networks and Systems, K. Arai, Hrsg., Bd. 711, Springer Nature Switzerland und Imprint Springer, 2023, S. 1263–1273, ISBN: 978-3-031-37716-7.

[18] C. Alisabeth und Y. Restu Pramadi, „Forensic Analysis of Instagram on Android“, *IOP Conference Series: Materials Science and Engineering*, Jg. 1007, Nr. 1, S. 012 116, 2020.

[19] A. O. Afolaranmi, „Prospect of Threads in Contrast to Twitter as an Online Social Network Tool for Conflict Resolution“, *British Journal of Multidisciplinary and Advanced Studies*, Jg. 4, Nr. 4, S. 1–13, 2023.

[20] G. Brunner, „Twitter-Alternative: Erste Euphorie um Threads scheint abgeflaut“, *Frankfurter Allgemeine Zeitung*, 2023.

[21] Deutschlandfunkkultur.de. „Threads: Bekommt Twitter erstmals echte Konkurrenz?“ (2023), Adresse: https://www.deutschlandfunkkultur.de/ernst-zu-nehmende-twitter-alternative-threads-100.html#Konkurrenz (besucht am 17. 10. 2023).

[22] tagesschau, „Facebook-Konzern Meta fordert Twitter mit Konkurrenz-App heraus“, *tagesschau.de*, 2023.

[23] M. Chin. „Instagram to shut down Threads“. (2021), Adresse: https://www.theverge.com/2021/11/17/22787783/instagram-threads-shutting-down-meta-messaging (besucht am 17. 10. 2023).

[24] NDR, „Threads: So funktioniert Zuckerbergs Twitter-Alternative“, *NDR*, 2023.

[25] Instagram. „Instagram kündigt neue textbasierte App an | Instagram Blog“. (2023), Adresse: https://about.instagram.com/de-de/blog/announcements/threads-instagram-text-feature (besucht am 11. 10. 2023).

[26] Y. Liu, Hrsg., *Social Media in China*. Wiesbaden: Springer Fachmedien Wiesbaden, 2016, ISBN: 978-3-658-11230-1.

[27] Meta. „Threads | Instagram-Hilfebereich“. (2023), Adresse: https://help.instagram.com/179980294969821 (besucht am 11. 10. 2023).

[28] Threads. „Threads“. (2023), Adresse: https://www.threads.net/login (besucht am 12. 10. 2023).

[29] Meta. „Introducing Threads: A New Way to Share With Text“. (2023), Adresse: https://about.fb.com/news/2023/07/introducing-threads-new-app-text-sharing/ (besucht am 12. 10. 2023).

[30] M. N. O. Sadiku und C. M. Akujuobi, *Fundamentals of Computer Networks* (Springer eBook Collection). Cham: Humana Press, 2022, ISBN: 978-3-031-09417-0.

[31] G. Schmalzried. „Neue Instagram-App Threads startet – aber nicht in Europa“. (2023), Adresse: https://www.br.de/nachrichten/netzwelt/neue-instagram-app-threads-startet-aber-nicht-in-europa,Tj8OLSG (besucht am 12. 10. 2023).

[32] E. Locard, *Die Kriminaluntersuchung und ihre wissenschaftlichen Methoden*. 1930.

[33] D. Labudde und M. Spranger, Hrsg., *Forensik in der digitalen Welt: Moderne Methoden der forensischen Fallarbeit in der digitalen und digitalisierten realen Welt*. Berlin und Heidelberg: Springer Spektrum, 2017, ISBN: 978-3-662-53801-2.

[34] E. Schicker, *Datenbanken und SQL: Eine praxisorientierte Einführung mit Anwendungen in Oracle, SQL Server und MySQL* (Lehrbuch), 5., aktualisierte und erweiterte Auflage. Wiesbaden: Springer Vieweg, 2017, ISBN: 978-3-658-16129-3.

[35] H. Jarosch, *Grundkurs Datenbankentwurf: Eine beispielorientierte Einführung für Studierende und Praktiker : mit 227 Abbildungen, 14 Tabellen und 5 Aufgaben mit Lösungen* (Lehrbuch), 4., überarbeitete und aktualisierte Auflage. Wiesbaden: Springer Vieweg, 2016, ISBN: 978-3-8348-2161-4.

[36] F. Herrmann, *Datenorganisation und Datenbanken: Praxisorientierte Übungen mit MS Access 2016* (Lehrbuch). Wiesbaden: Springer Vieweg, 2018, ISBN: 978-3-658-21331-2.

[37] C. Hummert und D. Pawlaszczyk, Hrsg., *Mobile Forensics – The File Format Handbook: Common File Formats and File Systems Used in Mobile Devices* (Springer eBook Collection), 1st ed. 2022. Cham: Springer International Publishing und Imprint Springer, 2022, ISBN: 978-3-030-98467-0.

[38] Android Developers. „SharedPreferences | Android Developers“. (2023), Adresse: https://developer.android.com/reference/android/content/SharedPreferences (besucht am 06. 11. 2023).

[39] M. Birbeck u. a., *Professional XML* (Programmer to programmer), 2. ed. Birmingham: Wrox Press, 2001, ISBN: 1861005059.

[40] T. Häberlein, *Technische Informatik: Ein Tutorium der Maschinenprogrammierung und Rechnertechnik* (Studium), 1. Aufl. Wiesbaden: Vieweg + Teubner, 2011, ISBN: 978-3-8348-1372-5.

[41] W. Ali, S. M. Shamsuddin und A. S. Ismail, „A Survey of Web Caching and Prefetching A Survey of Web Caching and Prefetching“, *International Journal of Advances in Soft Computing and its Applications*, Jg. 3, März 2011.

[42] D. Abts, *Masterkurs Client/Server-Programmierung mit Java: Anwendungen entwickeln mit Standard-Technologien* (Lehrbuch), 6. Auflage. Wiesbaden und Heidelberg: Springer Vieweg, 2022, ISBN: 978-3-658-37199-9.

[43] D. Westhoff, *Mobile Security: Schwachstellen verstehen und Angriffsszenarien nachvollziehen*. Berlin: Springer Vieweg, 2020, ISBN: 978-3-662-60855-5.

[44] I. M. Alsmadi, *Information Fusion for Cyber-Security Analytics* (Studies in Computational Intelligence Ser). Cham: Springer International Publishing AG, 2017, Bd. v.691, ISBN: 978-3-319-44257-0.

[45] Android Open Source Project. „System- und Kernel-Sicherheit“. (2023), Adresse: https://source.android.com/docs/security/overview/kernel-security?hl=de (besucht am 13. 10. 2023).

[46] G. Murugan u. a., „Implementation of New Secure File Transfer Protocol Using Triple-DES and MD5“, *International Journal of Advanced Science and Technology*, S. 4156–4170, 2020.

[47] M. Moreb, *Practical Forensic Analysis of Artifacts on iOS and Android Devices: Investigating Complex Mobile Devices*, 1st ed. 2022. Berkeley, CA: Apress und Imprint Apress, 2022, ISBN: 978-1-4842-8026-3.

[48] M. Rogge, „Forensik mobiler Endgeräte“, *Wirtschaftsinformatik & Management*, Jg. 7, Nr. 1, S. 22–25, 2015.

[49] Cellebrite. „Full File System Extraction - Mobile Device Forensics Archives“. (2023), Adresse: https://cellebrite.com/en/glossary/full-file-system-extraction-mobile-device-forensics/ (besucht am 20. 11. 2023).

[50] P. N. Astya, A. Swaroop, V. Sharma und M. Singh, Hrsg., *Proceeding, IEEE International Conference on Computing, Communication and Automation (ICCCA-2016): 29-30 April 2016*. Piscataway, NJ: IEEE, 2016, ISBN: 978-1-5090-1666-2.

[51] A. Raab-Düsterhöft. „Physische Extraktion“. IT-Forensik Wiki, Hrsg. (2023), Adresse: https://it-forensik.fiw.hs-wismar.de/index.php/Physische_Extraktion (besucht am 13. 10. 2023).

[52] S. Gunasekera, „Rooting Your Android Device“, in *Android apps security*, S. Gunasekera, Hrsg., Apress, 2020, S. 173–223, ISBN: 978-1-4842-1681-1.

[53] T. Kosse. „FileZilla - Frequently Asked Questions“. (2023), Adresse: https://filezilla-project.org/faq.php (besucht am 18. 10. 2023).

[54] Cellebrite. „Cellebrite Reader“. (2021), Adresse: https://cellebrite.com/de/cellebrite-reader-de/ (besucht am 26. 10. 2023).

[55] Z. Khalid, F. Iqbal, F. Kamoun, L. A. Khan und B. Shah, „Forensic investigation of Cisco WebEx desktop client, web, and Android smartphone applications“, *Annales des telecommunications*, Jg. 78, Nr. 3-4, S. 183–208, 2023.

[56] R. Hipp. „WAL-mode File Format“. (2022), Adresse: https://www.sqlite.org/walformat.html#the_wal_index_or_shm_file (besucht am 14. 12. 2023).

[57] R. Hipp. „The Rollback Journal“. (2022), Adresse: https://www.sqlite.org/lockingv3.html#rollback (besucht am 14. 12. 2023).

Eidesstattliche Erklärung

Hiermit versichere ich – Yasmin Scheithauer – an Eides statt, dass ich die vorliegende Arbeit selbstständig und nur unter Verwendung der angegebenen Quellen und Hilfsmittel angefertigt habe.

Sämtliche Stellen der Arbeit, die im Wortlaut oder dem Sinn nach Publikationen oder Vorträgen anderer Autoren entnommen sind, habe ich als solche kenntlich gemacht.

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

Mittweida, 03. Januar 2024	
Ort, Datum	Yasmin Scheithauer