FAST DETECT
SACHVERSTÄNDIGENBÜRO
FÜR IT-FORENSIK

HOCHSCHULE
MITTWEIDA
University of Applied Sciences

BACHELORARBEIT

Herr
Finn Hohlfeld, 53004

Analyse der Nutzungsspuren der Webclients von Threema und Instagram im Arbeitsspeicher

Mittweida, August 2023

Fakultät **Angewandte Computer- und Biowissenschaften**

BACHELORARBEIT

Analyse der Nutzungsspuren der Webclients von Threema und Instagram im Arbeitsspeicher

Autor:
Finn Hohlfeld

Studiengang:
IT-Forensik/Cybercrime

Seminargruppe:
CC19w1-B

Erstprüfer:
Prof. Ronny Bodach

Zweitprüfer:
M.Sc. Paul Prade

Einreichung:
Mittweida, 21.08.2023

Verteidigung/Bewertung:
Mittweida, 2023

Faculty of **Applied Computer Sciences and Biosciences**

BACHELOR THESIS

Analysis of the usage traces of the web clients of Threema and Instagram in the working memory

Author:
Finn Hohlfeld

Course of Study:
IT-Forensic/Cybercrime

Seminar Group:
CC19w1-B

First Examiner:
Prof. Ronny Bodach

Second Examiner:
M.Sc. Paul Prade

Submission:
Mittweida, 21.08.2023

Defense/Evaluation:
Mittweida, 2023

Bibliografische Beschreibung:

Hohlfeld, Finn:
Analyse der Nutzungsspuren der Webclients von Threema und Instagram im Arbeitsspeicher. – 2023. – 60 S.
Mittweida, Hochschule Mittweida – University of Applied Sciences, Fakultät Angewandte Computer- und Biowissenschaften, Bachelorarbeit, 2023.

Referat:

In dieser Bachelorarbeit werden die Artefakte im Arbeitsspeicher der Webclients des Instant-Messenger-Dienstes Threema und des Social-Media-Dienstes Instagram aus forensischer Sicht betrachtet. Hierfür werden die Funktionsweisen der Anwendungen und die auf dem Gerät im RAM enthaltenen Artefakte forensisch analysiert und diskutiert. Anhand der aus dieser Arbeit gezogenen Erkenntnisse sollen zukünftige forensische Untersuchungen, die in Verbindung mit einer oder beiden dieser Anwendungen stehen, unterstützt werden, gefundene Artefakte zu identifizieren und interpretieren.

Abstract:

This bachelor thesis looks at the artefacts in the working memory of the web clients of the instant messenger service Threema and the social media service Instagram from a forensic perspective. For this purpose, the functionalities of the applications and the artifacts contained on the device in the RAM are forensically analyzed and discussed. The knowledge gained from this work can be used to support future forensic investigations in connection with one or both of these applications, to identify and interpret the artifacts found.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

ALU . . . . . Arithmetic Logic Unit

CAS . . . . . column access strobe

CMD . . . . . Command Prompt

CPU . . . . . Central Processing Unit

CU . . . . . Control Unit

DDR . . . . . Double Data Rate

DRAM . . . . . Dynamic Random-Access-Memory

E2EE . . . . . End-to-end-encryption

HS . . . . . Hauptspeicher

IM . . . . . Instant-Messenger

MAR . . . . . Memory Address Register

MDR . . . . . Memory Data Register

MMU . . . . . Memory Management Unit

OS . . . . . Operating System

RAM . . . . . Random-Access-Memory

RAS . . . . . row access strobe

ROM . . . . . Read-Only-Memory

SRAM . . . . . Static Random-Access-Memory

VM . . . . . Virtuelle Maschine

VNM . . . . . Von-Neumann-Maschine

VS . . . . . virtueller Speicher

Danksagung

An dieser Stelle möchte ich mich bei all denen bedanken, die mich bei dieser Bachelorarbeit - aber auch während des gesamten Fernstudiums - emotional, finanziell und mit Ratschlägen und Hilfestellungen unterstützt haben. Zuerst will ich hier meinem Arbeitgeber FAST-DETECT danken, der mir das Fernstudium parallel zur Berufstätigkeit ermöglicht indem mich sowohl finanziell gefördert, auch als zeitlich freigestellt hat.
Insbesondere geht mein Dank auch an meine Arbeitskollegen Stefan Fuchs, Werner Poppitz und Michael Metzger, die mich nicht nur dazu ermutigt haben, das Fernstudium zu beginnen, sondern auch währenddessen jederzeit mit Rat und Tat zu Seite standen. Dank gilt auch meinen Kollegen und Freunden, die meine Arbeit sowohl auf inhaltliche, als auch auf sprachliche oder formale Mängel geprüft und Verbesserungsvorschläge angebracht haben.
Zuletzt bedanke ich mich bei meiner Freundin Alexandra, die mir stets den Rücken gestärkt und mich motiviert hat, sodass ich u. a. mehr Zeit und Kraft in die Erstellung der Bachelorarbeit investieren konnte.

1 Einleitung

Mit dem Begriff Instant-Messenger (IM) (deutsch: sofortiger Nachrichtenübermittler) werden Dienste bezeichnet, die eine Kommunikation zwischen zwei oder mehreren Anwendern in Echtzeit über das Internet ermöglichen. [1] Weltweit werden IM-Dienste von mehr als drei Milliarden Menschen (Tendenz steigend) auf Mobiltelefonen und Computern verwendet. [2] In Deutschland lag im Jahr 2022 die Nutzerzahl der Anwendung Instagram bei knapp 30.74 Millionen Nutzern. [3] Die Anzahl der Nutzer, welche die Chatanwendung Threema verwenden, lag im Jahr 2022 weltweit bei knapp elf Millionen. [4] Einige IM-Dienste bieten ihren Nutzern die Möglichkeit, den Dienst auch ohne Installation eines Programms oder einer Anwendung zu nutzen, indem sie Webclients des jeweiligen IM bereitstellen.

Heutzutage bieten viele IM mehr Funktionen als das simple Versenden und Empfangen von Textnachrichten. Bilder, Videos, Sprachnachrichten und weitere Inhalte können übermittelt werden. Zusätzlich wird häufig auch die Telefonie mit und ohne Videoübertragung mit einem oder mehreren Nutzern gleichzeitig ermöglicht. Durch Nutzung dieser Vielzahl an Funktionen können Nutzer weltweit in Kontakt stehen und sich miteinander austauschen. Diese Funktionen werden teilweise auch verwendet, um illegale Handlungen oder Absprachen zu diesen durchzuführen. Beispielhaft werden u. a. Betrug, Handel von illegalen Substanzen (BTM), sexueller Missbrauch und auch der Austausch von illegalen Inhalten über IM-Dienste geführt. Dass das Interesse an solchen Funktionen bei Nutzern, die entsprechende Handlungen durchführen wollen, gestiegen ist, ist u. a. anhand der steigenden Cyberkriminalitätsrate in den vergangenen Jahren zu erkennen. [5]

Aufgrund der steigenden Nutzerzahlen und der damit folgenden Verschiebung der zwischenmenschlichen Kommunikation in die digitale Welt, sowie der steigenden Cyberkriminalitätsrate besteht ein großes Interesse im Bereich der Strafverfolgung und entsprechend auch in der IT-Forensik darin, IM-Dienste forensisch auszulesen und analysieren zu können.

Hinweise

Zensierung

Zum Test verwendete Nutzerdaten und Kommunikationspartner wurden aus Datenschutzgründen zensiert oder anonymisiert. Jegliche Ähnlichkeiten mit realen Personen sind reiner Zufall.

Gender-Hinweis

„Zur besseren Lesbarkeit wird in dieser Arbeit das generische Maskulinum verwendet. Die in dieser Arbeit verwendeten Personenbezeichnungen beziehen sich – sofern nicht anders kenntlich gemacht – auf alle Geschlechter.“[6]

1.1 Motivation der Arbeit

Im Rahmen einer Post-Mortem-Analyse von Systemen fällt häufig auf, dass Nutzer vormals IM-Dienste im Webclient verwendet haben, jedoch zum Zeitpunkt der Analyse nicht mehr feststellbar ist, was der Nutzer getan bzw. geschrieben oder empfangen hat. Meist ist daraufhin nur noch feststellbar bzw. ausweisbar, dass die Nutzer mit an Sicherheit grenzender Wahrscheinlichkeit Kommunikationen über Webclients unterschiedlicher IM-Dienste geführt haben, die jedoch zum Zeitpunkt der Analyse weder feststellbar noch rekonstruierbar sind.
Im Verlauf der beruflichen Tätigkeiten als IT-Forensik Analyst[1] wurde festgestellt, dass u. a. die Anwendungen Threema und Instagram häufig durch Beschuldigte genutzt wurden. Aufgrund dessen steigt das Interesse, die Analysemöglichkeiten entsprechender Anwendungen zu explorieren. Anhand dieser Arbeit soll festgestellt werden, welche Möglichkeiten im Verlauf einer Sicherstellung bzw. Analyse bestehen, um mögliche relevante Inhalte zu sichern und daraufhin analysieren zu können.

1.2 Zielsetzung

Im Rahmen dieser Bachelorarbeit sollen die Möglichkeiten zur Identifikation, Extraktion und Rekonstruktion von Nutzungsspuren der Webclients von Threema und Instagram im Arbeitsspeicher analysiert und erläutert werden. Hierbei soll untersucht werden, in welcher Form und Vielfalt Webclients der Anwendungen Threema und Instagram Artefakte im Arbeitsspeicher hinterlassen. Dabei soll auch getestet werden, ob die Nutzung unterschiedlicher Internetbrowser einen Einfluss auf die gespeicherten Artefakte hat. Anschließend sollen mögliche festgestellte Artefakte aus dem Arbeitsspeicher extrahiert und rekonstruiert werden. Daraufhin sollen die Ergebnisse im Hinblick auf die Entwicklung eines Vorgehens verglichen werden. Ziel hierbei ist es, Ansätze für Vorgehen zu entwickeln, welche es zukünftigen forensischen Analysen vom Arbeitsspeicher ermöglichen, relevante Inhalte der Anwendungen Threema und Instagram extrahieren zu können.

1.3 Aufbau der Arbeit

Im Fokus dieser Arbeit steht die Analyse der Artefakte im Random-Access-Memory (RAM), welche möglicherweise durch die Webclients der IM-Dienste bzw. -Funktionen der Anwendungen Threema und Instagram entstanden sind. Es wird nicht der vollständige Funktionsumfang der Anwendung Instagram analysiert, da es sich bei dieser Anwendung um ein sogenanntes soziales Netzwerk handelt und die damit einhergehenden Funktionen dieser Anwendung das Forschungsinteresse dieser Arbeit vorerst übersteigen. Demzufolge liegt der Fokus auf den Chatfunktionen beider Anwendungen.

Zu Beginn der Arbeit werden theoretische Grundlagen und Definitionen von Fachbegriffen erläutert, u. a. die Zusammenführung der Begriffe 'Artefakt' und 'Spur' im Zusammenhang mit der IT-Forensik. Darauf folgend wird das allgemeine Prinzip der Kommunikation über IM-Dienste erläutert und auf die Anwendungen Threema und Instagram, inklusive der Chatfunktionen der jeweiligen Anwendungen, eingegangen. Abschließend wird der Aufbau, die Arbeitsweise und die Funktion des RAM aufgeführt, wobei auch kurz auf die Architektur heutiger Computer und die Funktionsweise von virtuellen Maschinen eingegangen wird.

[1] Beruf wird vom Verfasser dieser Bachelorarbeit seit Februar 2018 bei der Firma FAST-DETECT GmbH ausgeführt

In Kapitel 3 werden die für diese Arbeit verwendeten Methoden und das Vorgehen erläutert. Hierbei wird kurz auf die für die Durchführung verwendeten Programme sowie das Betriebssystem Windows 10 eingegangen. Dieses Kapitel unterteilt sich in die Planung und den Aufbau der Testumgebung, den Ablauf der jeweiligen Szenarien und das Erstellen der Testdatensätze[2].

Nachdem alle Datensätze erzeugt und extrahiert wurden, folgt in Kapitel 4 die Analyse der Daten und die daraus folgenden Erkenntnisse für die jeweilige Anwendung und das jeweilige Szenario. Anschließend werden die aus der Analyse gewonnenen Ergebnisse erläutert, gegenübergestellt und miteinander verglichen sowie ein Fazit gezogen.

Das letzte Kapitel fasst kurz die wichtigsten Punkte der Arbeit zusammen, listet die gewonnenen Erkenntnisse auf und zieht erneut ein Fazit. Abschließend folgt eine Erläuterung der Limitierungen dieser Arbeit, ein Ausblick für zukünftige Forschungsmöglichkeiten und Verbesserungsvorschläge und Hinweise für zukünftige Arbeiten im Bereich der forensischen Analyse von Artefakten im RAM.

1.4 Verwandte Literatur

Eine Suche nach wissenschaftlichen Publikationen, die ein ähnliches Themengebiet behandeln, ergab wenig verwertbare Ergebnisse. Überwiegend behandeln die vorliegenden Dokumente die Analyse der in dieser Arbeit gewählten Anwendungen auf einem mobilen Endgerät und die Auswertung der zu diesen Anwendungen gehörigen Ablagestrukturen und Datenbanken.
Es konnten nur wenige Veröffentlichungen gefunden werden, welche die Nutzung der jeweiligen Anwendungen in Verbindung mit Webclients und/oder Desktopanwendungen untersuchen. Jedoch lag auch hier der Fokus der Publikationen auf der Untersuchung von Datenbanken und weiteren Spuren der Anwendungen im aktiven Dateisystem.
Anschließend wurden Veröffentlichungen betrachtet, die nicht exklusiv die Analyse der genannten Anwendungen und/oder der Analyse der Webclients behandeln. Die im Verlauf dieser Arbeit durchgeführte Literaturrecherche zeigt deutlich, dass die Analyse von Artefakten im RAM aktiver behandelt und erforscht werden sollte.

Die Bachelorarbeit *'Analyse der Nutzungsspuren des Web Clients von WhatsApp und Telegram im Arbeitsspeicher'* wurde im August 2021 veröffentlicht.[7] In diesem Dokument wird der Arbeitsspeicher zweier virtueller Maschinen mit den Betriebssystemen Microsoft Windows und Linux analysiert, mit Fokus auf der Suche nach Artefakten der Webclients der Chatanwendungen Telegram und WhatsApp.
Dabei werden verschiedene Szenarien und Unterschiede in den Ergebnissen je Betriebssystem und Chatanwendung genauer betrachtet. Das Dokument kommt zu der Erkenntnis, dass innerhalb von RAM-Dumps Artefakte der Webclients der Chatanwendungen Telegram und WhatsApp feststellbar sind. Dabei sollen verwendete Betriebssysteme keinen direkten Einfluss auf die relevanten Inhalte der Webclients haben.
Eine Rekonstruktion der Chatverläufe war aufgrund fragmentierter Daten und teilweise fehlender Zusatzinformationen wie Zeitstempel etc. nur teilweise oder unter bestimmten Umständen möglich. Auch konnten nur Hinweise auf Dateiübertragungen festgestellt, aber die übertragenen Dateien

[2] Es werden pro Anwendung und pro Szenario eigene Testdatensätze erzeugt.

selbst nicht wiederhergestellt werden.
Das Dokument gibt an, dass die Rekonstruktion von Chatverläufen und Dateiübertragungen für WhatsApp wahrscheinlicher ist, als für die Chatanwendung Telegram.

In der Publikation *'Forensic Analysis of Communication Records of Web-based Messaging Applications from Physical Memory'*, die im Mai 2015 veröffentlicht wurde, behandeln die Autoren einen anderen Lösungsansatz und die Ergebnisse zur Analyse von Webbasierten Chatanwendungen innerhalb des RAMs.[8]
So werden unterschiedliche Chat- und Mailanwendungen (darunter Facebook, Skype, WhatsApp und Outlook), sowie die Internetbrowser Google Chrome, Mozilla Firefox, Opera und Microsoft Edge in die Tests mit einbezogen und die Ergebnisse gegenübergestellt.
Zur Erstellung und Extraktion der Daten aus dem RAM wird dabei das Werkzeug RAMAS verwendet.
Das Dokument betont die Problematik der forensischen Auswertung von Artefakten von Webclients unterschiedlicher Chatanwendungen im Bezug auf die Heterogenität der Datenformate einzelner Anwendungen und Browser, sowie die Persistenz einzelner Daten innerhalb des RAMs.

Das Paper *'Memory Forensics for Key Evidence Investigations in Case Illustrations'*, welches im Jahr 2013 veröffentlicht wurde, behandelt die Extraktion und Analyse von Artefakten der Chatanwendungen Skype Messenger und Facebook Messenger aus dem RAM.[9]
Im gewählten Vorgehen wird nach Erstellung der Testdaten das forensische Werkzeug MANDIANT Memoryze verwendet, um RAM-Dumps zu erzeugen. Anschließend werden die erzeugten RAM-Dumps mit dem Werkzeug WinHex analysiert. Anhand dieser Analyse können teilweise Chatnachrichten und auch Nutzerdaten mit Hilfe von festgestellten Identifikatoren festgestellt und extrahiert werden.

Die oben kurz zusammengefassten Publikationen befassen sich alle mit der Analyse von Artefakten im RAM und kommen zu dem Schluss, dass innerhalb des RAMs relevante Inhalte feststellbar und extrahierbar sind. Dies betont die Relevanz der weiteren Exploration von Vorgehen und Möglichkeiten im Bereich der RAM-Analyse.
Die aus den beschriebenen Untersuchungen gewonnenen Erkenntnisse wurden zur Erstellung und Planung der Testumgebung, Testdaten und Vorgehensweisen in Betracht gezogen.

2 Theoretische Grundlagen

Innerhalb dieses Kapitels werden theoretische Grundlagen erläutert, die für diese Bachelorarbeit Relevanz zeigen. Zu Beginn werden grundsätzliche Informationen zur IT-Forensik und den Spuren und Artefakten in der IT-Forensik erläutert. Anschließend wird der Begriff des Instant-Messaging (IM), sowie die End-to-end-encryption (E2EE) und Details zu den Anwendungen Threema und Instagram erklärt. Es folgen die Grundlagen der Kommunikation und der Bezug auf die jeweilige Anwendung, fokussiert auf die Messenger-Funktionen. Abschließend werden der Begriff RAM und die Eigenschaften und Arbeitsweise desselben dargelegt.

2.1 IT-Forensik

Unter dem Begriff der IT-Forensik, auch Computerforensik genannt, wird *„die Anwendung von Untersuchungs- und Analysetechniken, um Beweise von einem bestimmten Computergerät so zu sammeln und zu sichern, dass sie vor Gericht vorgelegt werden können.“* verstanden.[10] Dabei ist es das Ziel der forensischen Untersuchung, die Fragen nach dem „was, wo, wann und wie“ aufzudecken. Im Bereich der Strafverfolgung ist auch die Frage nach dem „wer“ relevant. [11][12] An die Vorgehensweise im Rahmen von IT-forensischen Untersuchungen werden die in der Tabelle 2.1 abgedruckten Anforderungen gestellt.[12]

Begriff	**Erläuterung**
Akzeptanz	Verwendete Methoden und Vorgehensweisen müssen in der Fachwelt bekannt und allgemein akzeptiert sein. Neue Verfahren und Methoden anzuwenden, ist nicht ausgeschlossen, benötigt aber Nachweise zur Korrektheit.
Glaubwürdigkeit	Robustheit und Funktionalität der Methoden ist auf jeden Fall gefordert und ggf. nachzuweisen.
Wiederholbarkeit	Alle verwendeten Hilfsmittel und Methoden müssen im Verlauf der Anwendung Dritter auf dasselbe Ausgangsmaterial dieselben Ergebnisse erzeugen.
Integrität	Sichergestellte Inhalte/Spuren sollten im Verlauf der Untersuchung nicht verändert werden. Die Integrität jedes einzelnen Beweismittels ist jederzeit nachzuweisen.
Ursache und Auswirkungen	Die Auswahl der Methoden muss es ermöglichen, logisch nachvollziehbare Verbindungen von Ergebnissen und Beweisspuren evtl. auch zu Personen herzustellen.
Dokumentation	Jegliche Handlung und jeder Schritt im Ermittlungsprozess ist angemessen zu dokumentieren.

Tabelle 2.1: Anforderung forensische Untersuchung BSI

Die Analyse der Daten auf relevanten Datenträgern wird in der IT-Forensik nach dem sogenannten S-A-P-Modell[3] unter Verwendung neuester Techniken und strenger Vorschriften durchgeführt. [13]

2.1.1 Artefakte und Spuren

Der Begriff Artefakt wird abhängig vom Fachgebiet interpretiert und genutzt. [14] Somit wird diesem Begriff keine allgemein verwertbare Definition gerecht. Fokussiert man sich auf den Bereich der IT, so wird der Begriff Artefakt wie folgt definiert:
„Ein digitales Artefakt ist ein Artefakt, dessen Gestaltung und Umsetzung mit informationstechnischen Mitteln erfolgt. Ein digitales Artefakt kann eingebettet sein in ein (physisches) Artefakt und kann gemeinsam mit diesem ein Produkt darstellen.“[15]
In Bezug auf die Informatik entstehen Artefakte demzufolge dort, wo durch elektronische Vorgänge Daten verarbeitet werden. Dies geschieht gerade bei Computern und mobilen Endgeräten, welche grundlegend Daten verwalten. Entsprechend sind dort entstandene Artefakte digital. Die IT-Forensik bedient sich einiger solcher Artefakte, die bei der Verwaltung von Daten anfallen, um digitale Informationen zu extrahieren, und beschreibt diese oder Teile daraus mit dem Synonym digitale Spur.[16]
Artefakte oder digitale Spuren werden z. B. durch Programme oder den Nutzer des Systems auf Speichermedien, wie z. B. auf einer Festplatte oder im Arbeitsspeicher (RAM) eines Geräts erzeugt und können Informationen enthalten, die im Rahmen einer IT-forensischen Untersuchung als relevant deklariert werden. Dabei handelt es sich beispielsweise um *„die Installationszeit, Logs, Benutzeraktivität, letzte Anwendung, persistente Daten (Cookies, Cache) und Applikationsdaten“*. [17]
Bezüglich Artefakten im RAM ist zu erwähnen, dass diese Informationen zu ausgeführten Prozessen, Programmen und Netzwerkverbindungen enthalten können.

2.2 Datenpersistenz

Als Persistenz ist allgemein das Bestehenbleiben eines Zustandes über längere Zeit oder auch die Beharrlichkeit bzw. Ausdauer definiert.[18]

In der Informatik bezieht sich die Persistenz bzw. auch Datenpersistenz auf die Fähigkeit von Daten, über einen längeren Zeitraum hinweg erhalten und gespeichert zu bleiben, auch nachdem der Prozess, das System oder das Programm, welches die Daten erzeugt hat, beendet wurde.[19]

Datenpersistenz besteht generell nicht im RAM, da es sich bei diesem um einen flüchtigen Speicher (siehe 2.5.1) handelt. Um eine Datenpersistenz in Bezug auf den RAM zu erstellen, müssten die Inhalte aus dem RAM auf einem nicht-flüchtigen/persistenten Speichermedium, wie z.B. Festplatten oder SSDs gespeichert werden. Dieser Vorgang wird als Speicherabbild (Memory Dump) oder Hibernation (siehe 2.6) bezeichnet.[19][20]

[3] Secure-Analyse-Present

2.3 Instant-Messenger-Dienste

Im Folgenden werden die allgemeinen Funktionen von IM-Diensten aufgelistet. Anschließend werden die Kommunikationsfunktionen der Anwendungen Threema und Instagram erläutert.

Heutzutage unterstützen IM-Dienste Funktionen, die weit über das Versenden und Empfangen von Textnachrichten hinausgehen. Im Laufe der Entwicklung von IM-Diensten wurde der Funktionsumfang kontinuierlich ausgebaut, wobei der essentielle Bestandteil, das Kommunizieren zwischen zwei oder mehreren Nutzern mittels textueller Nachrichten, weiterhin die Basis jeglicher Dienste darstellt. Innerhalb der Textnachrichten können mittlerweile sogenannte Emojis oder Emoticons[4] versendet werden, um hauptsächlich Hinweise auf die emotionale Gedankenrichtung oder Einstellung der sonst nur textuell vorliegenden Konversation zu geben.[21] Über die Zeit wurde der Funktionsumfang von IM-Diensten erweitert, sodass Nutzer inzwischen auch Sprachnachrichten aufnehmen und versenden können. Die Funktion zum Versenden und Empfangen von Dateien, besonders Bildern und Videos, stellt im Vergleich zum vormaligen Versenden solcher Inhalte per MMS[5] eine kostengünstige bzw. kostenfreie Alternative digital Inhalte auszutauschen. Manche IM-Dienste bieten ihren Nutzern auch die Möglichkeit, andere Inhalte als Bilder und Videos miteinander zu teilen. Das Versenden und Empfangen von Nachrichten beschränkt sich ebenfalls nicht mehr auf Konversationen zwischen zwei Nutzern, sondern kann anhand von sogenannten Gruppenchats mit mehreren Nutzern gleichzeitig durchgeführt werden. Innerhalb von Konversationen können teilweise auch Nachrichten und Inhalte versendet werden, die sich nach Öffnen oder nach gewisser Zeit selbstständig löschen.[6] Einige IM-Dienste, wie z.B. WhatsApp[7] stellen inzwischen die Option bereit, über die Anwendung Sprach- und Videotelefonate zu führen.[23]

2.3.1 Webclient

Im Allgemeinen wird als Webclient die Anwenderseite des Webs bezeichnet[8]. Bei dem Webclient handelt es sich um Webbrowser bzw. Internetbrowser. Dieser kommuniziert mit dem Webserver, indem HTTP(S)[9]-Anfragen versendet und entsprechende Antworten empfangen werden. Heutzutage werden sogenannte grafische Browser verwendet, die den Nutzern eine anwenderfreundliche und intuitive Bedienung und Nutzung der WWW-Dienste[10] ermöglichen.[24]

Mittels der Webclients können Nutzer unterschiedliche Dienste im Internet aufrufen und verwenden. Den Nutzern steht hier u. a. die Möglichkeit zur Verfügung IM-Dienste aufzurufen und mittels deren Webclients Konversationen zu führen und weitere vom IM gestellte Funktionen zu beanspruchen.

[4] Piktogramm, Logogramm oder Smiley
[5] Multimedia-Kurznachrichten
[6] Bsp. durch die Anwendung Snapchat
[7] Weltweit Nutzerzahlen von über 850 Millionen [22]
[8] Die Anbieterseite ist der Webserver
[9] Hypertext Transfer Protocol (Secure)
[10] WWW - World Wide Web

2.3.2 Ende-zu-Ende-Verschlüsselung

Die Ende-zu-Ende-Verschlüsselung oder auch E2EE wird heutzutage von vielen Kommunikations-Anwendungen genutzt, um die zu übertragenden Daten so zu versenden, dass nur Sender und Empfänger die Nachrichten lesen können.[25]

Im Folgenden wird mithilfe der Abbildung 2.1 das Prinzip von E2EE kurz erläutert.[26] Damit die vom Sender an den Empfänger versendeten Daten nur von den gewünschten Parteien gelesen, aber über einen Anbieter, wie z. B. einen IM-Dienst, übertragen werden können, verschlüsselt der Sender die zu versendenden Daten mit dem öffentlichen Schlüssel (engl. public key) des Empfängers. Die verschlüsselten Daten werden über den Anbieter an den Empfänger versendet, welcher mithilfe seines privaten Schlüssels (engl. private key) die verschlüsselten Daten des Senders entschlüsseln kann.

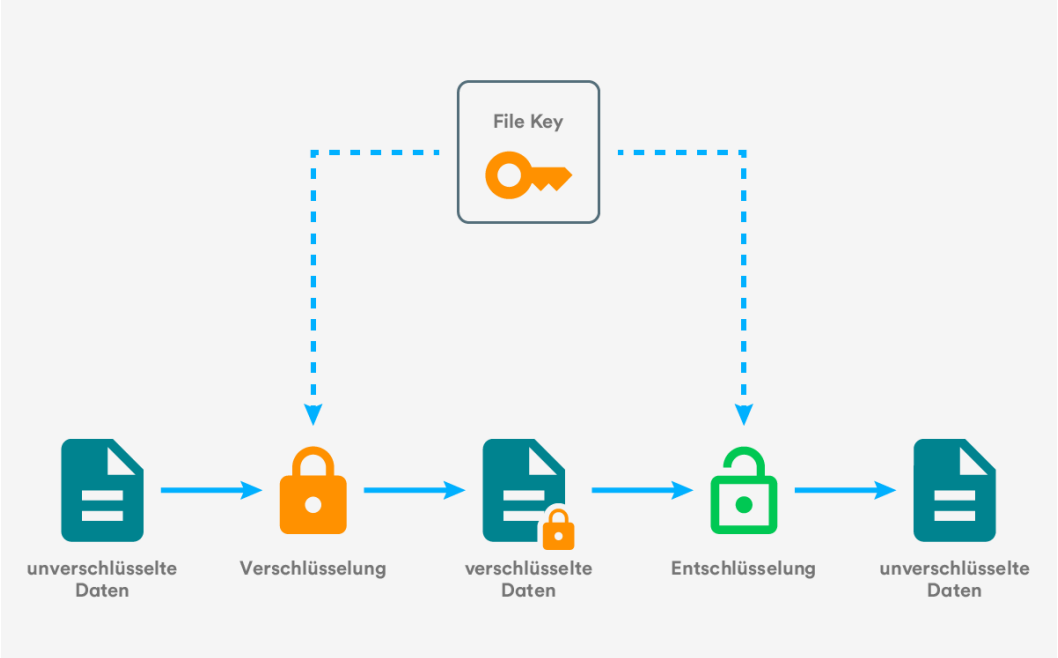

Abbildung 2.1: E2EE-Prinzip

Das Wählen von Schlüsseln und Verschlüsseln/Entschlüsseln versendeter und empfangener Nachrichten wird im Falle von IM-Diensten durch die zur Konversation gewählte Anwendung durchgeführt.

Um diese Art der Inhaltsübertragung zu ermöglichen, werden zur Verschlüsselung kryptografische Verfahren der symmetrischen[11] und asymmetrischen[12] Verschlüsselung genutzt.[27] Der für den Austausch von Nachrichten verwendete IM-Dienst erhält die verschlüsselten Inhalte inklusive der notwendigen Informationen, die benötigt werden, um die Nachricht an den Empfänger zu versenden. Anzumerken ist, dass häufig nur der Inhalt der Nachricht selbst, aber nicht die dazugehörigen Metadaten wie z. B. Zeitstempel und beteiligte Kommunikationspartner, verschlüsselt wird.

[11] Sender und Empfänger nutzen denselben Schlüssel.
[12] Sender und Empfänger nutzen zur Ver- und Entschlüsselung verschiedene Schlüssel.

2.3.3 Threema

Threema ist ein E2EE-verschlüsselter IM-Dienst, welcher von Nutzern auf Mobiltelefonen, Tablets und Computern verwendet werden kann. Der Dienst kann sowohl von Nutzern des mobilen Betriebssystems Android[13], als auch von iOS-Nutzern[14] verwendet werden. Die Anwendung kostet für Android 4,99 € und für Apple iOS 5,99 €. [28][29] Nach Kauf der Anwendung und Einrichten eines Nutzerkontos kann der Nutzer Kommunikationskanäle mit weiteren Threema-Nutzern aufbauen. Threema wirbt damit, dass Nutzer anonym und verschlüsselt mit anderen Nutzern kommunizieren können. Die Chatanwendung Threema wurde im Jahr 2012 in Zürich durch drei Schweizer entwickelt und wurde „*«End-to-End Encrypted Messaging Application» getauft, kurz «EEEMA». Wenig später werden die drei «E»s durch «three» (Englisch für «drei») ersetzt, so entsteht der Name «Threema»*“.[30] Die Anzahl der Nutzer liegt seit 2022 bei knapp 11 Millionen. [4]
Im Folgenden werden die Funktionen des IM-Dienstes Threema aufgelistet und erläutert.[31]

Einzel- und Gruppenkonversationen

Nutzer der Anwendung können mit einzelnen oder auch mehreren Personen gleichzeitig Konversationen führen. Hierzu hat der Nutzer innerhalb der Anwendung unterschiedliche Anzeigen. Für die Konversationen mit jeweils einem Nutzer wird der jeweilige Nutzername des Konversationspartners angezeigt. Bei Konversationen mit mehreren Nutzern gleichzeitig wird dem lokalen Nutzer die Bezeichnung des sogenannten Gruppenchats angezeigt. Nur Mitglieder einer Gruppe können sehen, wer sich ebenfalls darin befindet. Nutzer können private oder öffentliche Gruppen erstellen, bzw. diesen beitreten, wobei private Gruppen nur auf Einladung betreten werden können.

Verteilerlisten

Möchte der lokale Nutzer eine Nachricht an mehrere Personen schicken, aber keine Gruppe hierfür verwenden, kann er die Funktion der Verteilerliste verwenden. Hier kann der Nutzer entscheiden, an welche Personen die zu versendende Nachricht übermittelt werden soll.

Text- und Sprachnachrichten

Innerhalb von Konversationen können sich Nutzer durch die Verwendung von Textnachrichten miteinander austauschen. Auch steht den Nutzern die Möglichkeit zum direkten Aufnehmen von Ton und dem Übersenden der aufgenommenen Inhalte als sogenannte Sprachnachricht zur Verfügung. Textnachrichten bestehen heutzutage nicht mehr nur aus Buchstaben, Satzzeichen, Zahlen und anderen Sonderzeichen. Innerhalb der Nachrichten können auch Emojis versendet werden. Bereits gesendete Nachrichten können von den Sendern nachträglich gelöscht werden, wodurch die betreffenden Inhalte sowohl beim Sender, als auch beim Empfänger entfernt werden.

Übertragung von Medien

Nutzer können innerhalb von Konversationen Medien, wie z. B. Bilder, Videos, Audiodateien, animierte GIFs oder auch Dokumente austauschen. In welcher Qualität die Inhalte übertragen werden, kann durch jeden Nutzer individuell eingestellt werden. Inhalte mit einer Größe von über 5,00 MB werden nur auf Wunsch des Empfängers heruntergeladen. Auch können Nutzer Kontakte miteinander teilen.

[13] Betriebssystem für mobile Geräte, gegründet von Google. Android ist eine freie Software.
[14] iOS ist ein mobiles Betriebssystem, welches durch Apple für die eigenen mobilen Geräte entwickelt wurde.

Sprach- und Videotelefonie

Auch die über Threema geführten Telefonate sind durch E2EE verschlüsselt. Innerhalb von Telefonaten können die Nutzer sowohl eine Sprachübertragung, als auch eine Videoübertragung wählen. Die Übertragung von Videoinhalten wird nicht benötigt ,um ein Sprachtelefonat zu ermöglichen. Die Telefonate können zwischen einzelnen oder mehreren Nutzern gleichzeitig geführt werden. Gruppenteilnehmer können aktiven Anrufen innerhalb der Gruppe jederzeit beitreten oder diese verlassen.

Teilen von Standorten

Es besteht die Möglichkeit, Standorte mit den Chatpartnern zu teilen. Bei diesen Standorten muss es sich nicht um den aktuellen Standort des Senders handeln.

Umfragefunktionen

Innerhalb von Konversationen können Nutzer Umfragen starten, um z. B. Abstimmungen für einen Termin oder die Wahl eines Restaurants durchzuführen.

Private Chats

Sollte ein Nutzer eine Konversation in der Übersicht seiner geführten Konversationen ausblenden oder per Schutzmechanismen, wie PIN oder Biometrie, absichern wollen, so kann er sich die Funktion der privaten Chats zunutze machen. Konversationen können schon zu Beginn, aber auch nachträglich, als privat gekennzeichnet und nach den Wünschen des Nutzers abgesichert werden.

Threema am Computer

Threema bietet seinen Nutzern die Möglichkeit, ihre Chats auch über den Computer per Installation einer Desktop-Anwendung oder durch Nutzung des Webclients von Threema über unterschiedliche Browser zu führen. Um diese Funktion nutzen zu können, muss mit dem Mobilgerät, auf welchem das Threema-Nutzerkonto eingerichtet wurde, ein QR-Code vom Bildschirm gescannt werden. Das Scannen muss erneut durchgeführt werden, wenn der Nutzer kein sogenanntes Sitzungskennwort festlegt. Einen Unterschied im Funktionsumfang zwischen dem Webclient und der Desktop-App von Threema gibt es nicht.

Threema-ID

Für die Verwendung von Threema benötigen die Nutzer keine SIM-Karte. Die Identifikation der einzelnen Nutzer wird anhand der sogenannten eindeutigen Threema-ID durchgeführt. Diese ID ist achtstellig und besteht aus einer zufälligen Aneinanderreihung von Buchstaben und Zahlen. Zusätzlich zur Threema-ID wird ein Schlüsselpaar[15] bei der Installation der Anwendung eingerichtet und an die ID des Nutzers gekoppelt.[32] Threema-Nutzer können ihren Accounts auch ihre Rufnummer hinzufügen und bei Bedarf das lokale Telefonbuch ihres Mobiltelefons mit Threema synchronisieren, um mögliche bereits bekannte Chatpartner festzustellen.

[15] bestehend aus einem öffentlichen und einem privaten Schlüssel

Vertrauensstufen

Threema bietet seinen Nutzern die Funktion der Vertrauensstufe an. Hierbei handelt es sich um eine Anzeige von gefärbten Punkten neben der einzelnen Kontakte. Diese Vertrauensstufe gibt an, ob der gespeicherte öffentliche Schlüssel tatsächlich zu dem angezeigtem Kontakt gehört. [33]

- **Stufe 1**
  Ein roter Punkt. Sowohl die ID, als auch der öffentliche Schlüssel wurden über den Server bezogen. Der Kontakt befindet sich nicht im Telefonbuch des lokalen Mobiltelefons. Eine tatsächliche Identifikation der Person wurde nicht durchgeführt.
- **Stufe 2**
  Zwei orange Punkte. Zu dem Kontakt wurde im Telefonbuch des Mobiltelefons ein Eintrag festgestellt.
- **Stufe 3**
  Drei grüne Punkte. Der öffentliche Schlüssel des Kontakts wurde in Person durch Scannen des QR-Codes übertragen und bestätigt.

Für Stufe 2 und 3 gibt es jeweils auch die Variation in Blau, jedoch ist diese Funktion nur für die Anwendungsversion Threema Work vorhanden. Der Vertrauensstufe verändert jedoch nichts an der Art und Weise, wie die ausgetauschten Inhalte der Nutzer verschlüsselt sind.[33]

2.3.4 Instagram

Bei Instagram handelt es sich um ein soziales Netzwerk, welches seinen Nutzern ermöglicht, Bilder und Videos mit anderen Nutzern des Netzwerks zu teilen.[16] Instagram wurde 2010 gegründet und zwei Jahre später durch Facebook aufgekauft. Die Nutzung von Instagram ist kostenlos. Dafür werden den Nutzern regelmäßig Werbeinhalte angezeigt. Die Verwendung von Instagram kann sowohl über eine Web-Anwendung, als auch über eine auf einem Mobilgerät installierte Anwendung durchgeführt werden, wobei der installierten Variante mehr Funktionen zur Verfügung stehen. Um sich bei Instagram zu registrieren, benötigt der Nutzer eine Handynummer oder E-Mail-Adresse. Eine Identifizierung innerhalb des sozialen Netzwerks erfolgt anhand des gewählten Benutzernamens, der nicht dem sogenannten Anzeigenamen entsprechen muss. Instagram bietet seinen Nutzern nicht nur die Möglichkeit, Medien mit anderen Nutzern zu teilen, sondern stellt auch die Funktionen eines typischen IM-Dienstes zur Verfügung:
Die Nutzer können miteinander per Text- und Sprachnachrichten, aber auch per Sprach- und Videotelefonie kommunizieren. Auch Instagram verwendet die E2EE-Verschlüsselung, um die von Nutzern geführten Kommunikationen vor dem Zugriff Unbefugter zu schützen.
Im Folgenden werden die Chatfunktionen des sozialen Netzwerks Instagram aufgelistet und erläutert. Auf die weiteren Funktionen des sozialen Netzwerks soll hier nicht näher eingegangen werden.[34]

Instagram Web

Die Nutzung von Instagram ist mit eingeschränktem Funktionsumfang auch über einen Webclient möglich. Der Zugang dazu kann über die Webseite von Instagram geöffnet werden. Hier können sich Nutzer durch Eingabe ihres Nutzernamens und Kennworts anmelden. Die Chatfunktionen sind im Webclient von Instagram nutzbar.

[16] Wer die geteilten Inhalte sieht, hängt von den Privatsphäreeinstellungen des jeweiligen Nutzers ab.

Einzel- und Gruppenkonversationen

Instagram-Nutzer können in Einzel- oder Gruppenkonversationen mit einem weiteren oder mehreren Nutzern gleichzeitig kommunizieren. Die versendeten Nachrichten werden in Gruppenchats automatisch an alle Mitglieder der jeweiligen Gruppe versendet.

Text- und Sprachnachrichten

Innerhalb von Konversationen können sich Nutzer durch die Verwendung von Textnachrichten miteinander austauschen. Auch steht den Nutzern die Möglichkeit zum direkten Aufnehmen von Ton und dem Übersenden der aufgenommenen Inhalte als sogenannte Sprachnachricht zur Verfügung. Textnachrichten bestehen heutzutage nicht mehr nur aus Buchstaben, Satzzeichen, Zahlen und anderen Sonderzeichen. Innerhalb der Nachrichten können auch Emojis versendet werden. Die gesendeten Nachrichten können von den Sendern nachträglich gelöscht werden, wodurch die gelöschten Inhalte sowohl beim Sender, als auch beim Empfänger entfernt werden.

Übertragung von Medien

Neben dem Versenden und Empfangen von Text- und Sprachnachrichten können Nutzer über Instagram Inhalte wie Bilder, Videos und Sticker mit anderen Nutzern austauschen. Auch können sich Nutzer Beiträge dritter Nutzer zusenden.

Sprach- und Videotelefonie

Zusätzlich zur oben genannten Kommunikation können Chatpartner über Instagram auch Sprach- und/oder Videotelefonate miteinander führen. Hier ist die Anzahl der Teilnehmer ebenfalls an einem Telefonat nicht auf zwei begrenzt.

Selbstlöschende Nachrichten

Nutzer können innerhalb von Konversationen Nachrichten und Inhalte versenden, die sich nach einmaligem oder mehrfachem Öffnen oder nach einer gewählten Zeit, selbstständig löschen. Diese werden anschließend, wenn überhaupt, innerhalb der Konversation als gelöschte Nachricht gekennzeichnet und können nicht mehr aufgerufen werden.

2.4 Prinzip der Kommunikation

Als Kommunikation wird der Austausch von Informationen, durch Nutzung von Sprache oder Zeichen, zwischen einem Sender und mindestens einem Empfänger bezeichnet.[35]

Dieses sogenannte Sender-Empfänger-Modell wird kurz mithilfe der Abbildung 2.2 erläutert.[36]

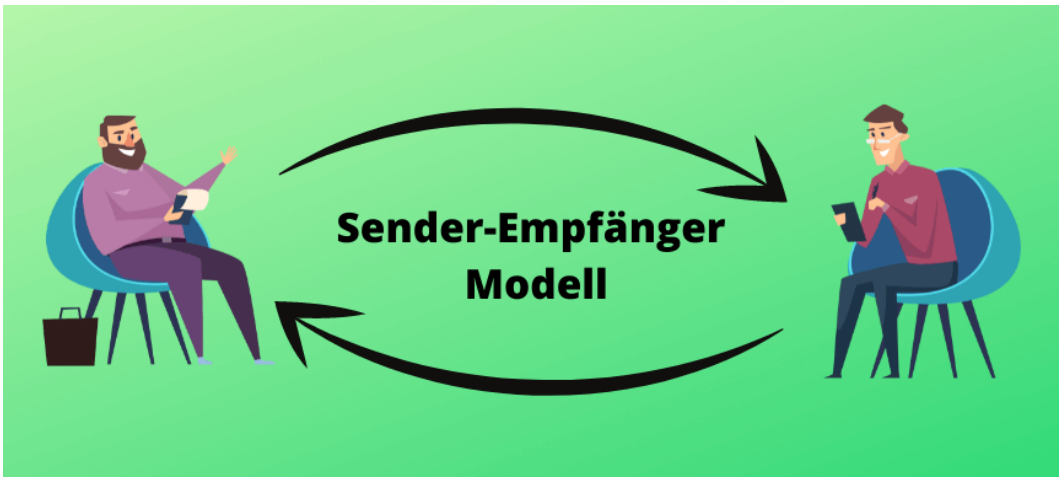

Abbildung 2.2: Sender-Empfänger-Modell

Der Sender möchte Informationen an den Empfänger vermitteln. Hierfür wählt der Sender z. B. das Mittel der Sprache. Die Informationen, die der Sender dem Empfänger mitteilen möchte, werden nun durch den Sender mittels Sprache mitgeteilt.[17] Der Empfänger nimmt das Gehörte auf und versucht die verstandenen Informationen zu verarbeiten. Nun kann auch der Empfänger zum Sender werden, indem er z. B. dem (ersten) Sender seinerseits Informationen mitteilt oder lediglich kenntlich macht, dass er die vermittelten Informationen erhalten hat.

Mittels IM-Diensten kann eine Kommunikation zwischen zwei oder mehreren Personen sowohl via Sprache als auch via Textinhalt geführt werden. Die Nutzung von IM-Diensten ermöglicht es Menschen, sich standortunabhängig und nahezu in Echtzeit miteinander auszutauschen. Im Gegensatz zum persönlichen Austausch wird bei der Kommunikation über das Internet die versendete Nachricht über Server an den Empfänger geschickt. Seit der Aufdeckung des Überwachungsprogramms Prism durch Edward Snowden im Jahr 2013 wurde die Öffentlichkeit bezüglich der Risiken der Kommunikation über das Internet sensibilisiert.[37] Um sicherzugehen, dass die über IM-Dienste geführte Kommunikation nur von denjenigen Personen erhalten und verstanden wird, für welche die Informationen gedacht ist, wurde die Methode der Verschlüsselung gewählt.[18]

2.4.1 Threema

Threema bietet seinen Nutzern die Möglichkeit, anonym und verschlüsselt mit anderen Nutzern zu kommunizieren. Zur Nutzung des Dienstes werden weder eine E-Mail-Adresse noch eine Telefonnummer benötigt. Nutzer können sich mittels der auf ihrem Mobiltelefon installierbaren Anwendung

[17] In der zwischenmenschlichen Kommunikation spielen hier auch Faktoren wie Gestik und Mimik eine Rolle, welche für die Definition vorerst vernachlässigt werden.
[18] Heutzutage handelt es sich hierbei häufig um die E2EE-Verschlüsselung.

registrieren und erhalten eine eindeutige ID. Um den Webclient von Threema nutzen zu können, muss der Nutzer die Webseite `web.threema.ch` aufrufen und kann seinen auf dem Mobiltelefon eingerichteten Nutzeraccount mit dem Webclient verbinden. Die Verbindung des Nutzeraccounts wird, wie in Abbildung 2.3 gezeigt, mittels Scan eines QR-Codes durchgeführt.

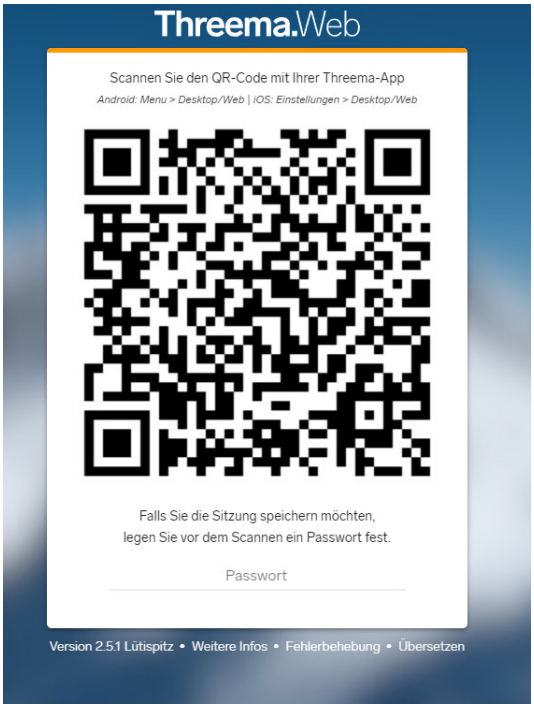

Abbildung 2.3: Threema-Web Login

Infolge der Auswahl eines Kennwortes muss bei erneutem Aufrufen der Webseite die Verbindung des Nutzerkontos nicht erneut durchgeführt werden.
Anschließend wird dem Nutzer am Mobiltelefon angezeigt, wie in Abbildung 2.4 dargestellt, wann eine Desktop- oder Websitzung erstellt wurde und ob diese aktiv ist.

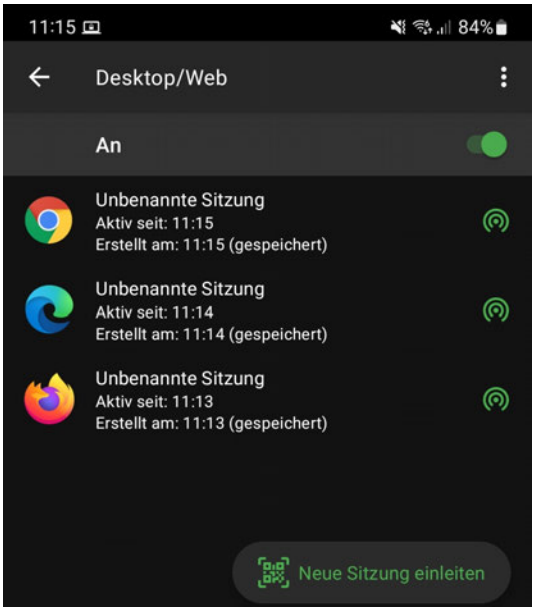

Abbildung 2.4: Threema-Login-Verwaltung

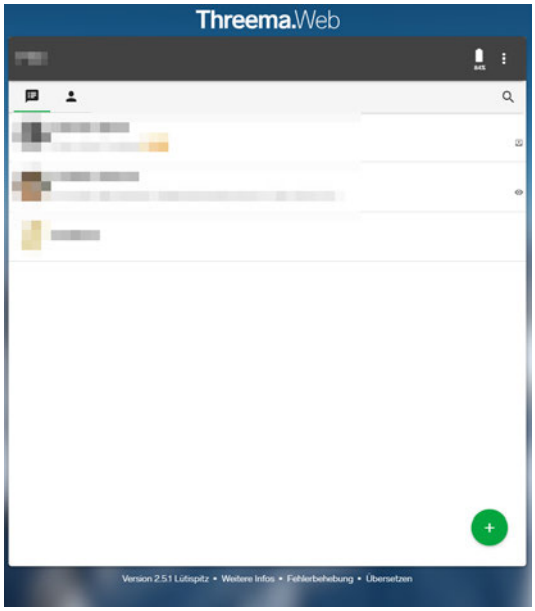

Abbildung 2.5: Threema-Web-Oberfläche

Abbildung 2.5 zeigt die Ansicht, die der Nutzer erhält, nachdem er seinen Nutzeraccount in Threema-Web aufgerufen hat.
Mittels dieser erhält der Nutzer eine Übersicht über seine geführten Konversationen, kann neue Konversationen starten oder bereits existierende Konversationen weiterführen.

2.4.2 Instagram

Um Instagram verwenden zu können, muss ein Nutzer sich mittels einer Rufnummer oder E-Mail-Adresse, Angaben zum vollständigen Namen, einem Benutzernamen und einem Kennwort, registrieren. Dieser Prozess kann sowohl per Anwendung auf einem Mobilgerät, als auch per Webbrowser, z. B. am Computer, stattfinden. Nach abgeschlossener Registrierung haben Nutzer Zugriff auf das soziale Netzwerk von Instagram und können Inhalte mit anderen teilen oder mittels Chatfunktionen kommunizieren. Um die Webfunktionen von Instagram nutzen zu können, muss die Webseite `www.instagram.com` mittels Internetbrowser aufgerufen werden. Hier kann der Nutzer sich in ein bestehendes Profil einloggen oder ein Konto erstellen, siehe Abbildung 2.6.

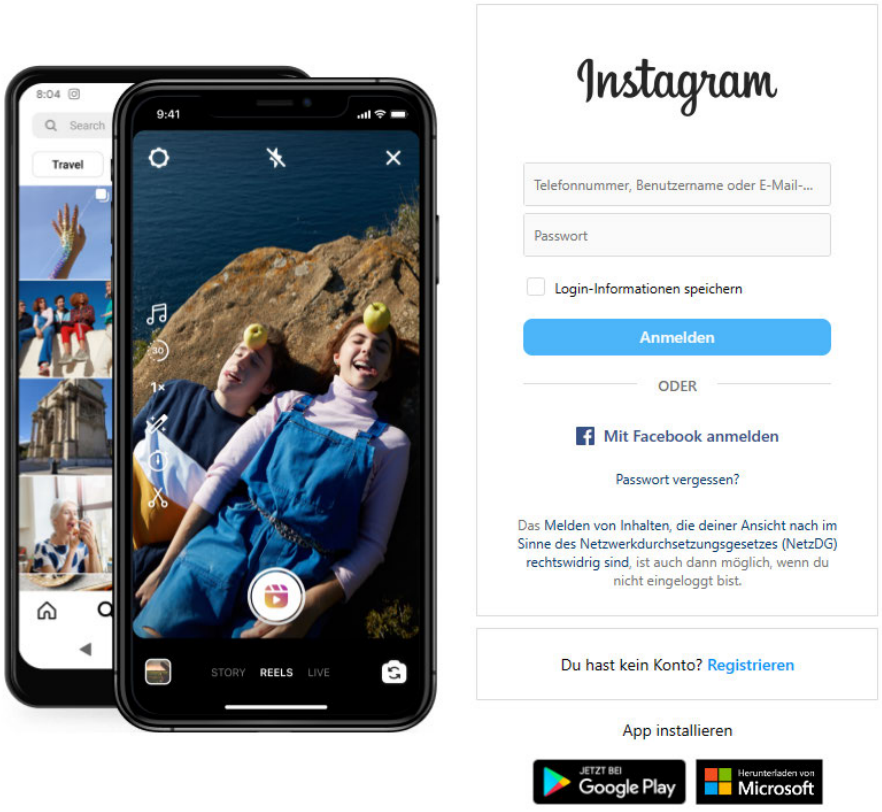

Abbildung 2.6: Instagram-Web-Login

In der in Abbildung 2.7 dargestellten Chatansicht erhält der Nutzer einen Überblick über geführte Kommunikationen mit einzelnen Nutzern oder auch Gruppen. Hier kann der Nutzer Nachrichten lesen, versenden und empfangen.

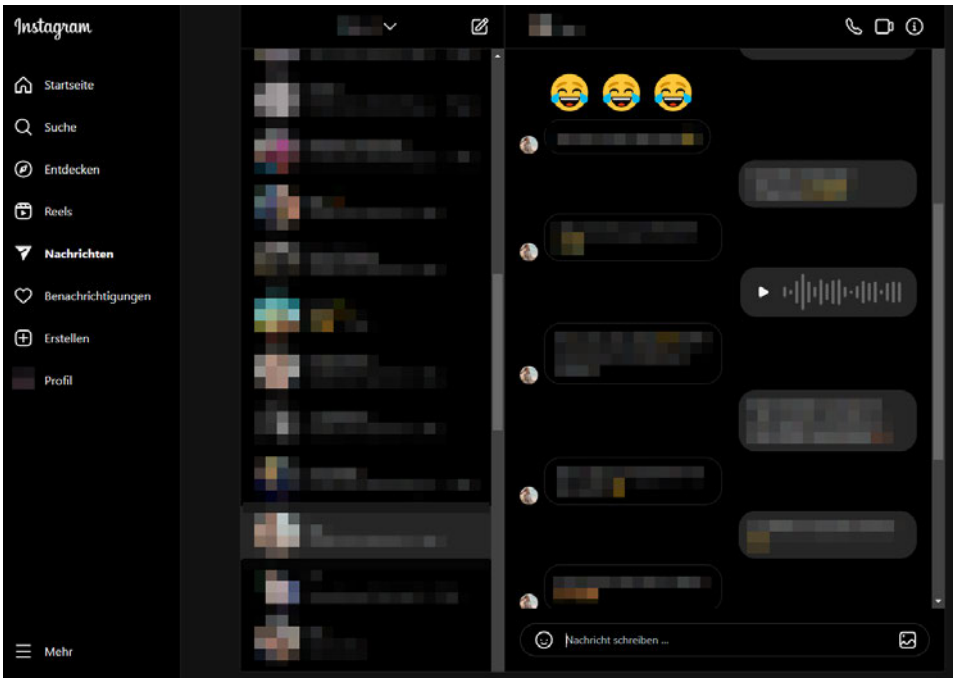

Abbildung 2.7: Instagram-Chatansicht

2.5 RAM

Im Folgenden wird kurz der Unterschied zwischen dem sogenannten flüchtigen Speicher (engl. volatile memory) und dem festen Speicher erläutert, um danach auf grundsätzliche Informationen zur Rechner-Archtitektur und den Zugriff auf den flüchtigen Speicher einzugehen. Abschließend werden die Prinzipien und die Durchführung der Sicherung von Daten im bzw. aus dem RAM dargelegt.

Die Abkürzung RAM steht für Random-Access-Memory (deutsch: Speicher mit wahlfreiem Zugriff), wobei die Bezeichnung Random-Access genauer betrachtet werden sollte.

- Im Gegensatz zu dem Read-Only-Memory (ROM), welcher nach einmaligem Beschreiben nur noch gelesen werden kann, können die Daten vom RAM jederzeit gelesen und verändert bzw. überschrieben werden.
- Der Begriff Random (deutsch. Zufall bzw. zufällig) bezieht sich darauf, dass auf jedes einzelne Byte in beliebiger Reihenfolge zugegriffen werden kann.[38]

2.5.1 Flüchtiger Speicher

Flüchtige Speichermedien (z. B. RAM, Register[19], Cache-Speicher[20]) speichern im Gegensatz zu festen Speichermedien (z. B. CDs/DVDs, Speicherkarten, Festplatten, USB-Sticks) Daten nur temporär, um eine Aufgabe oder einen Prozess durchzuführen. Alle gespeicherten Daten werden nach Trennen von der Stromzufuhr gelöscht.[39] Bei festen Speichermedien bleiben die Informationen auch nach Trennung von der Stromzufuhr erhalten.

[19] Befinden sich direkt neben der CPU und dienen der Zwischenspeicherung von Daten und Befehlen. Bieten eine geringe Zugriffszeit.

[20] Zwischenspeicher zwischen Prozessor und Hauptspeicher (RAM). Soll häufig genutzte Daten und Instruktionen in der Nähe des Prozessors halten, um Zugriffszeiten zu minimieren.

Bei den Bausteinen des RAM handelt es sich um flüchtigen Speicher. Damit es während des Betriebs nicht zu Datenverlusten kommt, muss der Arbeitsspeicher (bzw. RAM) dauerhaft mit Strom versorgt werden bis der Computer heruntergefahren wird. Im Folgenden werden die Eigenschaften der zwei RAM-Bauformen, Dynamic Random-Access-Memory (DRAM) und Static Random-Access-Memory (SRAM) in der Tabelle 2.2 aufgelistet.[40]

Eigenschaften	DRAM	SRAM
Stromzufuhr	bestehende Stromzufuhr Inhalt jeder Zelle muss mit jedem Taktzyklus aufgefrischt werden	bestehende Stromzufuhr
Herstellung	günstige Herstellung	teure Herstellung
Stromverbrauch	gering	hoch
Verwendungsort	Hauptspeicher	Cache-Speicher

Tabelle 2.2: Eigenschaften von DRAM und SRAM

Im Bereich der IT-Forensik ist jedoch auch die Analyse der im flüchtigen Speicher, dementsprechend auch im RAM, enthaltenen Daten relevant, da innerhalb dessen Informationen zu geführter Kommunikation, Kennwörtern, aufgerufenen Dokumenten oder auch Hinweise auf Schadsoftware festgestellt werden können. [39] Die Besonderheit der Daten, die im RAM auffindbar sein können, besteht darin, dass es sich hier teilweise auch um Daten handelt, bei denen der Nutzer keinerlei Intention hatte, sie zu speichern. So können z. B. Fragmente oder ganze Inhalte von versendeten, entworfenen und/oder empfangenen Nachrichten im RAM enthalten sein, obwohl diese nicht lokal abgespeichert wurden.[41]

2.5.2 Aufbau RAM

RAM, oder auch Arbeitsspeicher genannt, enthält die aktuell ausgeführten Programme, und die Daten, die von ihnen verarbeitet werden. In modernen Computersystemen wird der Arbeitsspeicher in die dafür bestimmten Slots auf dem Mainboard gesteckt. Wie in Abbildung 2.8 dargestellt, besteht der Arbeitsspeicher aus unterschiedlichen Bausteinen.

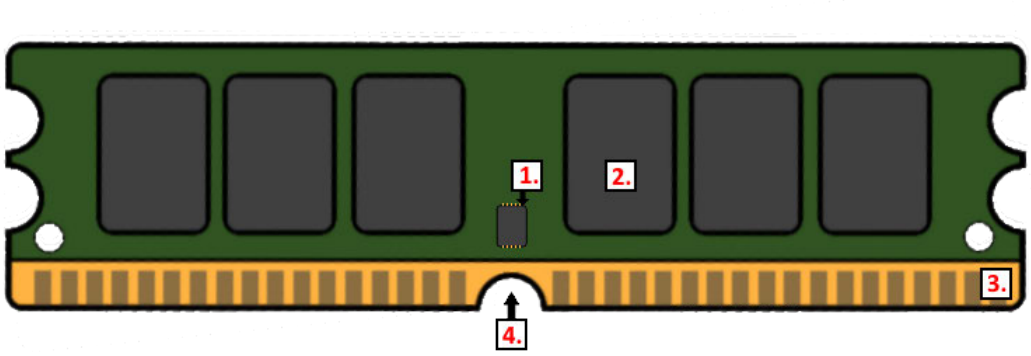

Abbildung 2.8: Aufbau RAM

Folgende Bausteine werden heutzutage verwendet, um Arbeitsspeicher-Riegel zu bauen:

1. EEPROM[21]
   EEPROM lässt Daten mit elektrischen Impulsen löschen [40]
2. Speicherzelle(n)
   eigentlicher Arbeitsspeicher
3. Kontaktleiste
   Die Anzahl der Pins ist abhängig von der DDR-Art[22] des RAM
4. Kerbe
   die Kerbe verhindert, dass zum System inkompatible RAM-Module verwendet oder kompatible Module falsch herum eingesetzt werden.

[21] Electrical Erasable Programable ROM
[22] Double Data Rate (DDR) (deutsch doppelte Datenrate)

2.5.3 Rechner-Architektur

In der heutigen Zeit sind Computer in der Lage, weit mehr zu leisten als ursprünglich vorgesehen war. Neben ihrem anfänglichen Zweck, wie beispielsweise einfache Rechenaufgaben und grundlegenden Verwaltungstätigkeiten durchzuführen, haben sie im Laufe der Jahre eine Vielzahl zusätzlicher Funktionen hinzugewonnen. John von Neumann, Mitglied des ENIAC-Projekts[23] entwickelte seine eigene Variante der EDVAC-Maschine[24], die IAS-Maschine. Der Entwurf ist als die Von-Neumann-Maschine (VNM) bekannt und ist heutzutage die Grundlage fast aller Computer.[40]
Die VNM besteht aus folgenden Teilen:

- Speicherwerk
- Central Processing Unit (CPU)
  - Steuerwerk (Control Unit (CU))
  - Rechenwerk (Arithmetic Logic Unit (ALU))
- Ein- und Ausgabewerk (I/O - Input/Output Unit)
- Systembus
  - Adressbus
  - Datenbus
  - Steuerbus

Verknüpft werden die Bestandteile, wie in Abbildung 2.9 dargestellt. Anzumerken ist, dass im ursprünglichen Entwurf die ALU und die CU nicht zu einer CPU zusammengefasst wurden.[42]

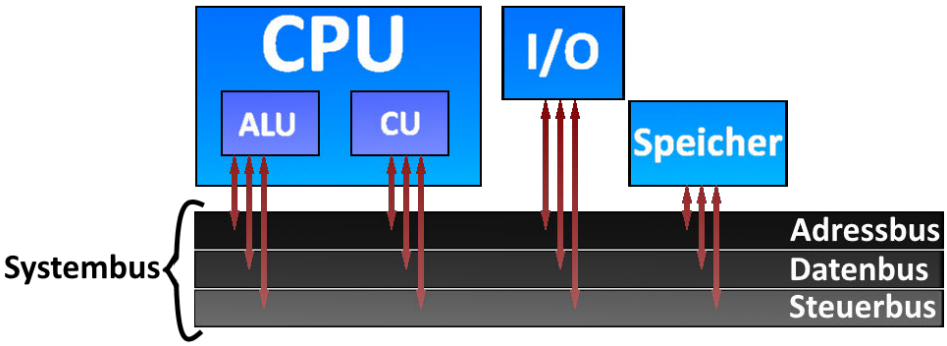

Abbildung 2.9: Von-Neumann-Arichtektur

Durch die Input-Unit werden Daten eingegeben. Anschließend werden diese durch die CU in das Speicherwerk gesendet. Die benötigten Daten werden mittels CU aus dem Speicherwerk entnommen und an die ALU vermittelt, um dort verarbeitet zu werden. Danach werden die Daten wiederum mittels CU in das Speicherwerk gesendet oder durch die Output-Unit ausgegeben. Die Kommunikation bzw. Datenübertragung zwischen den einzelnen Bausteinen geschieht über den Systembus, welcher aus dem Adressbus, Datenbus und Steuerbus besteht.[43] Als Speicherwerk wird der RAM verwendet. Die Input- und Output-Unit beinhalten sowohl Festplatten, als auch die Verbindung mit externen Geräten wie Maus und Tastatur. Mit diesem Bestandteil der VNM wird eine Schnittstelle zum System erstellt.[43]

[23] Electronic Numerical Interator And Computer
[24] Electronic Discrete Variable Automatic Computer

2.5.4 Speicherzugriff

Der RAM wird aus modular aneinander angeordneten Speicherzellen in Form einer Matrix zusammengesetzt. Aufgrund dieser Anordnung sind die Speicherzellen einzeln über Zeilen (row access strobe (RAS)) und Spalten (column access strobe (CAS)) adressierbar. [44] Die Adressierung des Speichers wird taktweise zwischen der Angabe von RAS und CAS gewechselt. Dieses Zugriffsverfahren wird im sogenannten Fast-Page-Mode optimiert. Hier wird auf das erneute Anlegen der gleichen RAS verzichtet und lediglich die jeweilige neue CAS angelegt. Entsprechend besteht der Speicher aus einzelnen Speicherzellen, die mittels Adressen[25] identifizierbar und wahlfrei ansprechbar sind. Jede Zelle besteht aus einer Adresse und einem Wert-Feld, welche hexadezimal codiert sind.[20][45]
Im Verlauf eines Speicherzugriffs ist zwischen zwei Adresstypen zu unterscheiden:
Der physischen Adresse der jeweiligen Speicherzelle und der virtuellen Adresse im Prozess/ Programm. Mittels dieser wird ein Mehrprogrammbetrieb ermöglicht. Auch kann der virtuelle Adressraum bzw. virtueller Speicher (VS) eine beliebige Größe annehmen und unabhängig vom physischen Adressraum fungieren.

Virtueller Speicher

Der VS simuliert Speicheradressen, die Prozesse und Systemnutzer wie physische Speicheradressen behandeln können. Die Grundidee des VS ist es, den RAM zu entlasten, indem aktuell nicht benötigte Daten temporär auf der Festplatte[26] des Systems gespeichert werden. Der VS lagert Inhalte aus dem RAM aus, um die Ausführbarkeit von mehreren Programmen unabhängig von der Größe des Hauptspeicher (HS) zu ermöglichen.

Die Nutzung des VS ist an einem vereinfachten Beispiel in Abbildung 2.10 dargestellt.[46]

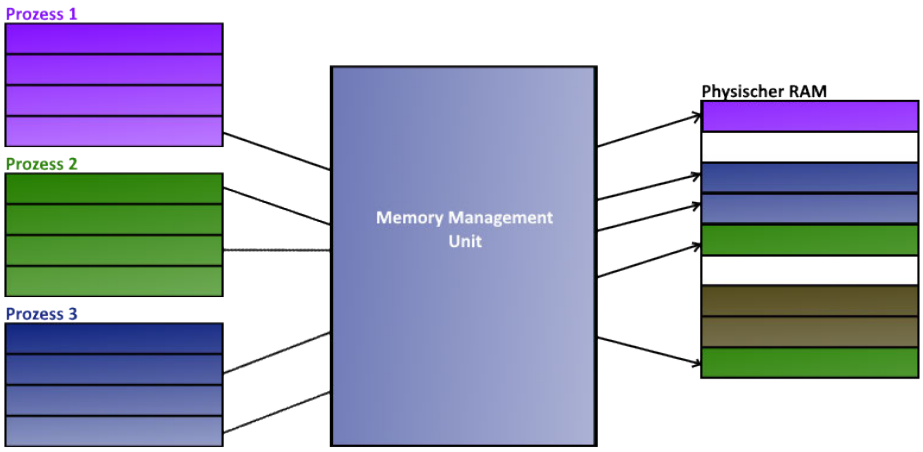

Abbildung 2.10: Nutzung virtueller und physischer Speicher

Aufgrund dieses Vorgehens, müssen die von Prozessen verwendeten virtuellen Adressen in physische übersetzt werden. Hierbei handelt es sich um die sogenannte Adressauflösung. Diese wird durch die Memory Management Unit (MMU)[27] übernommen und ist notwendig, da die CPU nur mit physischen Adressen arbeitet. Neben dem Vorteil, dass Programme nicht zwingend an die reale

[25] bestehend aus RAS und CAS
[26] Der VS funktioniert in der Regel nicht ohne Festplatte oder andere sekundäre Speichergeräte.
[27] Die MMU verwaltet u. a. auch Zugriffsberechtigungen im RAM.

Größe des RAM gebunden sind, bietet die Nutzung virtueller Adressen auch einen Schutzmechanismus. Jedes Programm erhält einen exklusiven, initial unfragmentierten, virtuellen Speicherbereich (VS).[20][46]

Ansprechen und Auslesen

Für den Betrieb des RAM wird eine durchgehende Stromzufuhr benötigt, da Spannungsimpulse verwendet werden, um den Speicher anzusprechen oder auszulesen. RAM und CPU sind über Bus-Systeme[28] verbunden.[43][44]

Der RAM nutzt die zwei Register Memory Address Register (MAR) und Memory Data Register (MDR) als Interface. Das MAR ist das Adressregister und das MDR das Datenregister.

- **MAR/Adressregister**: enthält Speicheradresse.
- **MDR/Datenregister**: enthält Wert, der in der angegebenen Adresse geschrieben oder von dieser gelesen werden soll.

Um eine RAM-Speicherzelle zu beschreiben oder zu lesen, wird als erstes ihre Adresse in das MAR abgelegt. Soll eine Speicherzelle nicht beschrieben, sondern überschrieben werden, wird der neue Inhalt im MDR gespeichert. Durch die entsprechenden Bussysteme wird die Übertragung von Daten und Adressen durchgeführt. So erhält der RAM mittels Steuerbus die Information, ob eine Speicherzelle gelesen oder beschrieben werden soll. Beim Lesevorgang werden die enthaltenen Daten mittels Datenbus an die CPU geleitet. Soll die Speicherzelle beschrieben werden, werden die betreffenden Daten aus der MDR entnommen und in die entsprechende Speicherzelle geschrieben.[44]

Speicherverwaltung

Wie genau die Speicherverwaltung funktioniert, ist betriebssystemabhängig. Mittels der Speicherverwaltungseinheit, genannt MMU, werden alle Operationen, die den RAM und/oder Zwischenspeicher (Cachespeicher[29]) betreffen, gesteuert und überwacht. Die MMU ist maßgebend für die Übersetzung von virtuellen Speicheradressen in physische Speicheradressen im Hauptspeicher.[30][47]

Um den für einzelne Prozesse benötigten Speicherplatz jederzeit erweitern oder freigeben zu können, erfolgt die Speicherverwaltung dynamisch. Damit der Speicher nicht unnötig befüllt ist, werden nur die Daten eines Prozesses in den RAM geladen, die zu dessen Ausführung bzw. der darin enthaltenen Aufgaben benötigt werden. Zusätzlich wird für jeden Prozess ein virtueller Adressraum initiiert, welcher mittels Seitentabellen durch die MMU codiert wird. Dabei funktionieren die Seitentabellen als eine Art Verweistabellen, welche die Adressierung zwischen den physischen Adressen im RAM und dem virtuellen Adressraum stellen.[20][47]

[28] Adress-, Daten- und Steuerbus. (siehe 2.5.3)
[29] Der Cachespeicher dient zur Speicher- und Zugriffsbeschleunigung. Häufig verwendete Daten werden temporär gespeichert, um den Zugriff, auf den langsameren RAM zu vermeiden.
[30] Dieses Vorgehen wird als Seitentabellenauflösung bezeichnet.

2.5.5 Datensicherung im RAM

Im Verlauf einer forensischen Sicherung von Computern werden alle Inhalte möglichst ohne schreibende Zugriffe erhalten, um Ihre Integrität zu garantieren (siehe Tabelle 2.1). Dies ist jedoch bei der Sicherung von Daten aus dem RAM nicht vollkommen möglich. Das betreffende Gerät muss noch im Betrieb sein, im Gegensatz einer Post-Mortem-Analyse[31], bei der der Computer bereits im abgeschalteten Zustand vorliegt und so die Daten im RAM, aufgrund seiner Definition als flüchtigen Speicher, nicht mehr vorhanden sind. Eine Datensicherung der Inhalte im RAM kann nur solange erfolgreich und zielführend sein, wie der entsprechende Computer eingeschaltet ist.[13]
Um während einer forensischen Datensicherung bzw. der Erstellung eines Abbilds des Datenträgers (bitweise eine 1:1-Kopie) keine Daten auf dem Original-Datenträger zu verändern, wird üblicherweise mit sogenannten Write-Blockern gearbeitet. Diese blockieren automatisch schreibende Zugriffe auf den angeschlossenen Datenträger. Zur Gewährleistung der Korrektheit und Integrität[32], sollten Datensicherungen, wenn möglich, immer auf dem aktuellsten Stand der Technik durchgeführt werden.[13][48]
Für die Sicherung der Daten im RAM, bzw. von flüchtigen Daten[33] wird spezielle Software benötigt, die teils auf einem Computer installiert werden muss, teils aber auch als portable Variante[34], die z. B. mittels eines USB-Sticks auf dem zu sichernden System zur Verfügung gestellt wird. Hierbei werden jedoch Daten auf dem entsprechenden Gerät verändert, meist Einträge in der Registry und Inhalte im RAM selbst.[13][48]

Werkzeuge zur Datensicherung im RAM

In Tabelle 2.3 werden kurz einige Werkzeuge zur forensischen Sicherung des RAM aufgelistet und beschrieben

Bezeichnung	Beschreibung
Volatility	Volatility ist ein Open-Source-Tool für die Speicherforensik. Mittels unterschiedlichen Befehlszeilenkommandos/Werkzeuge können die Inhalte des RAM interpretiert und analysiert werden.[49]
FTK Imager	Der FTK Imager ist ein forensisches Werkzeug, welches primär für die Sicherung von Festplatten verwendet wird. Mittels dieses Werkzeugs kann aber auch der Inhalt vom RAM gesichert werden.[50]
DumpIt	Mittels DumpIt kann der Inhalt des RAM erfasst und exportiert werden. Es kann direkt von einem bootfähigen USB-Stick gestartet werden und erfordert keine Installation.[51]
MemprocFS	Mit MemprocFS kann man Inhalte aus dem RAM sichern, ohne viele Kommandoline-Befehle nutzen zu müssen. Hierbei bedient MemprocFS sich u. a. der Funktionen von Dumpit und Volatility.[52]

Tabelle 2.3: Werkzeuge zur forensischen Sicherung des RAM

[31] Eine Analyse, die nach dem Ende/Abschluss des eigentlichen Ereignisses durchgeführt wird.
[32] Unversehrtheit von Daten
[33] Diese Art von Sicherung wird auch Live-System-Sicherung genannt.
[34] bedarf keiner Installation

Mögliche Probleme

Im Verlauf einer forensischen Sicherung des Hauptspeichers/RAM kann es zu unterschiedlichen Problemen bzw. Komplikationen kommen. Einige davon sind im Folgenden genannt.

- **Volatilität des Speichers:** Da es sich bei RAM um flüchtigen Speicher handelt, muss die Sicherung des RAMs vor dem Herunterfahren bzw. Abschalten des Systems durchgeführt werden.[53]
- **Zeitabhängigkeit:** Aus demselben Grund, besteht die Möglichkeit, dass Daten verloren gehen. Handeln unter Zeitdruck kann zu Fehlern oder gar unvollständigen Sicherungen führen.
- **Kompatibilität:** Nicht alle forensischen Werkzeuge sind mit jeder Hardware und jedem Operating System (OS) kompatibel.
- **Größe des Speichers:** Je größer der RAM desto zeitaufwändiger kann sich die Sicherung der im RAM befindlichen Daten gestalten.
- **Datenintegrität:** Fehlerhafte Sicherungsmethoden oder unprofessionelle Handhabung kann zu Beschädigungen der Daten bzw. ihrer Integrität führen.
- **Berechtigungen:** Meist sind für die Ausführung von forensischer Software, die u. a. Inhalte aus dem RAM sichert, ein Administrator- bzw. Root-Zugang oder Berechtigungen in gleichem Umfang von Nöten. Sind diese nicht verfügbar, können die Sicherungen kaum bis gar nicht durchgeführt werden.

2.6 Hiberfil und Pagefile

Im Verlauf einer forensichen Sicherung oder aber der Analyse von Computern sind neben den Inhalten im RAM auch die Inhalte auf Datenträgern (z. B. Festplatten) relevant. Darauf befinden sich hauptsächlich die Daten und Inhalte des Betriebsystems, der installierten Programme und Nutzer, wie z. B. Bilder, Videos, etc. Daneben befinden sich auf den Datenträgern teilweise aber auch Auslagerungs- und Systemdateien, die weitere wichtige Informationen enthalten können. Zu diesen Dateien gehören die Auslagerungsdatei Pagefile.sys und die Systemdatei Hiberfil.sys. Im Gegensatz zu den Inhalten im RAM werden die in der Pagefile.sys und der Hiberfil.sys enthaltenen Inhalte nicht standardmäßig durch das Herunterfahren des Systems gelöscht.[35][54]

2.6.1 Hiberfil.sys

Die Systemdatei Hiberfil.sys wird im Verlauf des sogenannten Hibernation-Modus bzw. auch Ruhezustands eines Comnputers genutzt, um den aktuellen Arbeitszwischenstand bzw. das aktuelle Setup des Nutzers zu speichern. Nach Beenden des Hibernation-Modus bzw. Ruhezustands wird anhand der Hiberfil.sys der vorherige Systemzustand wiederhergestellt.[54][55]

2.6.2 Pagefile.sys

Die Auslagerungsdatei Pagefile.sys dient auf einem Computer mit Windows-OS als Auslagerungsspeicher oder Entlastung für den RAM des Systems. In diese Datei werden Daten geschrieben, die aktuell nicht in den RAM passen, da dieser z. B. voll ist. Hierbei nutzt Windows einen Algorithmus, welcher entscheidet bzw. versucht zu prognostizieren, was als nächstes an Daten benötigt wird, um spezielle Aufgaben/Prozesse auszuführen.[54][56]

[35] Die Verwendung spezieller Sicherheitstools übernimmt teilweise das Löschen entsprechender Inhalte.

2.7 Virtualisierung

Im Folgenden werden der Grundgedanke bzw. die grundsätzlichen Funktionen und Aufgaben der Virtualisierung erläutert. Auch wird kurz auf den Begriff Virtuelle Maschine (VM), sowie auf die in dieser Bachelorarbeit verwendete Virtualisierungssoftware VirtualBox eingegangen.

Zuvor ist jedoch zu klären, was als physische Maschine definiert wird. Als solche wird ein Gerät, bestehend aus Hardware[36], wie z. B. ein Computer oder Server bezeichnet. Im Gegensatz zu VMs haben physische Maschinen einen fast direkten Zugriff auf die Hardware. VMs hingegen greifen auf Daten mittels ihrer Bezeichnungen zu und arbeiten so mit diesen.[58]

2.7.1 Virtuelle Maschine

Bei einer VM handelt es sich, laut den Herren Popek und Goldberg, um ein *„effizientes, isoliertes Duplikat einer echten Maschine“* (aus dem Englischen übersetzt).[58] Das grundsätzliche Prinzip einer VM beruht auf einer Software-Lösung, welche sich verhält, als wäre sie ein unabhängiges Gerät, z. B. ein Computer. Eine VM bietet dem Nutzer eine isolierte, vom OS des Hostsystems unabhängige Umgebung. In dieser Umgebung kann ein zum Hostsystem gleiches oder ähnliches, aber auch ganz anderes OS ausgeführt werden. Die VM ist lediglich von den physischen Ressourcen des Hostsystems abhängig. Jedoch sind diese virtualisiert, auf eine oder mehrere VMs aufgeteilt und bedarfsgerecht zuteilbar[37]. Diese Funktionalität ermöglicht es Nutzern, mehrere VMs mit unterschiedlichen OS und/oder Aufgaben auf einem physischen Gerät zu betreiben.[59] [60] VMs werden in zwei Typen unterteilt.[59]

- **Prozess-VM:** Temporäre Programmierumgebung, die plattformunabhängig als Anwendung fungiert, um einen Prozess auszuführen. Diese Art von VM wird erstellt, wenn der Prozess ausgeführt wird, und gelöscht, wenn der Prozess beendet ist.
- **System-VM:** Auf einem Hostsystem mittels Hypervisor erstellte und ausgeführte vollständig virtualisierte Umgebung, der ein eigenes OS zur Verfügung steht.

Über das Hostsystem bzw. den gewählten Hypervisor können die VMs durch den Nutzer eingerichtet und verwaltet werden.

Hypervisor

Computer, auf denen VMs betrieben werden, benötigen spezielle Software, die diese Funktion ermöglicht. Hierbei handelt es sich um einen sogenannten Hypervisor. Dieser emuliert die physischen Ressourcen und bei Bedarf auch das Netzwerk des Computers und erstellt daraus eine Art Pool, aus welchem den in Betrieb genommenen VMs die benötigten Ressourcen zugeordnet werden können. Die meisten Hypervisoren sind in eine der beiden in Tabelle 2.4 abgedruckten Kategorien einteilbar.[59]

[36] Als Hardware werden die technischen Bestandteile eines Gerätes bezeichnet. Sie sind sichtbar und physisch greifbar.[57]
[37] Dies sind z. B. Anzahl der Prozessorkerne, RAM-Größe etc.

	Typ 1	**Typ 2**
Ausführung	auf dem physischen Hostsystem	auf dem OS des Hostsystems
Hardwarezugriff	direkter Zugriff	Verwaltung durch OS des Hostsystems
Leistung	effizient und leistungsfähig	schwächer als Typ 1
Typische Anwendungsbereiche	Server-, Desktop- und Anwendungsvirtualisierung	Endbenutzersysteme (z.B. Entwickler)
Beispiele	Microsoft Hyper-V und VMware ESXi	VMware Workstation und Oracle VirtualBox

Tabelle 2.4: Unterschiedliche Hypervisor-Kategorien

Anwendungsbereiche

Heutzutage werden VMs in unterschiedlichen Bereichen genutzt. Neben der Verwendung von VMs in Unternehmen, i. d. R. zur besseren Überwachung und Verwaltung der verfügbaren Ressourcen, werden VMs auch von Privatpersonen, Studenten und einzelnen Arbeitskräften verwendet. So werden sie auch in den Bereichen der IT-Sicherheit und IT-Forensik verwendet. Hier können u. a. Prüfungen durchgeführt werden, ob gewisse Daten Schadsoftware enthalten und wie diese funktioniert. Auch können physische Maschinen mittels einer VM abgebildet und repliziert werden. Entsprechend können auch digitale Kopien von technischen Beweismitteln mittels VM hochgefahren werden, um im simulierten Live-Betrieb mögliche verfahrensrelevante Informationen zu sammeln.

Die Verwendung von VMs zur Prüfung auf und von Schadsoftware bietet den Vorteil, dass diese vom restlichen System und Netzwerk abgeschirmt durchgeführt und bei Bedarf auch auf ältere Zeitpunkte zurückgesetzt oder neu eingerichtet werden können, ohne wichtige Daten oder Inhalte zu gefährden.

2.7.2 Oracle VirtualBox

Die Virtualisierungs-Software VirtualBox wurde ursprünglich durch die deutsche Firma InnoTek Systemberatung GmbH entwickelt und nach Übernahme durch Oracle[38] weitergeführt.[58] Oracle bietet diese Software frei zum Download an, ebenso wie deren Quellcode. VirtualBox ist auf allen bekannten OS ausführbar und unterstützt auch das Betreiben entsprechender OS als VM.[61]

Mittels der in Abbildung 2.11 dargestellten Managementoberfläche können Nutzer ihre VMs einrichten, steuern und verwalten.

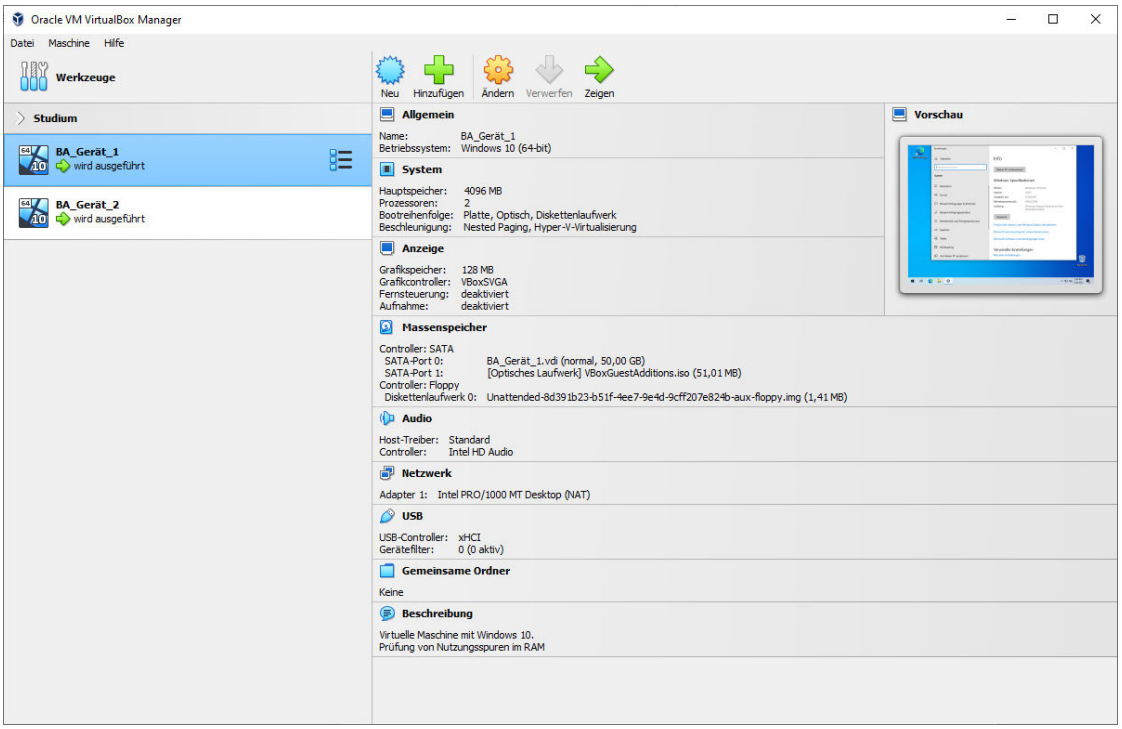

Abbildung 2.11: Oracle VirtualBox Benutzeroberfläche

Des Weiteren können hier die Ressourcen, die den jeweiligen VMs zugeteilt werden sollen, eingestellt und überwacht werden. Auch werden die VMs direkt über diese Oberfläche gestartet.

[38] Vormalig wurde die Übernahme durch Sun Microsystems durchgeführt, welche anschließend von Oracle übernommen wurden.

3 Methodik

Im Folgenden wird auf die Planung zum Testaufbau, die Testgeräte und die für die Durchführung benötigte Hard- und Software, sowie das Betriebssystem Windows eingegangen. Dabei werden vordefinierte Nachrichten, Systeminformationen und Informationen zu den für die Abwicklung erstellten Nutzerkonten aufgezeigt.[39]

3.1 Planung zum Testaufbau

Wie im Kapitel 2.5.5 erläutert, werden im Verlauf realer Sicherstellungen unterschiedliche Werkzeuge genutzt, um die auf den zu sichernden Systemen befindlichen Daten zu sichern. Dabei ist eine Unterscheidung zwischen der Sicherung von persistenten Daten, auf z. B. Festplatten etc., und der flüchtiger Daten, z. B. im RAM, zu treffen.
Nichtflüchtige Daten können im Verlauf einer Post-Mortem-Analyse mittels Anschließen über Write-Blocker[40] unverändert und gemäß der vorgeschriebenen Regelungen exportiert und untersucht werden. Flüchtige Daten müssen vor dem Herunterfahren des jeweiligen Systems gesichert werden, wobei es hier meist notwendig ist, ein Programm auf dem System auszuführen. Dieser Unterschied in der Vorgehensweise birgt die Gefahr, dass Daten auf dem betroffenen System verändert, gelöscht oder erstellt werden.

Für die in dieser Arbeit zu prüfenden Durchläufe werden zwei virtuelle Maschinen mit Hilfe des Hypervisors VirtualBox eingerichtet. Durch die Nutzung von VMs soll eine möglichst realitätsnahe Imitation einer Sicherstellung ermöglicht werden. Zu betonen ist, dass sich diese Arbeit auf die Analyse von Daten und Inhalten im RAM fokussiert. Mögliche Artefakte oder Spuren, die auf Festplatten vorhanden sein könnten, werden in dieser Arbeit nicht beachtet.

3.2 Planung zur Generierung der Testdaten

Um im Verlauf der Analyse der gesicherten Dateninhalte des RAMs schnellstmöglich auswertbare Ergebnisse zu erhalten, wird für jeden Versuchsdurchlauf eine vorab festgelegte Kommunikation geführt. Innerhalb dieser Konversation werden zwischen dem lokalen Nutzer und seinem Chatpartner Textnachrichten und Bilddateien ausgetauscht. Die Inhalte der Textnachrichten (Inhalt, Sender) sind in der Tabelle 3.1 und Details zu den übertragenen Dateien (Titel, MD5-Hashwert[41], Dateigröße in KB und Quelle der Bilddatei) in der Tabelle 3.2 abgedruckt.

[39] Informationen, die Rückschlüsse auf reale Personen erlauben, werden bestmöglich zensiert.
[40] Write-Blocker verhindern ungewollte Schreibzugriffe auf das angeschlossene Gerät.
[41] Message Digest Algorithm. Erzeugt 128-Bit Hashwerte für Zeichenketten oder Dateien. Eine Änderung der Datei verändert den Hashwert. Dateien lassen sich anhand von MD5-Hashes identifizieren.[62]

Typ	Inhalt/Beschreibung	Sender
Textnachricht 0	Hi!	Chatpartner
Textnachricht 1	Schau dir unbedingt mal die Aufnahme von dem Hundewelpen an! *(Übertragung der Bilddatei 1)*	lokaler Nutzer
Textnachricht 2	Oh wow. Der ist ja beeindruckend!	Chatpartner
Textnachricht 3	Ja, total. Ich bin mehr als begeistert!	lokaler Nutzer
Textnachricht 4	Hast du Bilder oder Videos von Hundewelpen, die wir tauschen können?	lokaler Nutzer
Textnachricht 5	Du da muss ich mal schauen, was ich so auftreiben kann. . .	Chatpartner
Textnachricht 6	Wie ist deine Meinung zu dem Kleinen hier? *(Übertragung der Bilddatei 2)*	Chatpartner
Textnachricht 7	Ich bin kein Fan von Shar Pei´s	lokaler Nutzer
Textnachricht 8	Dann kann ich dir leider nichts aus meiner Sammlung anbieten..	Chatpartner
Textnachricht 9	Das ist ärgerlich. Aber ich nehms dir nicht übel!	lokaler Nutzer
Textnachricht 10	Na da hab ich nochmal Glück gehabt!	Chatpartner

Tabelle 3.1: Auflistung der Nachrichten

Typ	Details
Bilddatei 1	Titel: `Pitbull_Welpe.jpg` MD5-Hashwert: `fdd4ec5ed0f395e02062bec3d29d890d` Dateigröße: 88,7 KB Quelle [63]
Bilddatei 2	Titel: `SharPei_Welpe.jpg` MD5-Hashwert: `fa8ca7a5fbcf0ac98f169f4212adba61` Dateigröße: 104 KB Quelle [64]

Tabelle 3.2: Auflistung der Testdaten

Im Gegensatz zu realen Untersuchungen sind die in dieser Arbeit genutzten Schlüsselbegriffe vorab bekannt. Bei realen Verfahren ist dies oft nicht der Fall, da meist wenige Nutzerdaten und teilweise nur Ausschnitte möglicher Übertragungen vorliegen. Das tatsächliche Feststellen relevanter Inhalte erfolgt erst im Verlauf und gestaltet sich daher in realen Analysen um ein Vielfaches arbeits- und zeitaufwändiger, als in einem geplanten Versuchsaufbau.

3.3 Erstellen der Testumgebung

Im Folgenden werden die Programme, das Betriebssystem und die einzelnen Spezifikationen der VMs erläutert. Die im Verlauf der Szenarien genutzten Anwendungen, sowie die Windows 10 Installationsdatei (ISO-Datei) werden soweit möglich jeweils von den Webseiten der jeweiligen Hersteller heruntergeladen. Als Host-System dient ein Computer mit dem Betriebssystem Windows 10 Pro[42]. In diesem sind 32GB DDR4-RAM und ein Intel Core i7-8700K @3.70GHz verbaut.

Virtual Box

In dieser Arbeit wird als Hypervisor die Software VirtualBox von Oracle in der Version 7.0.8 verwendet und auf dem OS des Host-Systems installiert.[61] Neben der Installation von benötigten Treibern[43] wurden keine Veränderungen an der Standardkonfiguration durchgeführt. Nach der Installation des Hypervisors werden die beiden VMs *BA Gerät 1* und *BA Gerät 2* installiert und eingerichtet. In der Tabelle 3.3 werden die Spezifikationen der einzelnen VMs aufgelistet. Die vom Hypervisor vorgeschlagenen Einstellungen wurden zum großen Teil übernommen. Abweichungen wurden aus Gründen der Performance vorgenommen und sind nachfolgend *kurisv* hervorgehoben.

Virtuelle Maschine	**BA_Gerät_1**	**BA_Gerät_2**
Betriebssystem/OS	Windows 10 Home 64Bit	Windows 10 Home 64Bit
Grafikspeicher	128MB	128MB
Prozessor	2 Kerne *default 1*	2 Kerne *default 1*
Arbeitsspeicher	4096MB *default 2048*	4096MB *default 2048*
Virtuelle Festplatte	50GB	50GB

Tabelle 3.3: Konfiguration der VMs

Windows 10

Windows 10 wurde im Jahr 2015 veröffentlicht und erhält seitdem regelmäßige Updates. Es *„wurde konzipiert, um die Produktivität von Nutzern in Zeiten der fortschreitenden Digitalisierung zu fördern.“*[65] Im Vergleich zu den Vorgängern will sich Microsoft mit Windows 10 stärker gegenüber Open Source öffnen und dank des Service-Modells ’WaaS’ - ’Windows as a Service’ sowohl im Unternehmens-, als auch im Privat-Bereich nutzbar sein. Dies soll durch regelmäßige Feature-Updates ermöglicht werden, die meist aktualisierte Versionen von Windows 10 darstellen und neue Funktionen, wichtige Änderungen und visuelle Verbesserungen beinhalten. Die Updates sollen etwa alle 6 Monate erscheinen. Kleinere Updates, die Bugs, Fehler und Sicherheitslücken behandeln, erscheinen normalerweise in 14-tägigen Abständen. Der Support für Windows 10 soll im Oktober 2025 eingestellt werden und Windows 10 durch das seit Oktober 2021 erhältliche Windows 11 ersetzt werden.[65][66][67]

[42] Version 22H2. Build 19045.2965
[43] Es wurden spezielle Treiber für die Virtualisierung benötigt.

Windows 10 bietet neben dem klassischen Herunterfahren noch weitere Energiesparmodi. Es wird zwischen Energie sparen und Ruhezustand unterschieden. Beide Modi versprechen dem Nutzer ein schnelleres Hochfahren des Computers und Wiederherstellen der aktiven Sitzung.

- **Energiesparen** (engl. Standby)[44]
  Der Computer wird in einen Niedrigenergiemodus versetzt, in welchem die Inhalte und laufenden Programme im RAM verbleiben. Nicht benötigte Komponenten werden ausgeschaltet. Wird der Computer wieder eingeschaltet, kann der Nutzer fast direkt dort fortfahren, wo er zuvor aufgehört hat.[67]
- **Ruhezustand** (engl. Hibernate)[45]
  Alle geöffneten Programme und Inhalte werden auf die Festplatte geschrieben[46]. Nachteil ist, dass das Herunter- und Hochfahren etwas länger brauchen, jedoch der Computer im Ruhezustand selbst kaum bis keinen Strom benötigt.[67]

Mittels des MediaCreationTool22H2 wurde ein Windows 10-Abbild bzw. eine .iso-Datei erzeugt und für das Einrichten der VMs in VirtualBox eingebunden.[68] Auf den VMs wurde das Betriebssystem Microsoft Windows 10[47] auf Deutsch mit entsprechendem Tastaturlayout und Zeitzone installiert. Die Aktivierung der Windows 10 Installationen mittels Lizenzschlüssel ist für diese Arbeit nicht erforderlich, da die VMs nur kurzzeitig in Verwendung sind und anschließend zurückgesetzt und/oder gelöscht werden. Des Weiteren wurden alle notwendigen Betriebssystemupdates heruntergeladen und eingerichtet.

Internetbrowser

Im Verlauf der Tests wird u.a. geprüft, ob die Nutzung unterschiedlicher Internetbrowser Auswirkungen auf die Menge an Befunden bzw. Art der Artefaktspeicherung hat. Zur Durchführung der Tests werden drei der weltweit meist verwendeten Internetbrowser gewählt: Google Chrome, Microsoft Edge und Mozilla Firefox.[69][48]

In Tabelle 3.4 werden Eigenschaften dieser Internetbrowser abgedruckt. Hierbei werden Unterschiede, wie Benutzeroberfläche, Design und Umfang von nutzbaren Erweiterungen nicht beachtet.[70] Alle Browser sind sowohl auf den Computer-OS Windows, macOS und Linux, als auch auf den mobilen OS Android und iOS verfügbar.

	Google Chrome	**Microsoft Edge**	**Mozilla Firefox**
Hersteller	Google	Microsoft	Mozilla
Rendering-Engine	Blink-Engine	Blink-Engine	Gecko-Engine
Speicher-Belastung (Leerlauf)	115 MByte	270 MByte	180 MByte
Speicher-Belastung (Belastung)	1,8 GByte	1,5 GByte	1,6 GByte

Tabelle 3.4: Browser-Vergleich

[44] Auch Suspend to RAM
[45] Auch Suspend to Disk
[46] Auch als Ist-Zustand des Computers bezeichnet
[47] Version 22H2
[48] Google Chrome V.113.0; Microsoft Edge V.114.0.1823.11; Mozilla Firefox V.113.0.2

Nutzerkonten

Im Folgenden sind die für diese Arbeit verwendeten Nutzerdaten aufgeführt.[49] Da für die Erstellung von Threema-Nutzerkonten jeweils eine Lizenz gekauft werden muss, wurden hierfür private Nutzerdaten verwendet, die nachstehend zensiert oder abgeändert sind.[50]

In der Tabelle 3.5 sind die Daten zu den Nutzerkonten von Instagram[51], in der Tabelle 3.6 die Daten zu denjenigen von Threema zu finden.

	Nutzerkonto 1	**Nutzerkonto 2**
Nutzername	*mustermann*	*musterfrau*
Nutzerkennung	*Mustermann*	*Musterfrau*
Nutzer-ID	*82801763244*	*39511522425*
VM	BA_Gerät_1	BA_Gerät_2

Tabelle 3.5: Nutzerdaten Instagram

	Nutzerkonto 1	**Nutzerkonto 2**
Nutzername	*Max Mustermann*	*Erika Musterfrau*
Nutzer-ID	*UGM3OY7Q*	*Y3OMKEQV*
VM	BA_Gerät_1	BA_Gerät_2

Tabelle 3.6: Nutzerdaten Threema

Vorbereitend wurden auf beiden VMs die zu verwendenden Nutzerkonten in jedem Internetbrowser angemeldet. Bei Instagram reicht es aus, ein Nutzerkonto einmalig anzumelden. Bei erneutem Öffnen des Internetbrowsers muss keine erneute Anmeldung durchgeführt werden. Gegensätzlich dazu muss für die Nutzung des Webclients von Threema mittels QR-Code eine Verbindung zwischen dem Mobiltelefon und dem gewählten Internetbrowser eingerichtet werden. Der Nutzer kann, um bei erneutem Öffnen des Internetbrowsers und Aufrufen des Webclients nicht erneut den QR-Code scannen zu müssen, ein Kennwort vergeben, welches stattdessen einzugeben ist. Hier wurde das Kennwort '`BA1_2023!`' gewählt.

Forensische Software

Nach Erstellung der RAM-Dumps sollen diese durch Verwendung der Software HxD-Editor stichprobenartig auf ihren Inhalt überprüft werden. Anschließend sollen die einzelnen RAM-Dumps mittels des Werkzeugs MemProcFS aufgearbeitet und mithilfe der forensischen Software Forensic-Explorer analysiert werden.

[49] Informationen, die Rückschlüsse auf reale Personen erlauben, werden bestmöglich zensiert.
[50] Stark veränderte, bzw. ausgetauschte Nutzerdaten sind *kursiv* markiert.
[51] Aufgrund der veränderten Richtlinien konnten keine Nutzerkonten ohne echten Personenbezug erstellt werden, ohne einen komplexeren Verifizierungsprozess zu durchlaufen.

3.4 Ablauf der Szenarien

Nachfolgend werden die für diese Arbeit gewählten Szenarien genauer erläutert. Diese werden für jede Anwendung (Threema und Instagram) und jeden Internetbrowser (Google Chrome, Microsoft Edge und Mozilla Firefox) individuell durchgeführt, was in sechs Testdatensätzen pro Szenario resultiert.
Durch Verwendung unterschiedlicher Szenarien soll geprüft werden, welchen Einfluss unterschiedliche Faktoren auf die Persistenz, das Vorhandensein und die Qualität von Inhalten innerhalb des RAM haben. Die Analyse der Datensicherung soll zeigen, ob Artefakte innerhalb der RAM-Dumps feststellbar sind und in Verbindung mit der jeweiligen Anwendung gebracht werden können. Dabei sollen mögliche Unterschiede und Gemeinsamkeiten zwischen den einzelnen Internetbrowsern festgestellt und mögliche Identifikatoren für relevante Inhalte herausgearbeitet werden.

3.4.1 Szenario 1: Sicherung bei laufendem Browser

Die Sicherung des RAM wird durchgeführt, während der Webclient der gewählten Anwendung mittels Internetbrowser aufgerufen vorliegt.

3.4.2 Szenario 2: Sicherung bei beendetem Browser

Zum Zeitpunkt der Sicherung des RAM ist der Internetbrowser und der darin aufgerufene Webclient der gewählten Anwendung bereits geschlossen.
Das Schließen des Internetbrowsers wurde kurz (1-3 Minuten) vor der Erzeugung des RAM-Dumps durchgeführt, ohne dass weitere Programme oder Aktionen ausgeführt werden.

3.5 Generierung der Testdaten

Es folgt ein Überblick über die Generierung der einzelnen RAM-Dumps[52], der mit dem grundlegenden Ablauf von der Erzeugung der Testdaten bis hin zur Erzeugung des RAM-Dumps beginnt.

3.5.1 Generierung

Für jede Anwendung wird mittels der bereits eingerichteten VMs ein Internetbrowser[53] gestartet und der jeweilige Webclient aufgerufen. Anschließend wird die geplante Konversation (siehe 3.2) zwischen den vorher eingerichteten Nutzerkonten (siehe 3.3) geführt. Daraufhin wird je nach durchzuführendem Szenario mit dem gewählten Browser umgegangen (siehe 3.4). Nachdem die Testdaten erzeugt sind, wird auf dem Host-System mittels der Windows-Eingabeaufforderung Command Prompt (CMD) geöffnet und in das Verzeichnis von VirtualBox navigiert. Hier wird nun mittels des im Folgendem abgedruckten Befehls ein RAM-Dump der VM **BA_Gerät_1** erzeugt.[54][71]

```
vboxmanage debugvm <VM> dumpvmcore -filename <Pfad><Dateiname>.dmp
```

[52] Als Dump wird ein Speicherauszug beschrieben.
[53] Google Chrome, Mozilla Firefox oder Microsoft Edge
[54] Auf das Erzeugen eines Dumps von **BA_Gerät_2** wird verzichtet, da beide VMs gleiche Konfigurationen vorweisen und sich nur der jeweilige lokale Nutzer der Chatanwendung unterscheidet.

Durch eine vorab definierte Bezeichnung der jeweiligen RAM-Dumps soll eine eindeutige Unterscheidung ermöglicht werden. Die Erzeugung der Bezeichnungen erfolgt nach dem Schema `BAX_RAM_Y_Z.dmp`. Die Werte der Variablen **X**, **Y** und **Z** werden in der Tabelle 3.7 abgedruckt.

Variable	Inhalt	Beispiele
X	Angabe des Szenarios	**1**: Szenario 1 (Abschnitt 3.4.1) **2**: Szenario 2 (Abschnitt 3.4.2)
Y	Angabe des Internetbrowsers	**g**: Google Chrome **m**: Moziila Firefox **e**: Microsoft Edge
Z	Angabe der Anwendung	**T**: Threema **IG**: Instagram

Tabelle 3.7: Mögliche Variablen-Inhalte

Jede Erstellung eines RAM-Dumps beginnt mit dem Hochfahren der VMs und dem Starten des für das aktuelle Vorgehen gewählten Internetbrowsers und der betreffenden Chatanwendung. Anschließend werden die im jeweiligen Szenario angegebenen Aktionen durchgeführt.
Nach Generierung des jeweiligen RAM-Dumps werden die Chatinhalte gelöscht, der jeweilige Browser-Cache geleert und die VM vollständig heruntergefahren.

3.5.2 Threema

Als nächstes ist beispielhaft die Generierung von Testdaten für die Anwendung Threema, unter Verwendung des Internetbrowsers Google Chrome, für Szenario 1 abgedruckt. Anzumerken ist, dass für die Nutzung des Threema-Webclients eine Kennworteingabe benötigt wird, sollte eine Sitzung bereits eingerichtet und gespeichert sein[55]. Wie die Abbildung 3.1 zeigt, wird die Erzeugung der Testdaten mittels Parallelbetrieb der VMs druchgeführt.

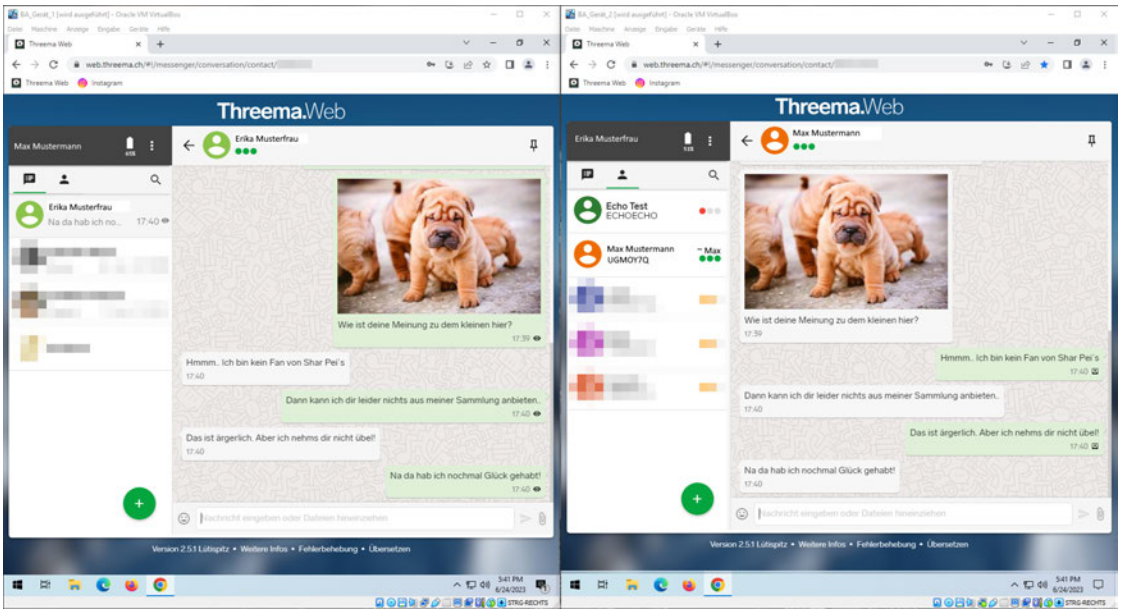

Abbildung 3.1: Testdaten-Erzeugung Threema

[55] In dieser Arbeit wurde die Sitzung bereits eingerichtet.

3.5.3 Instagram

Nachstehend ist beispielhaft die Generierung von Testdaten für die Anwendung Instagram, unter Verwendung des Internetbrowsers Microsoft Edge, für Szenario 2 abgedruckt. Wie die Abbildung 3.2 beispielhaft zeigt, wird auch hier die Erzeugung der Testdaten mittels Parallelbetrieb der VMs druchgeführt.

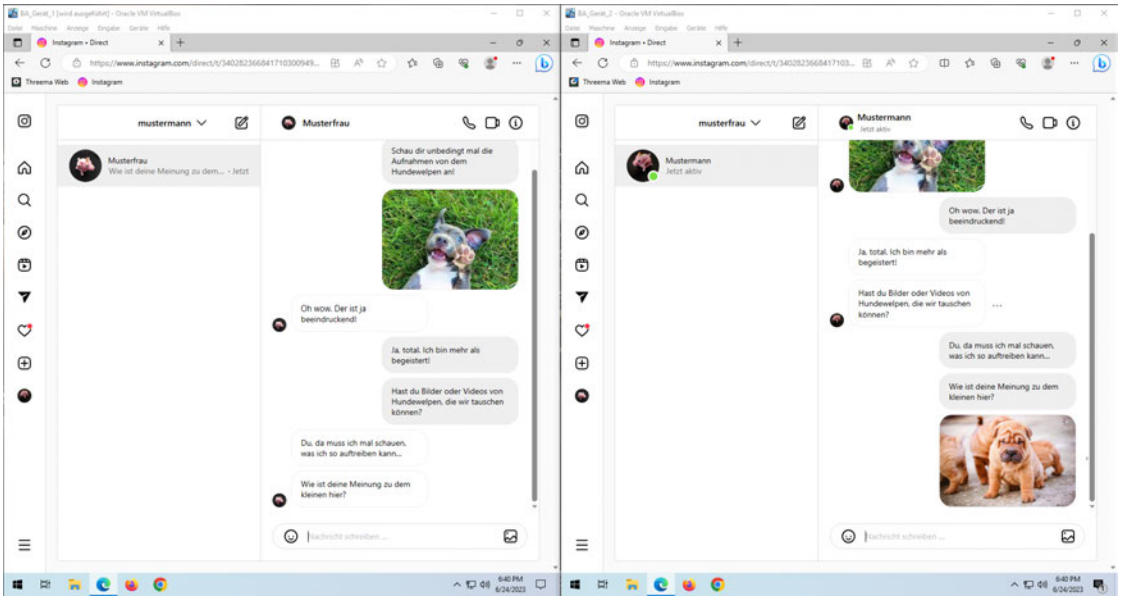

Abbildung 3.2: Testdaten-Erzeugung Instagram

3.6 Probleme

Nach Erstellung der RAM-Dumps sollten diese mit dem Werkzeug MemProcFS bearbeitet und gemountet[56] werden. Anschließend sollte das gemountete Laufwerk bzw. die darin enthaltenen Daten mittels der forensischen Software Forensik Explorer akquiriert und analysiert werden. Allerdings stellte sich im Verlauf der Prüfung des geplanten Vorgehens herraus, dass zum einen die Akquise jedes einzelnen RAM-Dumps sehr zeitaufwendig war und zum anderen auch eine Volltextsuche nach den vorab definierten Schlüsselbegriffen (siehe Tabelle 3.1) keine Suchtreffer ergab. Aufgrund dessen wurde der Ablauf der Datenanalyse wie folgt angepasst:
Einzelne RAM-Dumps werden mittels der Software HxD-Editor geöffnet und analysiert. Mit Hilfe der Funktionen des HxD-Editors werden u. a. Suchen nach den Schlüsselbegriffen vorgenommen, um relevante Stellen und Inhalte innerhalb der RAM-Dumps festzustellen.

[56] Das Einbinden eines physischen/virtuellen Laufwerks/Speichers

4 Analyse der Nutzungsspuren

In diesem Kapitel werden die erstellten Testdaten (RAM-Dumps) aufgearbeitet und analysiert. Hierbei werden zu Beginn aufgetretene Anomalien und anschließend die Untersuchung der Testdaten zu den einzelnen Szenarien und Anwendungen erläutert. Die Analyse der jeweiligen RAM-Dumps wird mittels HxD-Editor durchgeführt. Dabei wird das Vorhandensein der vorab festgelegten Chatinhalte mittels Suchfunktion überprüft. Zusätzlich wird geprüft, ob weitere Informationen, wie z.B. Zeitstempel, Nutzerinformationen, Zugangsdaten und Dateiübertragungsdetails feststellbar und identifizierbar sind. Die Durchführung der Volltextsuche im HxD-Editor erfolgte unter Verwendung der Textcodierung Windows (*ANSI*). Eine Prüfung verschiedener Bytereihenfolgen (*Little Endian* oder *Big Endian*) war nicht erforderlich, da in der gewählten Kodierung jedes Zeichen lediglich aus einem Byte besteht.

Die Resultate wurden in Tabellen festgehalten. Dabei wurde bei Mehrfachtreffern einzelner Schlüsselbegriffe bzw. Nachrichten zufällig ein Ergebnis als Beispiel gewählt. Die Anzahl der identischen Treffer (auch unter Berücksichtigung von Groß- und Kleinschreibung) wird in der jeweiligen Tabelle angegeben.

Hinweis:
Die im Folgenden abgedruckten Tabellen wurden zur besseren Lesbarkeit gekürzt und enthalten daher nur einen Auszug der Ergebnisse. Die vollständigen Ergebnisse sind im Anhang abgedruckt.

4.1 Szenario 1: Sicherung bei laufendem Browser

Im Folgenden werden die Inhalte der für Szenario 1 erstellten RAM-Dumps analysiert. Es werden die jeweiligen Feststellungen pro RAM-Dump, in Anwendung und Internetbrowser aufgeteilt, aufgelistet und beschrieben.

4.1.1 Threema

Die Analyse der RAM-Dumps `BA1_RAM_g_T`, `BA1_RAM_e_T` und `BA1_RAM_m_T` durch den des HxD-Editors ergaben unterschiedliche Feststellungen. Diese werden im Folgenden für jeden Internetbrowser auszugsweise durch Bildschirmaufnahmen von Ausschnitten aus den jeweiligen RAM-Dumps und weitere Inhalte in Form von Tabellen veranschaulicht.

Google Chrome

Die Analyse der RAM-Dump-Datei `BA1_RAM_g_T.dmp` ergab untenstehende Feststellungen:
Das Ergebnis der Suche nach dem vorab festgelegten Kennwort für den Weblogin des Webclients von Threema ist in der Abbildung 4.1 dargestellt.

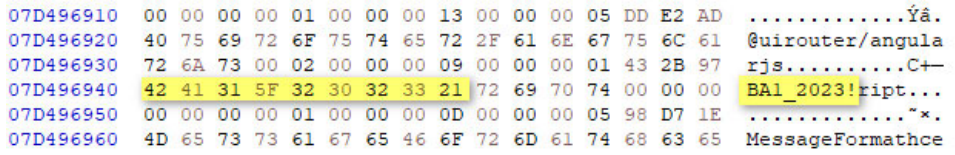

Abbildung 4.1: Threema Kennwort im Google Chrome RAM-Dump

Das für die Anmeldung des mit dem Browser verbundenen Threema-Nutzerkontos benötigte Kennwort ist vollständig im RAM-Dump vorhanden.

Aus den Tabellen 4.1 und 4.2 ist ersichtlich, ob die vorab definierten Nachrichten, Bilddateien[57] und Nutzerdaten (siehe Tabellen 3.1 und 3.6) in dem RAM-Dump teilweise oder vollständig vorhanden und möglicherweise rekonstruierbar sind.

Suchbegriff	Feststellbar	10 Hex-Werte vor	10 Hex-Werte nach
Threema	Vollständig vorhanden (8601 Treffer)	02 08 00 19 A9 B0 77 65 62 2E	2E 63 68 2F 69 6D 67 2F 66 61
Kennwort	Vollständig vorhanden (1 Treffer)	00 00 09 00 00 00 01 43 2B 97	72 69 70 74 00 00 00 00 00 00
Threema ID lokaler Nutzer	Vollständig vorhanden (46 Treffer)	73 61 74 69 6F 6E 2F 6D 65 2F	2F 64 65 74 61 69 6C 2F 65 64
Threema ID Chatpartner	Vollständig vorhanden (227 Treffer)	6E 2F 63 6F 6E 74 61 63 74 2F	2F 64 65 74 61 69 6C 00 69 73
Textnachricht 1	Vollständig vorhanden (8 Treffer)	00 00 3C 00 00 00 01 BC F4 EC	00 00 00 00 00 00 00 00 00 00
Textnachricht 2	Vollständig vorhanden (4 Treffer)	00 00 03 00 00 00 21 00 00 00	00 00 00 AD 09 00 00 58 00 00
Textnachricht 6	Vollständig vorhanden (7 Treffer)	00 00 03 00 00 00 2A 00 00 00	00 00 D5 09 00 00 0C 00 00 00

Tabelle 4.1: Auszug der Ergebnisse BA1_RAM_g_T.dmp Teil 1

[57] .jpg Dateien sind anhand der Hex-Start-Werte (Header) `FF D8 FF` und der Endwerte (Trailer) `FF D9` identifizierbar.[72]

Suchbegriff	Feststellbar	Beschreibung
Bilddatei 1 (durch lokalen Nutzer übertragen)	Hinweise feststellbar	Original-Pfad der Bilddatei 1 Bilddaten nicht rekonstruierbar
Bilddatei 2 (durch Chatpartner übertragen)	keine Hinweise feststellbar	-

Tabelle 4.2: Auszug der Ergebnisse BA1_RAM_g_T.dmp Teil 2

Neben den oben genannten Feststellungen konnten Hinweise auf folgende Inhalte in dem RAM-Dump registriert werden:

- Hinweise auf Status der Nachricht
  Die Nachricht ist beim Gerät des Empfängers angekommen
  Dieser Status konnte nur teilweise festgestellt werden.
- Die Threema-Nutzer-ID des lokalen Nutzers ist anhand folgenden Inhalts feststellbar:
  "*web.threema.ch/#!/messenger/conversation/me/**X***"
  Dabei steht das X als Variable für die jeweilige Threema-ID (in diesem Falle UGM3OY7Q).
- Die Threema-Nutzer-ID des Chatpartners ist anhand folgenden Inhalts feststellbar:
  "*web.threema.ch/#!/messenger/conversation/contact/**X***"
  Dabei steht das X als Variable für die jeweilige Threema-ID (in diesem Falle Y3OMKEQV).

Microsoft Edge

Während der Analyse der RAM-Dump-Datei `BA1_RAM_e_T.dmp` wurden die folgenden Erkenntnisse festgestellt:
In der Abbildung 4.2 ist ein Ergebnis der Suche nach der vordefinierten Nachricht 1 abgebildet. Zusätzlich konnte die folgende Meldung festgestellt werden: *Die Nachricht wurde erfolgreich an den Server übermittelt*.

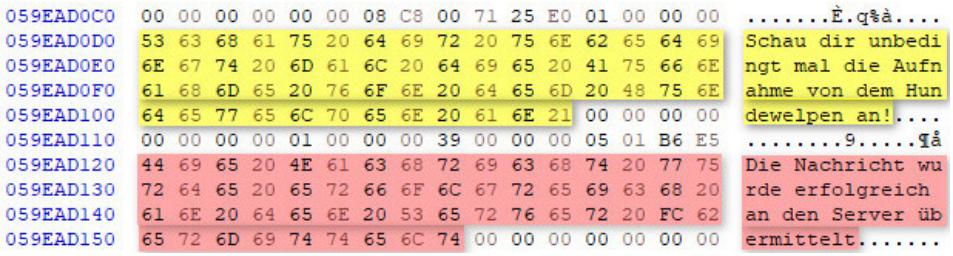

Abbildung 4.2: Vollständige Nachricht im Microsoft Edge RAM-Dump

Anhand der Tabellen 4.3 und 4.4 ist ersichtlich, ob die vorab definierten Nachrichten, Bilddateien und Nutzerdaten (siehe Tabellen 3.1 und 3.6) in dem RAM-Dump teils oder vollständig vorhanden und möglicherweise rekonstruierbar sind.

Suchbegriff	Feststellbar	10 Hex-Werte vor	10 Hex-Werte nach
Threema	Vollständig vorhanden (9455 Treffer)	74 70 73 3A 2F 2F 77 65 62 2E	2E 63 68 2F 23 21 2F 6D 65 73
Kennwort	Vollständig vorhanden (1 Treffer)	00 00 09 00 00 00 01 43 2B 97	00 00 00 00 00 00 00 00 00 00
Threema ID lokaler Nutzer	Vollständig vorhanden (1 Treffer)	00 00 22 9E CA D3 08 00 00 00	E9 01 00 00 20 00 00 00 9E FF
Threema ID Chatpartner	Vollständig vorhanden (258 Treffer)	6E 2F 63 6F 6E 74 61 63 74 2F	00 13 7A 6D 57 D2 E7 00 00 00
Textnachricht 1	Vollständig vorhanden (9 Treffer)	08 C8 00 71 25 E0 01 00 00 00	00 00 00 00 00 00 00 00 01 00
Textnachricht 2	Vollständig vorhanden (4 Treffer)	00 00 03 00 00 00 21 00 00 00	00 00 00 1D 05 00 00 8A DE 86
Textnachricht 6	Vollständig vorhanden (5 Treffer)	00 00 03 00 00 00 2A 00 00 00	00 00 E9 01 00 00 40 00 00 00

Tabelle 4.3: Auszug der Ergebnisse BA1_RAM_e_T.dmp Teil 1

Suchbegriff	Feststellbar	Beschreibung
Bilddatei 1 (durch lokalen Nutzer übertragen)	Hinweise feststellbar	Original-Pfad der Bilddatei 1 Bilddaten nicht rekonstruierbar
Bilddatei 2 (durch Chatpartner übertragen)	keine Hinweise feststellbar	-

Tabelle 4.4: Auszug der Ergebnisse BA1_RAM_e_T.dmp Teil 2

Neben den oben aufgelisteten Feststellungen konnten Hinweise auf folgende Inhalte in dem RAM-Dump festgestellt werden:

- Hinweise auf Status der Nachricht
  '*Die Nachricht wurde erfolgreich an den Server übermittelt*'
  Dieser Status konnte nur teilweise festgestellt werden.
- Die Threema-Nutzer-ID des Chatpartners ist anhand folgenden Inhalts feststellbar:
  '*web.threema.ch/#!/messenger/conversation/contact/**X***'
  Dabei steht das **X** als Variable für die jeweilige Threema-ID (in diesem Falle Y3OMKEQV).
- Teilweise werden vor oder nach der Übertragung von Nachrichten Zeitstempel (Bsp.: `25. Jun. 2023, 16:26`) angefügt. Dies geschieht nicht bei jeder Nachricht.

Mozilla Firefox

Bei der Analyse der RAM-Dump-Datei `BA1_RAM_m_T.dmp` wurden folgende Ergebnisse erzielt:
In der Abbildung 4.3 ist ein Ergebnis der Suche nach Hinweisen auf die Übertragung der Bilddatei 1 gezeigt. Innerhalb des RAM-Dumps kann der Original-Pfad der zu übertragenen Datei nachgewiesen werden.

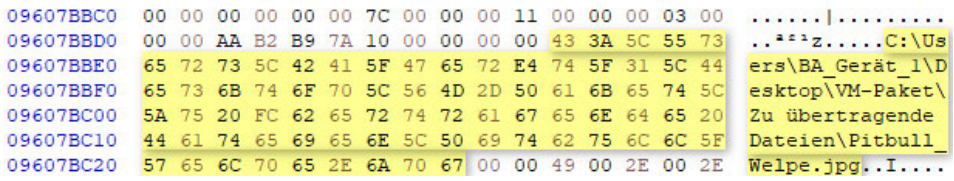

Abbildung 4.3: Pfadangabe der Bilddatei 1 im Mozilla Firefox RAM-Dump

Anhand der Tabellen 4.5 und 4.6 ist ersichtlich, ob die vorab definierten Nachrichten, Bilddateien und Nutzerdaten (siehe Tabellen 3.1 und 3.6) in dem RAM-Dump teilweise oder vollständig vorhanden und möglicherweise rekonstruierbar sind.

Suchbegriff	Feststellbar	10 Hex-Werte vor	10 Hex-Werte nach
Threema	Vollständig vorhanden (12218 Treffer)	74 70 73 3A 2F 2F 77 65 62 2E	2E 63 68 2F 23 21 2F 6D 65 73
Kennwort	Vollständig vorhanden (5 Treffer)	A1 A3 50 02 00 00 09 00 00 00	00 00 00 00 80 F8 FF 10 02 00
Threema ID lokaler Nutzer	Vollständig vorhanden (12 Treffer)	73 61 74 69 6F 6E 2F 6D 65 2F	2F 64 65 74 61 69 6C 2F 65 64
Threema ID Chatpartner	Vollständig vorhanden (480 Treffer)	6E 2F 63 6F 6E 74 61 63 74 2F	BF BF BF 80 D7 D0 C3 6B 02 00
Textnachricht 1	Vollständig vorhanden (2 Treffer)	E5 E5 E5 E5 E5 E5 E5 E5 E5 E5	E5 E5 E5 E5 C8 28 B2 FF 99 01
Textnachricht 2	Vollständig vorhanden (2 Treffer)	00 00 60 71 1F 02 9D 01 00 00	E5 E5 E5 E5 E5 E5 E5 E5 E5 E5
Textnachricht 6	Vollständig vorhanden (3 Treffer)	E5 E5 E5 E5 E5 E5 E5 E5 E5 E5	E5 E5 E5 E5 E5 E5 E5 E5 E5 E5

Tabelle 4.5: Auszug der Ergebnisse BA1_RAM_m_T.dmp Teil 1

Suchbegriff	Feststellbar	Beschreibung
Bilddatei 1 (durch lokalen Nutzer übertragen)	Hinweise feststellbar	Original-Pfad der Bilddatei 1 Bilddaten nicht rekonstruierbar
Bilddatei 2 (durch Chatpartner übertragen)	keine Hinweise feststellbar	-

Tabelle 4.6: Auszug der Ergebnisse BA1_RAM_m_T.dmp Teil 2

Neben den in den Tabellen 4.5 und 4.6 aufgelisteten Feststellungen konnten Hinweise auf folgende Inhalte in dem RAM-Dump festgestellt werden:

- Hinweise auf Status der Nachricht
  '*Die Nachricht wird an den Threema-Server übermittelt*'
  Dieser Status konnte nur teilweise festgestellt werden.
- Die Threema-Nutzer-ID des lokalen Nutzers ist anhand folgenden Inhalts feststellbar:
  '*web.threema.ch/#!/messenger/conversation/me/**X***'
  Dabei steht das **X** als Variable für die jeweilige Threema-ID (in diesem Falle UGM3OY7Q).
- Die Threema-Nutzer-ID des Chatpartners ist anhand folgenden Inhalts feststellbar:
  '*web.threema.ch/#!/messenger/conversation/contact/**Y***'
  Dabei steht das **Y** als Variable für die jeweilige Threema-ID (in diesem Falle Y3OMKEQV).
- Die Threema-Nutzer-ID des Chatpartners kann teilweise anhand des Schlüsselbegriffs `partnerId` festgestellt werden.
- Teilweise werden vor oder nach der Übertragung von Nachrichten Zeitstempel (Bsp.: `25. Jun. 2023, 16:26`) angefügt. Dies geschieht nicht bei jeder Nachricht.

4.1.2 Instagram

Die Analyse der RAM-Dumps `BA1_RAM_g_IG`, `BA1_RAM_e_IG` und `BA1_RAM_m_IG` durch den HxD-Editor ergaben unterschiedliche Feststellungen. Diese werden im Folgenden für jeden Internetbrowser auszugsweise durch Bildschirmaufnahmen von Ausschnitten aus den jeweiligen RAM-Dumps und weitere Inhalte in Form von Tabellen veranschaulicht..

Google Chrome

Die Analyse der RAM-Dump-Datei `BA1_RAM_g_IG.dmp` ergab folgende Feststellungen:
In der Abbildung 4.4 ist ein Auszug aus dem RAM-Dump des Testdurchlaufs mit dem Internetbrowser Google Chrome abgedruckt. In diesem Auszug wurde die vollständige Nachricht 2 (siehe Tabelle 3.1) festgestellt.

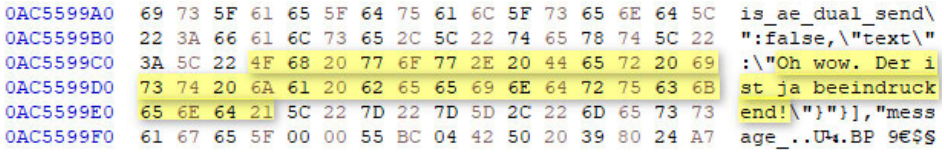

Abbildung 4.4: Vollständige Nachricht im Google Chrome RAM-Dump

Anhand der Tabellen 4.7 und 4.8 ist ersichtlich, ob die vorab definierten Nachrichten, Bilddateien und Nutzerdaten (siehe Tabellen 3.1 und 3.5) in dem RAM-Dump teils oder vollständig vorhanden und möglicherweise rekonstruierbar sind.

Suchbegriff	Feststellbar	10 Hex-Werte vor	10 Hex-Werte nach
Instagram	Vollständig vorhanden (31090 Treffer)	74 70 73 3A 2F 2F 77 77 77 2E	2E 63 6F 6D 00 76 61 72 79 3A
Nutzername lokaler Nutzer	Vollständig vorhanden (65 Treffer)	00 00 03 00 00 00 11 00 00 00	00 00 00 9D 05 00 00 03 00 00
Nutzername Chatpartner	Vollständig vorhanden (35 Treffer)	72 6E 61 6D 65 5C 22 3A 5C 22	5C 22 2C 5C 22 66 75 6C 6C 5F
Nutzer-ID lokaler Nutzer	Vollständig vorhanden (31 Treffer)	00 00 28 7E FE BD 0B 00 00 00	00 99 44 1A 00 08 00 00 00 E1
Nutzer-ID Chatpartner	Vollständig vorhanden (2 Treffer)	22 75 73 65 72 5F 69 64 22 3A	2C 22 74 69 6D 65 73 74 61 6D
Textnachricht 1	Vollständig vorhanden (15 Treffer)	00 00 3D 00 00 00 01 00 00 00	03 00 00 DF 00 00 00 FF 15 FE
Textnachricht 2	Vollständig vorhanden (4 Treffer)	22 74 65 78 74 5C 22 3A 5C 22	5C 22 7D 22 7D 5D 2C 22 6D 65
Textnachricht 6	Vollständig vorhanden (5 Treffer)	22 74 65 78 74 5C 22 3A 5C 22	5C 22 7D 22 7D 5D 2C 22 6D 65

Tabelle 4.7: Auszug der Ergebnisse BA1_RAM_g_IG.dmp Teil 1

Suchbegriff	Feststellbar	Beschreibung
Bilddatei 1 (durch lokalen Nutzer übertragen)	Hinweise feststellbar	Original-Pfad der Bilddatei 1 Bilddaten nicht rekonstruierbar
Bilddatei 2 (durch Chatpartner übertragen)	Hinweise auf gleich benannte Datei feststellbar	Link-Dateien Vollständiger Pfad des lokalen Nutzers (gleich benannte Datei)

Tabelle 4.8: Auszug der Ergebnisse BA1_RAM_g_IG.dmp Teil 2

Neben den in den Tabellen 4.7 und 4.8 aufgelisteten Feststellungen konnten Hinweise auf folgende Inhalte in dem RAM-Dump festgestellt werden:

- Nutzernamen und Nutzer-IDs können anhand der Schlüsselworte '`username`', '`full_name`' und '`user_id`' überprüft werden.
- Vollständige Textnachrichten können teilweise von folgenden Daten umschlossen sein: '`\"text\":\"`' und '`\"`' .

Microsoft Edge

In der Auswertung der RAM-Dump-Datei `BA1_RAM_g_IG.dmp` ergaben sich folgende Erkenntnisse: In der Abbildung 4.5 sind anhand eines Auszuges aus dem geprüften RAM-Dump festgestellte Nutzerinformationen abgedruckt.

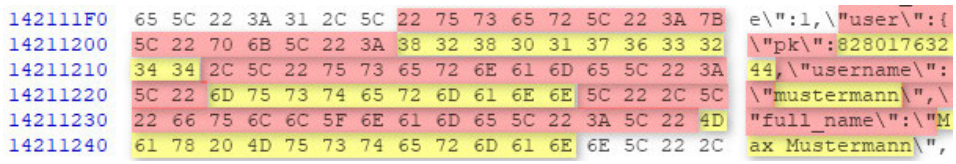

Abbildung 4.5: Instagram Nutzerdaten im Microsoft Edge RAM-Dump

Anhand der Tabellen 4.9 und 4.10 ist ersichtlich, ob die vorab definierten Nachrichten, Bilddateien und Nutzerdaten (Siehe Tabellen 3.1 und 3.5) in dem RAM-Dump teils oder vollständig vorhanden und möglicherweise rekonstruierbar sind.

Suchbegriff	Feststellbar	10 Hex-Werte vor	10 Hex-Werte nach
Instagram	Vollständig vorhanden (71033 Treffer)	00 00 11 00 00 00 77 77 77 2E	2E 63 6F 6D 00 76 61 72 79 3A
Nutzername lokaler Nutzer	Vollständig vorhanden (137 Treffer)	6E 61 6D 65 5C 22 3A 5C 22 61	2E 63 6F 6D 00 00 00 00 00 00
Nutzername Chatpartner	Vollständig vorhanden (35 Treffer)	72 6E 61 6D 65 5C 22 3A 5C 22	5C 22 2C 5C 22 66 75 6C 6C 5F
Nutzer-ID lokaler Nutzer	Vollständig vorhanden (1176 Treffer)	67 5F 75 73 65 72 69 64 22 3A	2C 22 70 6B 22 3A 35 36 38 39
Nutzer-ID Chatpartner	Vollständig vorhanden (79 Treffer)	22 75 73 65 72 5F 69 64 22 3A	2C 22 74 69 6D 65 73 74 61 6D
Textnachricht 1	Vollständig vorhanden (10 Treffer)	22 74 65 78 74 5C 22 3A 5C 22	5C 22 7D 22 7D 5D 2C 22 6D 65
Textnachricht 2	Vollständig vorhanden (3 Treffer)	22 74 65 78 74 5C 22 3A 5C 22	5C 22 7D 22 7D 5D 2C 22 6D 65
Textnachricht 6	Vollständig vorhanden (4 Treffer)	22 74 65 78 74 5C 22 3A 5C 22	5C 22 7D 22 7D 5D 2C 22 6D 65

Tabelle 4.9: Auszug der Ergebnisse BA1_RAM_e_IG.dmp Teil 1

Suchbegriff	Feststellbar	Beschreibung
Bilddatei 1 (durch lokalen Nutzer übertragen)	Hinweise feststellbar	Original-Pfad der Bilddatei 1 Bilddaten nicht rekonstruierbar
Bilddatei 2 (durch Chatpartner übertragen)	Hinweise auf gleich benannte Datei feststellbar	Link-Dateien Vollständiger Pfad des lokalen Nutzers (gleich benannte Datei)

Tabelle 4.10: Auszug der Ergebnisse BA1_RAM_e_IG.dmp Teil 2

Neben den in den Tabellen 4.9 und 4.10 aufgelisteten Feststellungen konnten Hinweise auf folgende Inhalte in dem RAM-Dump festgestellt werden:

- Nutzernamen und Nutzer-IDs können anhand der Schlüsselworte '`username`', '`full_name`' und '`ig_userid`' überprüft werden.
- Vollständige Textnachrichten können teilweise von folgenden Daten umschlossen sein: '`\"text\":\"`' und '`\"`' (siehe Abbildung 4.5 - rote Markierungen).

Mozilla Firefox

Es wurden folgende Feststellungen gemacht, während die RAM-Dump-Datei `BA1_RAM_g_IG.dmp` analysiert wurde:
In der Abbildung 4.6 ist ein Auszug aus dem RAM-Dump des Testdurchlaufs mit dem Internetbrowser Mozilla Firefox abgedruckt. In diesem Auszug wurde die vollständige Nachricht 2 (siehe Tabelle 3.1) festgestellt.

```
0B4D21F20  2C 5C 22 69 73 5F 61 65 5F 64 75 61 6C 5F 73 65  ,\"is_ae_dual_se
0B4D21F30  6E 64 5C 22 3A 66 61 6C 73 65 2C 5C 22 74 65 78  nd\":false,\"tex
0B4D21F40  74 5C 22 3A 5C 22 53 63 68 61 75 20 64 69 72 20  t\":\"Schau dir
0B4D21F50  75 6E 62 65 64 69 6E 67 74 20 6D 61 6C 20 64 69  unbedingt mal di
0B4D21F60  65 20 41 75 66 6E 61 68 6D 65 6E 20 76 6F 6E 20  e Aufnahmen von
0B4D21F70  64 65 6D 20 48 75 6E 64 65 77 65 6C 70 65 6E 20  dem Hundewelpen
0B4D21F80  61 6E 21 5C 22 7D 22 7D 5D 2C 22 6D 65 73 73 61  an!\"}"}],"messa
0B4D21F90  67 65 5F 74 79 70 65 22 3A 31 2C 22 73 65 71 5F  ge_type":1,"seq_
```

Abbildung 4.6: Vollständige Nachricht im Mozilla Firefox RAM-Dump

Anhand der Tabellen 4.11 und 4.12 ist ersichtlich, ob die vorab definierten Nachrichten, Bilddateien und Nutzerdaten (siehe Tabellen 3.1 und 3.5) in dem RAM-Dump teils oder vollständig vorhanden und möglicherweise rekonstruierbar sind.

Suchbegriff	Feststellbar	10 Hex-Werte vor	10 Hex-Werte nach
Instagram	Vollständig vorhanden (16670 Treffer)	74 70 73 3A 2F 2F 77 77 77 2E	2E 63 6F 6D 2F 64 69 72 65 63
Nutzername lokaler Nutzer	Vollständig vorhanden (37 Treffer)	72 6E 61 6D 65 5C 22 3A 5C 22	5C 22 2C 5C 22 62 61 64 67 65
Nutzername Chatpartner	Vollständig vorhanden (56 Treffer)	72 6E 61 6D 65 5C 22 3A 5C 22	5C 22 2C 5C 22 66 75 6C 6C 5F
Nutzer-ID lokaler Nutzer	Vollständig vorhanden (700 Treffer)	73 5F 75 73 65 72 5F 69 64 3D	3B 20 44 6F 6D 61 69 6E 3D 2E
Nutzer-ID Chatpartner	Vollständig vorhanden (53 Treffer)	75 73 65 72 5F 69 64 5C 22 3A	2C 5C 22 74 69 6D 65 73 74 61
Textnachricht 1	Vollständig vorhanden (4 Treffer)	22 74 65 78 74 5C 22 3A 5C 22	5C 22 7D 22 7D 5D 2C 22 6D 65
Textnachricht 2	Vollständig vorhanden (2 Treffer)	22 74 65 78 74 5C 22 3A 5C 22	5C 22 7D 22 7D 5D 2C 22 6D 65
Textnachricht 6	Vollständig vorhanden (5 Treffer)	22 74 65 78 74 5C 22 3A 5C 22	5C 22 7D 22 7D 5D 2C 22 6D 65

Tabelle 4.11: Auszug der Ergebnisse BA1_RAM_m_IG.dmp Teil 1

Suchbegriff	Feststellbar	Beschreibung
Bilddatei 1 (durch lokalen Nutzer übertragen)	Hinweise feststellbar	Original-Pfad der Bilddatei 1 Bilddaten nicht rekonstruierbar
Bilddatei 2 (durch Chatpartner übertragen)	Hinweise auf gleich benannte Datei feststellbar	Link-Dateien Vollständiger Pfad des lokalen Nutzers (gleich benannte Datei)

Tabelle 4.12: Auszug der Ergebnisse BA1_RAM_m_IG.dmp Teil 2

Neben den in den Tabellen 4.11 und 4.12 aufgelisteten Feststellungen konnten Hinweise auf folgende Inhalte in dem RAM-Dump festgestellt werden:

- Nutzernamen und Nutzer-IDs können anhand der Schlüsselworte '`username`', '`full_name`' und '`ds_user_id=`' überprüft werden.
- Vollständige Textnachrichten können teilweise von folgenden Daten umschlossen sein: '`\"text\":\"`' und '`\"`'.

4.2 Szenario 2: Sicherung bei beendetem Browser

Im Folgenden werden die Inhalte der für Szenario 2 erstellten RAM-Dumps analysiert. Hierbei werden die jeweiligen Feststellungen pro RAM-Dump, in Anwendung und Internetbrowser aufgeteilt, aufgelistet und beschrieben. Suchbegriffe, die keine Treffer ergaben, werden in den Tabellen, die lediglich Auszüge der Ergebnisse enthalten, ausgeblendet.

4.2.1 Threema

Die Analyse der RAM-Dumps `BA2_RAM_g_T`, `BA2_RAM_e_T` und `BA2_RAM_m_T` mittels des HxD-Editors ergaben unterschiedliche Feststellungen. Im Folgenden werden für jeden Internetbrowser Feststellungen auszugsweise durch Bildschirmaufnahmen von Ausschnitten aus den jeweiligen RAM-Dumps und weitere Inhalte mit Hilfe von Tabellen abgedruckt.

Google Chrome

Die Analyse der RAM-Dump-Datei `BA2_RAM_g_T.dmp` ergab folgende Feststellungen:
In dem in Abbildung 4.7 abgedruckten Auszug ist die im RAM-Dump vollständig festgestellte Threema-Nutzer-ID des Chatpartners zu sehen.

```
DF1EC8D0  00 00 00 00 00 00 00 00 00 00 02 00 00 00 41 00  ..............A.
DF1EC8E0  00 00 68 74 74 70 73 3A 2F 2F 77 65 62 2E 74 68  ..https://web.th
DF1EC8A0  72 65 65 6D 61 2E 63 68 2F 23 21 2F 6D 65 73 73  reema.ch/#!/mess
DF1EC8B0  65 6E 67 65 72 2F 63 6F 6E 76 65 72 73 61 74 69  enger/conversati
DF1EC8C0  6F 6E 2F 63 6F 6E 74 61 63 74 2F 59 33 4F 4D 4B  on/contact/Y3OMK
DF1EC8D0  45 51 56 00 00 00 00 00 00 00 02 7F E1 0E 8B 5D  EQV.........á.<]
DF1EC8E0  2F 00 00 00 00 00 C8 00 00 00 03 00 00 00 00 00  /.....È.........
```

Abbildung 4.7: Threema Chatpartner-ID im Google Chrome RAM-Dump

Anhand der Tabelle 4.13 ist ersichtlich, ob die vorab definierten Nutzerdaten (siehe Tabelle 3.6) in dem RAM-Dump teils oder vollständig vorhanden und möglicherweise rekonstruierbar sind.

Suchbegriff	Feststellbar	10 Hex-Werte vor	10 Hex-Werte nach
Threema	Vollständig vorhanden (2108 Treffer)	2F 70 75 73 68 2D 77 65 62 2E	2E 63 68 20 68 74 74 70 73 3A
Threema ID lokaler Nutzer	Vollständig vorhanden (34 Treffer)	73 61 74 69 6F 6E 2F 6D 65 2F	2F 64 65 74 61 69 6C 07 27 03
Threema ID Chatpartner	Vollständig vorhanden (78 Treffer)	6E 2F 63 6F 6E 74 61 63 74 2F	00 00 00 0B 00 00 00 54 00 68

Tabelle 4.13: Auszug der Ergebnisse BA2_RAM_g_T.dmp

Es konnten keine vollständigen Textnachrichten festgestellt werden. Auch wurden zu den übertragenen Bildinhalten nur Hinweise auf den Original-Pfad der Bilddatei 1 gefunden.

Neben der in der Tabelle 4.13 aufgelisteten Feststellungen konnten Hinweise auf folgende Inhalte in dem RAM-Dump festgestellt werden:

- Die Threema-Nutzer-ID des lokalen Nutzers ist anhand folgenden Inhalts feststellbar:
  '*web.threema.ch/#!/messenger/conversation/me/**X**'
  Dabei steht das **X** als Variable für die jeweilige Threema-ID (in diesem Falle UGM3OY7Q).
- Die Threema-Nutzer-ID des Chatpartners ist anhand folgenden Inhalts feststellbar:
  '*web.threema.ch/#!/messenger/conversation/contact/**Y**'
  Dabei steht das **Y** als Variable für die jeweilige Threema-ID (in diesem Falle Y3OMKEQV).

Microsoft Edge

Eine Analyse der RAM-Dump-Datei `BA2_RAM_e_T.dmp` ließ folgende Erkentnisse zu:
In dem in Abbildung 4.8 abgedruckten Auszug ist die im RAM-Dump vollständig festgestellte, vordefinierte Nachricht 6 zu sehen.

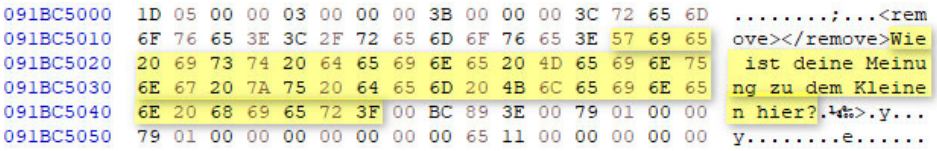

Abbildung 4.8: Threema Nachricht 6 im Microsoft Edge RAM-Dump

Anhand der Tabellen 4.14 und 4.15 ist ersichtlich, ob die vorab definierten Nachrichten und Bilddateien (siehe Tabelle 3.1) in dem RAM-Dump teilweise oder vollständig vorhanden und möglicherweise rekonstruierbar sind.
Auch wird geprüft, ob zusätzliche Informationen, wie z.B. Nutzerdaten oder Zeitstempel feststellbar sind (siehe Tabelle 3.6).

Suchbegriff	Feststellbar	10 Hex-Werte vor	10 Hex-Werte nach
Threema	Vollständig vorhanden (141 Treffer)	20 22 6E 61 6D 65 22 3A 20 22	20 57 65 62 22 2C 0D 0A 20 20
Threema ID Chatpartner	Vollständig vorhanden (71 Treffer)	6E 2F 63 6F 6E 74 61 63 74 2F	00 00 00 00 00 00 00 10 00 00
Textnachricht 1	Vollständig vorhanden (1 Treffer)	3A 00 03 00 00 00 3D 00 00 00	00 00 00 51 01 00 00 22 00 00
Textnachricht 6	Vollständig vorhanden (2 Treffer)	3E 3C 2F 72 65 6D 6F 76 65 3E	00 BC 89 3E 00 79 01 00 00 79

Tabelle 4.14: Auszug der Ergebnisse BA2_RAM_e_T.dmp Teil 1

Suchbegriff	Feststellbar	Beschreibung
Bilddatei 1 (durch lokalen Nutzer übertragen)	Hinweise feststellbar	Original-Pfad der Bilddatei 1 Bilddaten nicht rekonstruierbar

Tabelle 4.15: Auszug der Ergebnisse BA2_RAM_e_T.dmp Teil 2

Neben den in den Tabellen 4.14 und 4.15 aufgelisteten Feststellungen konnten Hinweise auf folgende Inhalte in dem RAM-Dump festgestellt werden:

- Die Threema-Nutzer-ID des Chatpartners ist anhand folgenden Inhalts feststellbar:
  '*web.threema.ch/#!/messenger/conversation/contact/**X***'
  Dabei steht das **X** als Variable für die jeweilige Threema-ID (in diesem Falle Y3OMKEQV).

Mozilla Firefox

Bei der Analyse der RAM-Dump-Datei `BA2_RAM_m_T.dmp` wurden folgende Feststellungen getroffen: In dem in Abbildung 4.9 abgedruckten Auszug ist die im RAM-Dump vollständig festgestellte Threema-Nutzer-ID des lokalen Nutzers zu sehen.

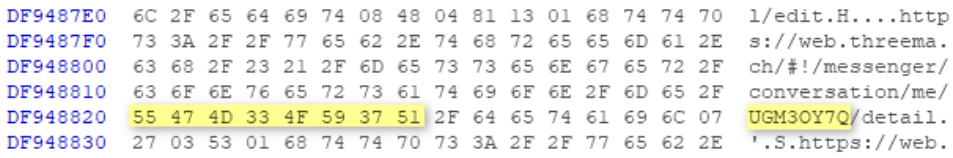

Abbildung 4.9: Threema-ID des lokalen Nutzers im Mozilla Firefox RAM-Dump

Anhand der Tabelle 4.16 ist ersichtlich, ob die vorab definierten Nutzerdaten (siehe Tabelle 3.6) in dem RAM-Dump teils oder vollständig vorhanden und möglicherweise rekonstruierbar sind.

Suchbegriff	Feststellbar	10 Hex-Werte vor	10 Hex-Werte nach
Threema	Vollständig vorhanden (36 Treffer)	20 22 6E 61 6D 65 22 3A 20 22	20 57 65 62 22 2C 0D 0A 20 20
Threema ID lokaler Nutzer	Vollständig vorhanden (12 Treffer)	73 61 74 69 6F 6E 2F 6D 65 2F	2F 64 65 74 61 69 6C 77 65 62
Threema ID Chatpartner	Vollständig vorhanden (87 Treffer)	6E 2F 63 6F 6E 74 61 63 74 2F	BF BF BF 80 07 79 72 DB 01 00

Tabelle 4.16: Auszug der Ergebnisse BA2_RAM_m_T.dmp

Es konnten keine vollständigen Textnachrichten festgestellt werden. Auch wurden zu den übertragenen Bildinhalten nur Hinweise auf den Original-Pfad der Bilddatei 1 gefunden.

Neben der in der Tabelle 4.16 aufgelisteten Feststellungen konnten Hinweise auf folgende Inhalte in dem RAM-Dump festgestellt werden:

- Die Threema-Nutzer-ID des lokalen Nutzers ist anhand folgenden Inhalts feststellbar:
  '*web.threema.ch/#!/messenger/conversation/me/**X***'
  Dabei steht das **X** als Variable für die jeweilige Threema-ID (in diesem Falle UGM3OY7Q).
- Die Threema-Nutzer-ID des Chatpartners ist anhand folgenden Inhalts feststellbar:
  '*web.threema.ch/#!/messenger/conversation/contact/**Y***'
  Dabei steht das **Y** als Variable für die jeweilige Threema-ID (in diesem Falle Y3OMKEQV).

4.2.2 Instagram

Im Verlauf der Analyse der RAM-Dumps `BA2_RAM_g_IG`, `BA2_RAM_e_IG` und `BA2_RAM_m_IG` wurden unterschiedliche Feststellungen erziehlt. Im Folgenden werden für jeden Internetbrowser Feststellungen auszugsweise durch Bildschirmaufnahmen von Ausschnitten aus den jeweiligen RAM-Dumps und weitere Inhalte mit Hilfe von Tabellen abgedruckt.

Google Chrome

Die Analyse der RAM-Dump-Datei `BA2_RAM_g_IG.dmp` ergab folgende Feststellungen:
In dem in Abbildung 4.10 abgedruckten Auszug ist die im RAM-Dump vollständig festgestellte Instagram-Nutzer-ID des lokalen Nutzers zu sehen.

```
33AB47A0  22 72 65 74 72 79 22 3A 66 61 6C 73 65 2C 22 73  "retry":false,"s
33AB47B0  74 61 74 75 73 22 3A 30 2C 22 75 73 65 72 49 44  tatus":0,"userID
33AB47C0  22 3A 22 38 32 38 30 31 37 36 33 32 34 34 22 7D  ":"82801763244"}
33AB47D0  5D 5D 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ]].............
```

Abbildung 4.10: Instagram-ID des lokalen Nutzers im Google Chrome RAM-Dump

Anhand der Tabelle 4.17 ist ersichtlich, ob die vorab definierten Nachrichten, Bilddateien und Nutzerdaten (siehe Tabellen 3.1 und 3.5) in dem RAM-Dump teils oder vollständig vorhanden und möglicherweise rekonstruierbar sind.

Suchbegriff	Feststellbar	10 Hex-Werte vor	10 Hex-Werte nach
Instagram	Vollständig vorhanden (203 Treffer)	6D 2E 61 6E 64 72 6F 69 64 05	0D 0F C8 00 03 0F B8 00 0F B8
Nutzername lokaler Nutzer	Vollständig vorhanden (25 Treffer)	75 73 65 72 6E 61 6D 65 22 11	22 07 77 65 62 73 69 74 65 22
Nutzer-ID lokaler Nutzer	Vollständig vorhanden (82 Treffer)	22 75 73 65 72 49 64 22 3A 22	22 7D D8 41 0D 97 45 6F FA F4

Tabelle 4.17: Auszug der Ergebnisse BA2_RAM_g_IG.dmp

Es konnten keine vollständigen Textnachrichten und Hinweise auf übertragene Bildinhalte oder Dateien festgestellt werden.

Neben der in der Tabelle 4.17 aufgelisteten Feststellungen konnten Hinweise auf folgende Inhalte in dem RAM-Dump festgestellt werden:

- Nutzer-IDs können anhand des Schlüsselworts '`user_id`' überprüft werden.

Microsoft Edge

Die Analyse der RAM-Dump-Datei `BA2_RAM_e_IG.dmp` ergab folgende Feststellungen:
In dem in Abbildung 4.11 abgedruckten Auszug ist die im RAM-Dump festgestellte Nachricht 4 zu sehen.

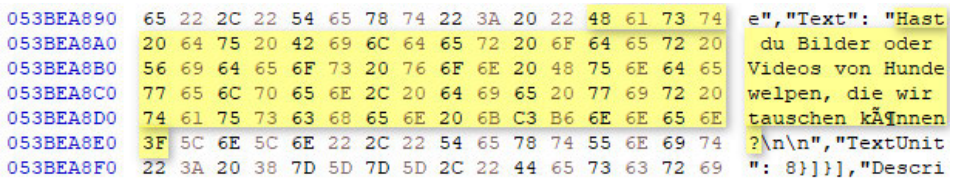

Abbildung 4.11: Nachricht 4 im Microsoft Edge RAM-Dump

Anhand der Tabelle 4.18 ist ersichtlich, ob die vorab definierten Nachrichten, Bilddateien und Nutzerdaten (siehe Tabellen 3.1 und 3.5) in dem RAM-Dump teils oder vollständig vorhanden und möglicherweise rekonstruierbar sind.

Suchbegriff	Feststellbar	10 Hex-Werte vor	10 Hex-Werte nach
Instagram	Vollständig vorhanden (399 Treffer)	61 67 72 61 6D 2E 63 6F 6D 2F	22 01 04 3B 01 19 68 74 74 70
Nutzername lokaler Nutzer	Vollständig vorhanden (16 Treffer)	75 73 65 72 6E 61 6D 65 22 11	22 07 77 65 62 73 69 74 65 22
Nutzer-ID lokaler Nutzer	Vollständig vorhanden (76 Treffer)	22 75 73 65 72 49 44 22 3A 22	22 7D 5D 2C 5B 22 6F 64 73 3A

Tabelle 4.18: Auszug der Ergebnisse BA2_RAM_e_IG.dmp

Es konnten keine vollständigen Textnachrichten und Hinweise auf übertragene Bildinhalte oder Dateien festgestellt werden.

Neben den in der Tabelle 4.18 aufgelisteten Feststellungen konnten Hinweise auf folgende Inhalte in dem RAM-Dump festgestellt werden:

- Nutzer-IDs können anhand des Schlüsselworts '`user_id`' überprüft werden.

Mozilla Firefox

Die Analyse der RAM-Dump-Datei `BA2_RAM_m_IG.dmp` ergab folgende Feststellungen:
In dem in Abbildung 4.12 abgedruckten Auszug ist die im RAM-Dump vollständig festgestellte Instagram-Nutzer-ID des Chatpartners zu sehen.

```
8B5BB7C0  31 31 36 2E 33 35 2C 22 65 78 74 72 61 22 3A 22  116.35,"extra":"
8B5BB7D0  7B 5C 22 69 67 5F 75 73 65 72 69 64 5C 22 3A 38  {\"ig_userid\":8
8B5BB7E0  32 38 30 31 37 36 33 32 34 34 2C 5C 22 70 6B 5C  2801763244,\"pk\
8B5BB7F0  22 3A 38 32 38 30 31 37 11 13 90 72 6F 6C 6C 6F  ":828017...rollo
```

Abbildung 4.12: Instagram-Nutzer-ID des lokalen Nutzers im Mozilla Firefox RAM-Dump

Anhand der Tabelle 4.19 ist ersichtlich, ob die vorab definierten Nachrichten, Bilddateien und Nutzerdaten (siehe Tabellen 3.1 und 3.5) in dem RAM-Dump teils oder vollständig vorhanden und möglicherweise rekonstruierbar sind.

Suchbegriff	Feststellbar	10 Hex-Werte vor	10 Hex-Werte nach
Instagram	Vollständig vorhanden (399 Treffer)	61 67 72 61 6D 2E 63 6F 6D 2F	22 01 04 3B 01 19 68 74 74 70
Nutzername lokaler Nutzer	Vollständig vorhanden (16 Treffer)	75 73 65 72 6E 61 6D 65 22 11	22 07 77 65 62 73 69 74 65 22
Nutzer-ID lokaler Nutzer	Vollständig vorhanden (76 Treffer)	22 75 73 65 72 49 44 22 3A 22	22 7D 5D 2C 5B 22 6F 64 73 3A

Tabelle 4.19: Auszug der Ergebnisse BA2_RAM_m_IG.dmp

Es konnten keine vollständigen Textnachrichten festgestellt werden. Auch wurden zu den übertragenen Bildinhalten nur Hinweise auf den Original-Pfad der Bilddatei 1 gefunden.

Neben den in der Tabelle 4.19 aufgelisteten Feststellungen konnten Hinweise auf folgende Inhalte in dem RAM-Dump festgestellt werden:

- Nutzer-IDs können anhand des Schlüsselworts ’`user_id`’ überprüft werden.

5 Ergebnisse

In diesem Kapitel werden die zuvor abgedruckten Ergebnisse der jeweiligen Anwendungen (Threema und Instagram), Internetbrowser (Google Chrome, Microsoft Edge und Mozilla Firefox) und Szenarien analysiert und miteinander verglichen.
Dabei werden Ansätze zur Analyse bzw. mögliche Identifikatoren relevanter Inhalte, sowie Auffälligkeiten betrachtet. Auch werden Gemeinsamkeiten und Unterschiede der Ergebnisse je Browser herausgearbeitet.
Anschließend wird ein Vergleich der Ergebnisse zwischen Threema und Instagram vorgenommen.

Hinweise:
In den Tabellen dieses Kapitels werden Symbole verwendet, um die Lesbarkeit bzw. Übersicht der Tabellen zu garantieren. Die Bedeutung der jeweiligen Symbole wird mittels der Tabelle 5.1 definiert.

Symbol	Bedeutung
✓	Vollständig feststellbar
✗	Nicht feststellbar
~	Hinweise feststellbar
/	Teilweise feststellbar (in Kombination mit anderen Symbolen nutzbar)

Tabelle 5.1: Symbol-Bedeutung

In den folgenden Unterkapiteln wird mehrfach auf unterschiedliche RAM-Dumps und die damit jeweils betroffenen Internetbrowser referenziert.
Um die Lesbarkeit der Texte sicherzustellen werden die jeweiligen RAM-Dumps innerhalb der einzelnen Kapitel durch eine Kombination der Abkürzungen der jeweiligen Anwendung und des Internetbrowsers bezeichnet. Eine Identifikation des jeweils verwendeten Szenarios wird durch die Zahlen 1 und 2 ermöglicht.
Die Bezeichnung der RAM-Dumps lautet beispielhaft wie folgt:

- **Tgc1**: Threema, Google Chrome, Szenario 1
- **Tme1**: Threema, Microsoft Edge, Szenario 1
- **Tmf1**: Threema, Mozilla Firefox, Szenario 1

- **IGgc2**: Instagram, Google Chrome, Szenario 2
- **IGme2**: Instagram, Microsoft Edge, Szenario 2
- **IGmf2**: Instagram, Mozilla Firefox, Szenario 2

5.1 Threema

Im Folgenden werden die Ergebnisse der Analyse der RAM-Dumps in Bezug auf die Anwendung Threema erläutert und mit den Resultaten der einzelnen Testdaten je Internetbrowser verglichen. Anfangs werden die Ergebnisse je Szenario (S1 und S2, siehe Kapitel 3.4) aufgezeigt und anschließend gegenübergestellt.

5.1.1 Szenario 1

Im Verlauf der Analyse der betroffenen RAM-Dumps für Szenario 1 fiel auf, dass unterschiedliche relevante Dateninhalte innerhalb der RAM-Dumps feststellbar sind. Eine vereinfachte Übersicht dieser Inhalte ist in Tabelle 5.2 abgedruckt.
Anhand der Tabelle ist zu erkennen, dass unabhängig vom Internetbrowser relevante Daten im RAM vorhanden sind, während der jeweilige Prozess betrieben wird.

	Google Chrome	**Microsoft Edge**	**Mozilla Firefox**
Nutzerdaten	✓	✓	✓
Kennwort	✓	✓	✓
Nachrichten	✓	✓	✓
Dateiübertragungen	/~	/~	/~

Tabelle 5.2: Threema Szenario 1 - Vergleich der Ergebnisse

Innerhalb des RAM-Dumps der in dieser Arbeit genutzten Internetbrowser konnte das zum Threema-Login verwendete Kennwort '`BA1_2023!`' ermittelt werden.
Dabei wiesen die Dumps **Tgc1** und **Tme1** Ähnlichkeiten bzw. identische Hex-Werte vor dem Kennwort auf (`01 43 2B 97` in ANSI `.C+-`). Eine Suche nach diesen Hex-Werten innerhalb der jeweiligen Dumps ergab keine Mehrfachtreffer.
Demzufolge könnte mithilfe der angegebenen Hex-Werte eine Suche nach möglichen Kennwörtern in RAM-Dumps mit Inhalten der Internetbrowser Google Chrome und Microsoft Edge durchgeführt werden.
Im Gegensatz dazu konnte im RAM-Dump **Tmf1** zwar das Kennwort aber kein möglicher Identifikator festgestellt werden.

Eine Suche nach den Threema-IDs des lokalen Nutzers und Chatpartners war in allen RAM-Dumps erfolgreich. Im Verlauf der Suche zeigte sich, dass in den RAM-Dumps **Tgc1** und **Tmf1** mögliche Identifikatoren für diese Nutzerdaten wie folgt lauten:

- Threema-ID des lokalen Nutzers: `/messenger/conversation/me/`
- Threema-ID des Chatpartners: `/messenger/conversation/contact/`

Dabei ist anzumerken, dass die Identifikation des Chatpartners mittels des oben genannten Identifikators auch im RAM-Dump **Tme1** anwendbar ist. Eine Suche nach der Threema-ID des lokalen Nutzers ließ hier jedoch keine Hinweise auf einen möglichen Identifikator zu.

Zwar konnten in jedem der RAM-Dumps die vorab definierten Nachrichten (siehe Tabelle 3.1) vollständig und teilweise mehrfach festgestellt werden, jedoch wiesen diese auch innerhalb der einzelnen Dumps keine eindeutigen Ähnlichkeiten vor oder nach den Nachrichteninhalten auf. Auch konnten nur teilweise bzw. zu wenigen der Nachrichten Informationen zu Übertragungszeiten oder anderen Eigenschaften aufgefunden werden. Entsprechend ist das Bezeichnen eines bestimmten Identifikators, anhand dessen die Suche nach ausgetauschten Nachrichten ermöglicht werden würde, nicht realisierbar.

Eine Suche nach den übertragenen Bilddateien ergab in jedem der RAM-Dumps zwar Treffer auf sogenannte LINK-Dateien[58] und den Ablageort der Bilddatei 1, jedoch konnte im Verlauf keine der Bilddateien rekonstruiert werden.

5.1.2 Szenario 2

Im Verlauf der Analyse der betroffenen RAM-Dumps für Szenario 2 wurden verschiedene relevante Dateninhalte nur in Teilen festgestellt. Eine vereinfachte Übersicht der festgestellten Inhalte ist in Tabelle 5.3 abgedruckt.
Anhand dieser Tabelle ist zu erkennen, dass nach Beenden des Internetbrowsers nur noch wenige Inhalte der Chatanwendung nachweisbar sind.

	Google Chrome	**Microsoft Edge**	**Mozilla Firefox**
Nutzerdaten	/✓	/✓	/✓
Kennwort	✗	✗	✗
Nachrichten	✗	/✓	✗
Dateiübertragungen	/~	/~	/~

Tabelle 5.3: Threema Szenario 2 - Vergleich der Ergebnisse

Während die Suche nach dem vordefinierten Kennwort und den Nachrichten für die RAM-Dumps **Tgc2** und **Tmf2** negativ verlief, konnten im Dump **Tme2** noch einige Nachrichten bzw. Fragmente dieser gefunden werden. Jedoch ließ sich hier kein Identifikator definieren.

Eine Suche nach den Threema-IDs des lokalen Nutzers und Chatpartners konnte in den RAM-Dumps **Tgc2** und **Tmf2** erfolgreich durchgeführt werden. Im RAM-Dump **Tme2** konnte die Threema-ID des lokalen Nutzers nicht aufgefunden werden.
Die Suche ergab, dass in den RAM-Dumps mögliche Identifikatoren für diese Nutzerdaten folgendermaßen lauten:

- Threema-ID des lokalen Nutzers: '`/messenger/conversation/me/`'
- Threema-ID des Chatpartners: '`/messenger/conversation/contact/`'

Die Suche nach den übertragenen Bilddateien führte in jedem der RAM-Dumps zu Treffern auf sogenannte LINK-Dateien und den Ablageort der Bilddatei 1. Während im Verlauf der Analyse keine Rekonstruktion der Bilddatei/en erfolgreich war.

[58] .lnk-Dateien dienen als Verlinkung und verweisen auf die Originaldatei im System

5.1.3 Vergleich der Ergebnisse

In der Tabelle 5.4 werden die Ergebnisse der Szenarien 1 und 2 der Anwendung Threema gegenübergestellt.
Dabei werden die Angaben, ob Daten feststellbar waren nach dem Prinzip des *OR-Logikgatters* eingetragen: (Wobei das Auffinden von Treffern '1' darstellt und das Nicht-Auffinden '0').[73]
Sollten sich die Ergebnisse innerhalb eines Szenarios zwischen den Internetbrowsern unterscheiden, sind entsprechende Zeilen mit einem * gekennzeichnet.

	Szenario 1	**Szenario 2**
Nutzerdaten	✓	/✓
Kennwort	✓	✗
Nachrichten	✓	/✓*
Dateiübertragungen	/~	/~

Tabelle 5.4: Threema - Vergleich der Ergebnisse beider Szenarien

Während in den in Szenario 1 erstellten RAM-Dumps unabhängig vom Internetbrowser alle geprüften Nutzerdaten, inklusive Kennwort und übertragener Nachrichten vollständig nachweisbar sind, konnten in den RAM-Dumps aus Szenario 2 Nutzerdaten nur teilweise und Nachrichten, wenn überhaupt, nur teilweise und/oder fragmentiert festgestellt werden. Sowohl in Szenario 1 als auch in Szenario 2 konnten zu den übertragenen Bilddateien nur Hinweise auf den Originalpfad der Bilddatei 1 gefunden werden.

Insgesamt konnten nicht uneingeschränkt Identifikatoren für die Suche nach Nutzerdaten definiert werden. Weder konnten Identifikatoren für ausgetauschte Nachrichten, noch Nachrichtendetails, wie Zeitstempel etc., innerhalb der RAM-Dumps gefunden werden.

5.2 Instagram

Es folgen die Ergebnisse der Analyse der RAM-Dumps im Hinblick auf die Anwendung Instagram, mit besonderem Augenmerk auf Auffälligkeiten und mögliche Identifikatoren. Zunächst werden die Ergebnisse je Szenario (S1 und S2) erläutert, gefolgt von einer Gegenüberstellung.

5.2.1 Szenario 1

Im Verlauf der Analyse der betroffenen RAM-Dumps für Szenario 1 konnte festgestellt werden, dass unterschiedliche relevante Dateninhalte innerhalb der RAM-Dumps feststellbar sind. Eine vereinfachte Übersicht der festgestellten Inhalte ist in Tabelle 5.5 abgedruckt.
Daraus geht hervor, dass während der Ausführung des Prozesses unabhängig vom Internetbrowser relevante Daten im RAM vorhanden sind.

	Google Chrome	Microsoft Edge	Mozilla Firefox
Nutzerdaten	✓	✓	✓
Nachrichten	✓	✓	✓
Dateiübertragungen	/~	/~	/~

Tabelle 5.5: Instagram Szenario 1 - Vergleich der Ergebnisse

Bei genauerer Betrachtung der Suchtreffer fällt auf, dass mittels unterschiedlicher Identifikatoren relevante Nutzerdaten und Nachrichteninhalte im RAM-Dump nachgewiesen werden können. Diese Identifikatoren sind:

- 'username' und 'full_name': Treffer zu Nutzernamen und Anzeigenamen
- 'user_id': Treffer zu Nutzer-ID (sowohl lokaler Nutzer, als auch Chatpartner)
- '\"text\":\"': Treffer auf ausgetauschte Nachrichten

Des Weiteren wurde festgestellt, dass die Übertragung von Nachrichten über den Webclient von Instagram durch das Versenden von sogenannten JSON-Dateien durchgeführt wird. Die Tabelle 5.6 enthält beispielhaft Auszüge aus einer JSON-Datei. Die vollständigen Inhalte sind im Anhang in Abbildung A.1 abgedruckt.

Identifikator	Wert
op	add
user_id	82801763244
timestamp	:1687624549804501,
item_type	text
text	Hast du Bilder oder Videos von Hundewelpen, die wir tauschen k\\u00f6nnen?

Tabelle 5.6: Auszug JSON-Datei

Anhand der in dieser Datei enthaltenen Informationen können neben der ID des Senders auch Zusatzinformationen, wie u. a. Zeitstempel und Nachrichtentyp, ausgewiesen werden.

5.2.2 Szenario 2

Im Verlauf der Analyse der betroffenen RAM-Dumps für Szenario 2 wurde deutlich, dass unterschiedliche relevante Dateninhalte lediglich teilweise innerhalb der RAM-Dumps gesichert werden konnten. Eine vereinfachte Übersicht darüber ist in Tabelle 5.7 abgedruckt.
Anhand dieser Tabelle ist zu erkennen, dass nach Beenden des Internetbrowsers keine Nachrichteninhalte und nur vereinzelt Nutzerdaten der Chatanwendung nachweisbar sind.

	Google Chrome	Microsoft Edge	Mozilla Firefox
Nutzerdaten	/✓	/✓	/✓
Nachrichten	✗	✗	✗
Dateiübertragungen	✗	✗	/~

Tabelle 5.7: Instagram Szenario 2 - Vergleich der Ergebnisse

Auch bei einer Erstellung eines RAM-Dumps nach Beenden des Internetbrowsers, in welchem der Instagram Webclient betrieben wurde, können sporadisch Nutzerinformationen, wie z. B. die Nutzer-ID anhand des Identifikators '`user_id`', ermittelt werden.

5.2.3 Vergleich der Ergebnisse

In der Tabelle 5.8 werden die Resultate der Szenarien 1 und 2 der Anwendung Instagram vergleichsweise beurteilt.
Dabei werden die Angaben, ob Daten feststellbar waren nach dem Prinzip des *OR-Logikgatters* eingetragen: (Wobei das Auffinden von Treffern '1' darstellt und das Nicht-Auffinden '0'). Sollten die Ergebnisse innerhalb der Szenarien sich pro Internetbrowser unterscheiden, sind entsprechende Zeilen mit einem * gekennzeichnet.

	Szenario 1	Szenario 2
Nutzerdaten	✓	/✓
Nachrichten	✓	✗
Dateiübertragungen	/~	~*

Tabelle 5.8: Threema - Vergleich der Ergebnisse beider Szenarien

Während die in Szenario 1 erstellten RAM-Dumps, unabhängig vom Internetbrowser, alle geprüften Nutzerdaten und übertragenen Nachrichten innerhalb von JSON-Dateien vollständig enthalten, konnten in den RAM-Dumps aus Szenario 2 nur lückenhaft Nutzerdaten festgestellt werden. In beiden Szenarien konnten zu den übertragenen Bilddateien nur Indizien für den Originalpfad der Bilddatei 1 gefunden werden.

Im Verlauf der Analyse der Testdaten zeigte sich, dass das Versenden von Nachrichten über den Webclient der Anwendung Instagram per JSON-Dateien erfolgt.
Diese JSON-Dateien weisen selbst weitere Informationen, wie eine ID der Nachricht auf, anhand welcher gegebenenfalls eine Rekonstruktion von Chatverläufen ermöglicht werden kann. Nach Beenden des Internetbrowsers, in welchem der Webclient ausgeführt wurde, sind im RAM-Dump wenige Informationen zugänglich.

5.3 Vergleich

Werden die obigen Ergebnisse vergleichend betrachtet, so können folgende Schlüsse gezogen werden:

Wird eine Sicherung des RAM durchgeführt während der Webclient von Threema oder Instagram mittels eines Internetbrowsers geöffnet ist, so können sowohl Nutzer- als auch teilweise Zugangsinformationen sowie vollständige Nachrichten innerhalb des RAM-Dumps festgestellt werden.
Der Webclient von Instagram führt die Übertragung der Nachrichten mittels JSON-Dateien durch. Somit sind Informationen, die eine Rekonstruktion von Chatverläufen unterstützen, nachweisbar. Innerhalb der versendeten JSON-Dateien werden regelmäßig Ausdrücke verwendet, die als Identifikatoren nutzbar sind und somit nicht nur die Suche nach Nutzerdaten, sondern auch nach Nachrichten und Zusatzinformationen zu diesen ermöglichen.

In RAM-Dumps, die Inhalte des Webclients von Threema enthalten, können zwar die Nachrichteninhalte, jedoch wenig bis keine Zusatzinformationen zu diesen ermittelt werden. Somit kann sich die Rekonstruktion der mittels Threema geführten Chatverläufe schwierig gestalten.

Auch die Verwendung von Identifikatoren gestaltet sich bei der Suche nach relevanten Inhalten in RAM-Dumps in Verbindung mit Threema schwierig, da im Verlauf der Analyse keine eindeutigen Identifikatoren für die Suche nach Nachrichteninhalten bekannt werden konnten.
Lediglich die Suche nach Nutzerinformationen, wie der Threema-ID oder zum Teil den Kennworten weist auf mögliche Identifikatoren hin, die den Nachweis dieser Inhalte vereinfachen können.

Wird eine Sicherung des RAM nach dem Beenden des Internetbrowsers durchgeführt, in welchem der jeweilige Webclient geöffnet war, so können unabhängig von Anwendung und Browser wenige bis keine Nachrichteninhalte und nur noch vereinzelte Nutzerdaten festgestellt werden. Ein Großteil der Daten der Webclients liegt in diesem Fall nicht mehr bzw. nur fragmentiert im RAM vor.

6 Fazit und Ausblick

In diesem Kapitel wird ein Fazit gezogen. Anschließend werden Limitierungen dieser Arbeit erläutert und ein Ausblick auf mögliche zukünftige Untersuchungen gegeben.

6.1 Fazit

Die Arbeit behandelt die Frage, ob Artefakte der Webclients von Threema und Instagram im RAM feststellbar sind und welche Informationen aus diesen gewonnen werden können.
Dabei lag der Fokus darauf, ob zu den gesicherten Artefakten der Nachrichtenübertragungen über die Webclients der jeweiligen Anwendungen Identifikatoren ableitbar sind, anhand welcher eine zukünftige Suche nach Artefakten vereinfacht und eine Rekonstruktion geführter Konversationen ermöglicht werden kann.
Die Arbeit beruht auf der Annahme, dass im Verlauf der letzten Nutzung des Computers der Webclient über Internetbrowser geöffnet und genutzt wurde.
Zur Überprüfung dieser, wurden vorbereitend die Grundkenntnisse in den Bereichen der Kommunikation über IM-Dienste und RAM geschaffen. Besondere Aufmerksamkeit galt dem Aufbau und der Funktionsweise des RAMs und dem Funktionsumfang sowie dem Kommunikationsprinzip der gewählten Anwendungen. Anhand der aus der Grundlagenforschung gezogenen Erkenntnisse wurde die Analyse der RAM-Dumps und die damit verbundene Untersuchung der Artefakte erleichtert.
Bei der Planung und Vorbereitung der Struktur konnten das Wissen und die Erkenntnisse aus vorab gelesenen Fremdliteraturen (siehe Kapitel 1.4) genutzt werden, um die Erhebung und Analyse der vordefinierten Testinhalte zu vereinfachen. Das Erstellen der Testdaten erfolgte über die Nutzung von VMs und jeweils zwei Nutzerkonten der gewählten Anwendungen.
Während der Aufbereitung der Testdaten fiel ein technisches Problem des ursprünglich geplanten Vorgehens auf, welches die Nutzung des forensischen Werkzeugs MemProcFS verhinderte. Das Verfahren wurde entsprechend angepasst, sodass eine Analyse möglich wurde und authentische Ergebnisse liefern konnte. Anschließend wurden die zwölf Datensicherungen forensisch aufbereitet, dokumentiert und die so erhaltenen Ergebnisse der jeweiligen Szenarien in Relation zueinander gesetzt.
Resultat der Arbeit ist, dass sowohl für den Webclient der Anwendung Threema, als auch für Instagram Artefakte im RAM feststellbar sind. Dabei hat der genutzte Internetbrowser keinen bis nur geringen Einfluss auf die Artefakte der Webclients. Problematisch in der forensischen Analyse gestaltet sich jedoch die Formatierung und teilweise vorhandene Fragmentierung der Inhalte. Zu den Artefakten der Webclients von Threema fehlen meist Zusatzinformationen, wie z. B. Zeitstempel. Hier erweist sich die Analyse der Artefakte des Webclients von Instagram als simpler, da die Nachrichten u. a. in JSON-Dateien innerhalb des RAMs feststellbar sind. Diese Dateien enthalten Zusatzinformationen, die für eine Rekonstruktion hilfreich und notwendig sind. Eine Rekonstruktion der geführten Konversationen ist somit für die Webclients der Anwendungen Threema und Instagram teils bis ganz möglich. Dateiübertragungen können nur bedingt nachgewiesen bzw. nachvollzogen werden. Eine Rekonstruktion der übertragenen Dateiinhalte ist nicht möglich. Insgesamt sind die Erfolgschancen, Konversationen vollständig und korrekt zu rekonstruieren, für den Webclient von Instagram deutlich höher, als für den Webclient von Threema.

Die aus dieser Arbeit gewonnenen Erkenntnisse sind unter Beachtung der im Folgenden erläuterten Limitierungen nutzbar, um zukünftige forensische Analysen im Bereich des RAM oder der jeweiligen Anwendungen zu erleichtern.
Es wird offenbar, dass insbesondere die Analyse des RAM großen Wert im Bereich der IT-Forensik aufweisen kann und Möglichkeiten sowie Vorgehensweisen zur Sicherung und Prüfung des RAM in der Zukunft genauer exploriert werden sollte.

6.2 Limitierungen und Ausblick

Diese Arbeit kann als ein Einblick in bzw. Ansatz für die forensische Auswertung von RAM-Dumps mit möglichen Nutzungsspuren der Anwendungen von Instagram und/oder Threema verwendet werden. Dennoch sind die durch die in dieser Arbeit gewählten Anwendungen und Vorgehensweisen entstandenen Limitierungen zu betonen. Sie können so in zukünftigen Arbeiten beachtet und durch abweichende Vorgehensweisen und Testumgebungen überprüft werden.

6.2.1 Stichwortsuche

In dieser Arbeit wurden sowohl Nachrichten, als auch Nutzerdaten vorab definiert und konnten dadurch mittels Volltextsuche überprüft werden. Zum einen kann dies teilweise nicht umgesetzt werden, da die Daten innerhalb vom RAM nicht pro Programm angereiht vorliegen, sondern meist fragmentiert innerhalb des Speichers verteilt sind. Zum anderen nutzen andere Anwendungen ebenfalls Kapazitäten des RAMs. Beide Aspekte wurden in dieser Arbeit nicht fokussiert behandelt weshalb bei der Erstellung der einzelnen Testdaten keine weiteren Programme durchgeführt wurden, die möglicherweise in realen Situationen verwendet werden könnten.

Eine Analyse mittels anderer forensischer Werkzeuge könnte die Fragmentierung partiell aufheben und die jeweiligen RAM-Inhalte der jeweiligen Anwendung bzw. des jeweiligen Prozesses zuteilen.
Zukünftige Arbeiten könnten zum einen die automatisierte Rekonstruktion von Chatinhalten des Webclients von Instagram behandeln. Zum anderen könnte geprüft werden, ob vorab nicht bekannte Inhalte anhand der in dieser Arbeit festgestellten Identifikatoren gefunden und reproduziert werden können.

6.2.2 Fokus auf RAM

Im Verlauf der Untersuchung wurde nur der RAM und die dem RAM zuzuordnenden Speicherbereiche beachtet. Es wurde vernachlässigt, dass durch das Verwenden von Webclients auch Artefakte in den einzelnen Datenbanken der jeweiligen Internetbrowser entstehen können. Diese könnten ebenfalls ausgewertet und mit den im RAM festgestellten Artefakten verglichen werden, sodass dadurch Ergebnisse ergänzt werden.

6.2.3 Dateiübertragungen

In dieser Arbeit konnten die für den Test erzeugten Dateiübertragungen nicht vollständig nachgewiesen und die übertragenen Daten nicht rekonstruiert werden. Dies war aufgrund des durch die jeweiligen Chatanwendungen verwendeten Kommunikationsprinzips (siehe Kapitel 2.3.2) zu erwarten. Die Verwendung anderer forensischer Werkzeuge könnte hier jedoch andere Ergebnisse liefern.

6.2.4 RAM-Größe

Den für diese Arbeit verwendeten VMs wurden jeweils 4GB RAM zugeteilt. Je nach Betriebssystem sind jedoch in einer vollständigen Analyse auch unterschiedliche Auslagerungsdateien, wie z. B. Hiberfil.sys und die Pagefile.sys (siehe Kapitel 2.6) vorhanden und möglicherweise relevant. Aufgrund der Tatsache, dass in den gewählten Szenarien keine größeren Datenmengen im RAM verarbeitet werden mussten, wurden die Auslagerungsdateien höchstwahrscheinlich auch nicht für relevante Artefakte verwendet.

6.2.5 Einschränkung der Gegebenheiten

Zu Beginn der Arbeit fiel die Entscheidung, für die Erstellung der Testdaten, das Betriebssystem Microsoft Windows 10 und die drei Internetbrowser Google Chrome, Microsoft Edge und Mozilla Firefox. Dabei wurden einerseits die Erkenntnisse aus der Bachelorarbeit *Analyse der Nutzungsspuren des Web Clients von WhatsApp und Telegram im Arbeitsspeicher* beachtet, dass unterschiedliche Betriebssysteme wenig bis keinen Einfluss auf die Artefakte der Webclients im RAM haben. Andererseits wurden die oben genannten Internetbrowser anhand von Nutzungsstatistiken gewählt.
Des Weiteren wurde in dieser Arbeit nicht beachtet, ob und in welchem Ausmaß die Desktopversionen der Anwendungen andere Artefakte im RAM hinterlassen als die Webclients.
Bei der Erstellung der Testdaten fand eine Beschränkung auf den Austausch von Textnachrichten und 2 Bilddateien statt. Somit wurden z. B. Sprachnachrichten und Telefonate vorerst nicht beachtet. Dieses Vorgehen wurde bewusst gewählt, um eine möglichst hohe Wahrscheinlichkeit für positive Ergebnisse bei der Suche nach den vordefinierten Inhalten zu erhalten. Die Übertragung anderer Nachrichtentypen wäre voraussichtlich zumindest teilweise in komprimierter Form im RAM vorhanden und hätte so nicht eindeutig identifiziert werden können.

6.2.6 Regelmäßige Updates

Die in dieser Arbeit durchgeführten Ergebnisse beruhen auf dem momentanen Entwicklungsstand der gewählten Internetbrowser (Google Chrome, Microsoft Edge und Mozilla Firefox) und der Anwendungen Threema und Instagram. Zukünftige Updates und Veränderungen u. a. an dem Kommunikationsprinzip, sind nicht absehbar. Mögliche Veränderungen an der geprüften Software können Einflüsse auf die Ausführlichkeit und das Vorhandensein von Artefakten im RAM haben.

6.2.7 Szenarien

In dieser Arbeit wurden zwei Szenarien analysiert, nach welchen eine Sicherung des RAM durchgeführt wurde. Weitere Szenarien, die ein realitätsnahes Geschehen nachstellen, könnten in weiteren Untersuchungen geprüft werden.

6.2.8 Nutzung von virtuellen Maschinen

Für die Erstellung der Testdaten wurden VMs genutzt. Dies könnte u. a. Einfluss auf die erhaltenen Ergebnisse genommen haben, da z. B. die Sicherung des RAM ohne direktes Ausführen einer forensischen Software innerhalb der VM durchgeführt wurde.

Anhang A: Tabellen

Vollständige Tabelle zu `BA1_RAM_g_T.dmp`:

Suchbegriff	Feststellbar	10 Hex-Werte vor	10 Hex-Werte nach
Threema	Vollständig vorhanden (8601 Treffer)	02 08 00 19 A9 B0 77 65 62 2E	2E 63 68 2F 69 6D 67 2F 66 61
Kennwort	Vollständig vorhanden (1 Treffer)	00 00 09 00 00 00 01 43 2B 97	72 69 70 74 00 00 00 00 00 00
Threema ID lokaler Nutzer	Vollständig vorhanden (46 Treffer)	73 61 74 69 6F 6E 2F 6D 65 2F	2F 64 65 74 61 69 6C 2F 65 64
Threema ID Chatpartner	Vollständig vorhanden (227 Treffer)	6E 2F 63 6F 6E 74 61 63 74 2F	2F 64 65 74 61 69 6C 00 69 73
Textnachricht 0	Vollständig vorhanden (32 Treffer)	F8 FF 3F 3F 00 B6 00 00 00 00	F7 60 01 00 00 18 00 00 00 00
Textnachricht 1	Vollständig vorhanden (8 Treffer)	00 00 3C 00 00 00 01 BC F4 EC	00 00 00 00 00 00 00 00 00 00
Textnachricht 2	Vollständig vorhanden (4 Treffer)	00 00 03 00 00 00 21 00 00 00	00 00 00 AD 09 00 00 58 00 00
Textnachricht 3	Vollständig vorhanden (5 Treffer)	00 00 26 00 00 00 01 63 22 5F	FF FF FF FF FF FF FF FF FF FF
Textnachricht 4	Vollständig vorhanden (3 Treffer)	00 00 03 00 00 00 44 00 00 00	9D 05 00 00 03 00 00 00 08 00
Textnachricht 5	Vollständig vorhanden (4 Treffer)	00 00 03 00 00 00 3A 00 00 00	00 00 99 44 1A 00 12 00 00 00
Textnachricht 6	Vollständig vorhanden (7 Treffer)	00 00 03 00 00 00 2A 00 00 00	00 00 D5 09 00 00 0C 00 00 00
Textnachricht 7	Vollständig vorhanden (12 Treffer)	00 00 03 00 00 00 27 00 00 00	00 AD 09 00 00 48 02 00 00 90
Textnachricht 8	Vollständig vorhanden (7 Treffer)	00 00 03 00 00 00 3E 00 00 00	00 00 9D 05 00 00 16 20 FA C8
Textnachricht 9	Vollständig vorhanden (15 Treffer)	00 00 03 00 00 00 31 00 00 00	00 00 00 39 71 19 00 19 02 00
Textnachricht 10	Vollständig vorhanden (12 Treffer)	00 00 03 00 00 00 23 00 00 00	00 9D 05 00 00 16 20 FA C8 08

Tabelle A.1: Ergebnisse BA1_RAM_g_T.dmp

Vollständige Tabelle zu `BA1_RAM_e_T.dmp`:

Suchbegriff	Feststellbar	10 Hex-Werte vor	10 Hex-Werte nach
Threema	Vollständig vorhanden (9455 Treffer)	74 70 73 3A 2F 2F 77 65 62 2E	2E 63 68 2F 23 21 2F 6D 65 73
Kennwort	Vollständig vorhanden (1 Treffer)	00 00 09 00 00 00 01 43 2B 97	00 00 00 00 00 00 00 00 00 00
Threema ID lokaler Nutzer	Vollständig vorhanden (1 Treffer)	00 00 22 9E CA D3 08 00 00 00	E9 01 00 00 20 00 00 00 9E FF
Threema ID Chatpartner	Vollständig vorhanden (258 Treffer)	6E 2F 63 6F 6E 74 61 63 74 2F	00 13 7A 6D 57 D2 E7 00 00 00
Textnachricht 0	Vollständig vorhanden (24 Treffer)	72 74 2F 72 65 6D 6F 76 65 3E	02 00 00 00 05 00 00 00 01 00
Textnachricht 1	Vollständig vorhanden (9 Treffer)	08 C8 00 71 25 E0 01 00 00 00	00 00 00 00 00 00 00 00 01 00
Textnachricht 2	Vollständig vorhanden (4 Treffer)	00 00 03 00 00 00 21 00 00 00	00 00 00 1D 05 00 00 8A DE 86
Textnachricht 3	Vollständig vorhanden (18 Treffer)	78 00 03 00 00 00 27 00 00 00	00 66 29 78 00 3C 00 00 00 00
Textnachricht 4	Vollständig vorhanden (11 Treffer)	00 00 44 00 00 00 01 00 00 00	E0 0E 26 00 C8 08 00 00 00 CA
Textnachricht 5	Vollständig vorhanden (4 Treffer)	00 00 03 00 00 00 39 00 00 00	00 00 00 45 72 19 00 79 01 00
Textnachricht 6	Vollständig vorhanden (5 Treffer)	00 00 03 00 00 00 2A 00 00 00	00 00 E9 01 00 00 40 00 00 00
Textnachricht 7	Vollständig vorhanden (12 Treffer)	00 00 03 00 00 00 26 00 00 00	00 00 1D 05 00 00 03 00 00 00
Textnachricht 8	Vollständig vorhanden (16 Treffer)	08 C8 00 70 CC 80 01 5F 48 8E	31 34 22 08 00 00 03 00 00 00
Textnachricht 9	Vollständig vorhanden (38 Treffer)	00 00 03 00 00 00 31 00 00 00	00 00 00 11 0C 00 00 06 00 00
Textnachricht 10	Vollständig vorhanden (27 Treffer)	CF FF 03 00 00 00 23 00 00 00	00 51 01 00 00 22 00 00 00 F9

Tabelle A.2: Ergebnisse BA1_RAM_e_T.dmp

Vollständige Tabelle zu `BA1_RAM_m_T.dmp`:

Suchbegriff	Feststellbar	10 Hex-Werte vor	10 Hex-Werte nach
Threema	Vollständig vorhanden (12218 Treffer)	74 70 73 3A 2F 2F 77 65 62 2E	2E 63 68 2F 23 21 2F 6D 65 73
Kennwort	Vollständig vorhanden (5 Treffer)	A1 A3 50 02 00 00 09 00 00 00	00 00 00 00 80 F8 FF 10 02 00
Threema ID lokaler Nutzer	Vollständig vorhanden (12 Treffer)	73 61 74 69 6F 6E 2F 6D 65 2F	2F 64 65 74 61 69 6C 2F 65 64
Threema ID Chatpartner	Vollständig vorhanden (480 Treffer)	6E 2F 63 6F 6E 74 61 63 74 2F	BF BF BF 80 D7 D0 C3 6B 02 00
Textnachricht 0	Vollständig vorhanden (30 Treffer)	FF FF 76 6B 00 00 4E 00 00 00	02 01 00 00 00 00 00 00 00 A8
Textnachricht 1	Vollständig vorhanden (2 Treffer)	E5 E5 E5 E5 E5 E5 E5 E5 E5 E5	E5 E5 E5 E5 C8 28 B2 FF 99 01
Textnachricht 2	Vollständig vorhanden (2 Treffer)	00 00 60 71 1F 02 9D 01 00 00	E5 E5 E5 E5 E5 E5 E5 E5 E5 E5
Textnachricht 3	Vollständig vorhanden (2 Treffer)	E5 E5 E5 E5 E5 E5 E5 E5 E5 E5	E5 E5 E5 E5 E5 E5 E5 E5 E5 E5
Textnachricht 4	Vollständig vorhanden (2 Treffer)	E5 E5 E5 E5 E5 E5 E5 E5 E5 E5	E5 E5 E5 E5 E5 E5 E5 E5 E5 E5
Textnachricht 5	Vollständig vorhanden (2 Treffer)	00 00 00 00 00 00 00 00 00 00	E5 E5 E5 E5 E5 E5 E0 01 00 00
Textnachricht 6	Vollständig vorhanden (3 Treffer)	E5 E5 E5 E5 E5 E5 E5 E5 E5 E5	E5 E5 E5 E5 E5 E5 E5 E5 E5 E5
Textnachricht 7	Vollständig vorhanden (4 Treffer)	E5 E5 E5 E5 E5 E5 E5 E5 E5 E5	E5 E5 E5 E5 E5 E5 E5 E5 E5 E5
Textnachricht 8	Vollständig vorhanden (12 Treffer)	75 73 C2 A4 62 6F 64 79 D9 3E	A9 70 61 72 74 6E 65 72 49 64
Textnachricht 9	Vollständig vorhanden (14 Treffer)	E5 E5 E5 E5 E5 E5 E5 E5 E5 E5	E5 E5 E5 E5 E5 E5 E5 E5 E5 E5
Textnachricht 10	Vollständig vorhanden (10 Treffer)	E5 E5 E5 E5 E5 E5 E5 E5 E5 E5	E5 E5 E5 E5 E5 E5 E5 E5 E5 E5

Tabelle A.3: Ergebnisse BA1_RAM_m_T.dmp

Vollständige Tabelle zu `BA1_RAM_e_IG.dmp`:

Suchbegriff	Feststellbar	10 Hex-Werte vor	10 Hex-Werte nach
Instagram	Vollständig vorhanden (31090 Treffer)	74 70 73 3A 2F 2F 77 77 77 2E	2E 63 6F 6D 00 76 61 72 79 3A
Nutzername lokaler Nutzer	Vollständig vorhanden (65 Treffer)	00 00 03 00 00 00 11 00 00 00	00 00 00 9D 05 00 00 03 00 00
Nutzername Chatpartner	Vollständig vorhanden (35 Treffer)	72 6E 61 6D 65 5C 22 3A 5C 22	5C 22 2C 5C 22 66 75 6C 6C 5F
Nutzer-ID lokaler Nutzer	Vollständig vorhanden (31 Treffer)	00 00 28 7E FE BD 0B 00 00 00	00 99 44 1A 00 08 00 00 00 E1
Nutzer-ID Chatpartner	Vollständig vorhanden (2 Treffer)	22 75 73 65 72 5F 69 64 22 3A	2C 22 74 69 6D 65 73 74 61 6D
Textnachricht 0	Vollständig vorhanden (69 Treffer)	04 80 01 00 00 00 00 00 00 00	98 01 D2 FF FF 60 04 D8 FA 79
Textnachricht 1	Vollständig vorhanden (15 Treffer)	00 00 3D 00 00 00 01 00 00 00	03 00 00 DF 00 00 00 FF 15 FE
Textnachricht 2	Vollständig vorhanden (4 Treffer)	22 74 65 78 74 5C 22 3A 5C 22	5C 22 7D 22 7D 5D 2C 22 6D 65
Textnachricht 3	Vollständig vorhanden (6 Treffer)	22 74 65 78 74 5C 22 3A 5C 22	5C 22 7D 22 7D 5D 2C 22 6D 65
Textnachricht 4	Vollständig vorhanden (2 Treffer)	00 00 44 00 00 00 01 00 00 00	14 00 00 00 E0 01 00 00 A4 01
Textnachricht 5	Vollständig vorhanden (3 Treffer)	22 74 65 78 74 5C 22 3A 5C 22	5C 5C 75 32 30 32 36 5C 22 7D
Textnachricht 6	Vollständig vorhanden (5 Treffer)	22 74 65 78 74 5C 22 3A 5C 22	5C 22 7D 22 7D 5D 2C 22 6D 65
Textnachricht 7	Vollständig vorhanden (6 Treffer)	22 74 65 78 74 5C 22 3A 5C 22	5C 5C 75 30 30 62 34 73 5C 22
Textnachricht 8	Vollständig vorhanden (5 Treffer)	22 74 65 78 74 5C 22 3A 5C 22	5C 22 7D 22 7D 5D 2C 22 6D 65
Textnachricht 9	Vollständig vorhanden (3 Treffer)	00 00 31 00 00 00 01 00 00 00	55 00 00 00 00 00 00 00 00 00
Textnachricht 10	Vollständig vorhanden (4 Treffer)	00 00 23 00 00 00 01 00 00 00	00 02 00 00 00 1F 00 00 00 05

Tabelle A.4: Ergebnisse BA1_RAM_g_IG.dmp

Vollständige Tabelle zu `BA1_RAM_e_IG.dmp`:

Suchbegriff	Feststellbar	10 Hex-Werte vor	10 Hex-Werte nach
Instagram	Vollständig vorhanden (71033 Treffer)	00 00 11 00 00 00 77 77 77 2E	2E 63 6F 6D 00 76 61 72 79 3A
Nutzername lokaler Nutzer	Vollständig vorhanden (137 Treffer)	6E 61 6D 65 5C 22 3A 5C 22 61	2E 63 6F 6D 00 00 00 00 00 00
Nutzername Chatpartner	Vollständig vorhanden (35 Treffer)	72 6E 61 6D 65 5C 22 3A 5C 22	5C 22 2C 5C 22 66 75 6C 6C 5F
Nutzer-ID lokaler Nutzer	Vollständig vorhanden (1176 Treffer)	67 5F 75 73 65 72 69 64 22 3A	2C 22 70 6B 22 3A 35 36 38 39
Nutzer-ID Chatpartner	Vollständig vorhanden (79 Treffer)	22 75 73 65 72 5F 69 64 22 3A	2C 22 74 69 6D 65 73 74 61 6D
Textnachricht 0	Vollständig vorhanden (26 Treffer)	04 00 01 66 0A 00 60 A6 00 00	5B 85 C2 FF FF 70 04 38 CD 4E
Textnachricht 1	Vollständig vorhanden (10 Treffer)	22 74 65 78 74 5C 22 3A 5C 22	5C 22 7D 22 7D 5D 2C 22 6D 65
Textnachricht 2	Vollständig vorhanden (3 Treffer)	22 74 65 78 74 5C 22 3A 5C 22	5C 22 7D 22 7D 5D 2C 22 6D 65
Textnachricht 3	Vollständig vorhanden (7 Treffer)	22 74 65 78 74 5C 22 3A 5C 22	5C 22 7D 22 7D 5D 2C 22 6D 65
Textnachricht 4	Vollständig vorhanden (2 Treffer)	00 00 44 00 00 00 01 00 00 00	35 00 00 00 44 04 00 00 EA 00
Textnachricht 5	Vollständig vorhanden (2 Treffer)	22 74 65 78 74 5C 22 3A 5C 22	5C 5C 75 32 30 32 36 5C 22 7D
Textnachricht 6	Vollständig vorhanden (4 Treffer)	22 74 65 78 74 5C 22 3A 5C 22	5C 22 7D 22 7D 5D 2C 22 6D 65
Textnachricht 7	Vollständig vorhanden (20 Treffer)	65 2C 22 74 65 78 74 22 3A 22	22 7D 00 00 00 E9 01 00 00 40
Textnachricht 8	Vollständig vorhanden (5 Treffer)	22 74 65 78 74 5C 22 3A 5C 22	5C 22 7D 22 7D 5D 2C 22 6D 65
Textnachricht 9	Vollständig vorhanden (3 Treffer)	12 30 08 4B 7B 00 01 00 00 00	00 00 00 00 00 12 30 08 4B 52
Textnachricht 10	Vollständig vorhanden (3 Treffer)	00 00 23 00 00 00 01 00 00 00	00 00 00 12 30 03 DD AA 90 00

Tabelle A.5: Ergebnisse BA1_RAM_e_IG.dmp

Vollständige Tabelle zu `BA1_RAM_e_IG.dmp`:

Suchbegriff	Feststellbar	10 Hex-Werte vor	10 Hex-Werte nach
Instagram	Vollständig vorhanden (16670 Treffer)	74 70 73 3A 2F 2F 77 77 77 2E	2E 63 6F 6D 2F 64 69 72 65 63
Nutzername lokaler Nutzer	Vollständig vorhanden (37 Treffer)	72 6E 61 6D 65 5C 22 3A 5C 22	5C 22 2C 5C 22 62 61 64 67 65
Nutzername Chatpartner	Vollständig vorhanden (56 Treffer)	72 6E 61 6D 65 5C 22 3A 5C 22	5C 22 2C 5C 22 66 75 6C 6C 5F
Nutzer-ID lokaler Nutzer	Vollständig vorhanden (700 Treffer)	73 5F 75 73 65 72 5F 69 64 3D	3B 20 44 6F 6D 61 69 6E 3D 2E
Nutzer-ID Chatpartner	Vollständig vorhanden (53 Treffer)	75 73 65 72 5F 69 64 5C 22 3A	2C 5C 22 74 69 6D 65 73 74 61
Textnachricht 0	Vollständig vorhanden (31 Treffer)	41 08 4A 21 21 42 82 0A 48 11	46 42 52 01 01 00 10 C5 01 00
Textnachricht 1	Vollständig vorhanden (4 Treffer)	22 74 65 78 74 5C 22 3A 5C 22	5C 22 7D 22 7D 5D 2C 22 6D 65
Textnachricht 2	Vollständig vorhanden (2 Treffer)	22 74 65 78 74 5C 22 3A 5C 22	5C 22 7D 22 7D 5D 2C 22 6D 65
Textnachricht 3	Vollständig vorhanden (4 Treffer)	22 74 65 78 74 5C 22 3A 5C 22	5C 22 7D 22 7D 5D 2C 22 6D 65
Textnachricht 4	Vollständig vorhanden (2 Treffer)	E5 E5 E5 E5 E5 E5 E5 E5 E5 E5	E5 E5 E5 E5 E5 E5 E5 E5 E5 E5
Textnachricht 5	Vollständig vorhanden (1 Treffer)	22 74 65 78 74 5C 22 3A 5C 22	5C 5C 75 32 30 32 36 5C 22 7D
Textnachricht 6	Vollständig vorhanden (5 Treffer)	22 74 65 78 74 5C 22 3A 5C 22	5C 22 7D 22 7D 5D 2C 22 6D 65
Textnachricht 7	Vollständig vorhanden (10 Treffer)	22 74 65 78 74 5C 22 3A 5C 22	5C 5C 75 30 30 62 34 73 5C 22
Textnachricht 8	Vollständig vorhanden (6 Treffer)	22 74 65 78 74 5C 22 3A 5C 22	5C 22 7D 22 7D 5D 2C 22 6D 65
Textnachricht 9	Vollständig vorhanden (7 Treffer)	00 00 00 00 00 00 00 00 00 00	E5 E5 E5 E5 E5 E5 E5 E5 E5 E5
Textnachricht 10	Vollständig vorhanden (3 Treffer)	00 00 E5 E5 E5 E5 E5 E5 E5 E5	E5 E5 E5 E5 E5 E5 E5 E5 E5 E5

Tabelle A.6: Ergebnisse BA1_RAM_m_IG.dmp

Vollständige Tabelle zu `BA2_RAM_g_T.dmp`**:**

Suchbegriff	Feststellbar	10 Hex-Werte vor	10 Hex-Werte nach
Threema	Vollständig vorhanden (2108 Treffer)	2F 70 75 73 68 2D 77 65 62 2E	2E 63 68 20 68 74 74 70 73 3A
Kennwort	nicht feststellbar	-	-
Threema ID lokaler Nutzer	Vollständig vorhanden (34 Treffer)	73 61 74 69 6F 6E 2F 6D 65 2F	2F 64 65 74 61 69 6C 07 27 03
Threema ID Chatpartner	Vollständig vorhanden (78 Treffer)	6E 2F 63 6F 6E 74 61 63 74 2F	00 00 00 0B 00 00 00 54 00 68
Textnachricht 0	nicht feststellbar	-	-
Textnachricht 1	nicht feststellbar	-	-
Textnachricht 2	nicht feststellbar	-	-
Textnachricht 3	nicht feststellbar	-	-
Textnachricht 4	nicht feststellbar	-	-
Textnachricht 5	nicht feststellbar	-	-
Textnachricht 6	nicht feststellbar	-	-
Textnachricht 7	nicht feststellbar	-	-
Textnachricht 8	nicht feststellbar	-	-
Textnachricht 9	nicht feststellbar	-	-
Textnachricht 10	nicht feststellbar	-	-

Tabelle A.7: Ergebnisse BA2_RAM_g_T.dmp

Vollständige Tabelle zu `BA2_RAM_e_T.dmp`**:**

Suchbegriff	Feststellbar	10 Hex-Werte vor	10 Hex-Werte nach
Threema	Vollständig vorhanden (141 Treffer)	20 22 6E 61 6D 65 22 3A 20 22	20 57 65 62 22 2C 0D 0A 20 20
Kennwort	nicht feststellbar	-	-
Threema ID lokaler Nutzer	nicht feststellbar	-	-
Threema ID Chatpartner	Vollständig vorhanden (71 Treffer)	6E 2F 63 6F 6E 74 61 63 74 2F	00 00 00 00 00 00 00 10 00 00
Textnachricht 0	Vollständig vorhanden (10 Treffer)	FF FF 76 6B 00 00 4E 00 00 00	02 01 00 00 00 00 00 00 00 A8
Textnachricht 1	Vollständig vorhanden (1 vollständiger Treffer 1 teil-Treffer)	3A 00 03 00 00 00 3D 00 00 00	00 00 00 51 01 00 00 22 00 00
Textnachricht 2	nicht feststellbar	-	-
Textnachricht 3	nicht feststellbar	-	-
Textnachricht 4	nicht feststellbar	-	-
Textnachricht 5	nicht feststellbar	-	-
Textnachricht 6	Vollständig vorhanden (2 Treffer)	3E 3C 2F 72 65 6D 6F 76 65 3E	00 BC 89 3E 00 79 01 00 00 79
Textnachricht 7	nicht feststellbar	-	-
Textnachricht 8	nicht feststellbar	-	-
Textnachricht 9	Vollständig vorhanden (12 Treffer)	3E 3C 2F 72 65 6D 6F 76 65 3E	00 00 02 D3 0F 00 79 01 00 00
Textnachricht 10	nicht feststellbar	-	-

Tabelle A.8: Ergebnisse BA2_RAM_e_T.dmp

Vollständige Tabelle zu `BA2_RAM_m_T.dmp`:

Suchbegriff	Feststellbar	10 Hex-Werte vor	10 Hex-Werte nach
Threema	Vollständig vorhanden (36 Treffer)	20 22 6E 61 6D 65 22 3A 20 22	20 57 65 62 22 2C 0D 0A 20 20
Kennwort	nicht feststellbar	-	-
Threema ID lokaler Nutzer	Vollständig vorhanden (12 Treffer)	73 61 74 69 6F 6E 2F 6D 65 2F	2F 64 65 74 61 69 6C 77 65 62
Threema ID Chatpartner	Vollständig vorhanden (87 Treffer)	6E 2F 63 6F 6E 74 61 63 74 2F	BF BF BF 80 07 79 72 DB 01 00
Textnachricht 0	Vollständig vorhanden (12 Treffer)	21 00 58 68 21 00 D0 68 21 00	00 C0 69 21 00 38 6A 21 00 B0
Textnachricht 1	nicht feststellbar	-	-
Textnachricht 2	nicht feststellbar	-	-
Textnachricht 3	nicht feststellbar	-	-
Textnachricht 4	nicht feststellbar	-	-
Textnachricht 5	nicht feststellbar	-	-
Textnachricht 6	nicht feststellbar	-	-
Textnachricht 7	nicht feststellbar	-	-
Textnachricht 8	nicht feststellbar	-	-
Textnachricht 9	nicht feststellbar	-	-
Textnachricht 10	nicht feststellbar	-	-

Tabelle A.9: Ergebnisse BA2_RAM_m_T.dmp

Vollständige Tabelle zu `BA2_RAM_g_IG.dmp`:

Suchbegriff	Feststellbar	10 Hex-Werte vor	10 Hex-Werte nach
Instagram	Vollständig vorhanden (203 Treffer)	6D 2E 61 6E 64 72 6F 69 64 05	0D 0F C8 00 03 0F B8 00 0F B8
Nutzername lokaler Nutzer	Vollständig vorhanden (25 Treffer)	75 73 65 72 6E 61 6D 65 22 11	22 07 77 65 62 73 69 74 65 22
Nutzername Chatpartner	nicht feststellbar	-	-
Nutzer-ID lokaler Nutzer	Vollständig vorhanden (82 Treffer)	22 75 73 65 72 49 64 22 3A 22	22 7D D8 41 0D 97 45 6F FA F4
Nutzer-ID Chatpartner	nicht feststellbar	-	-
Textnachricht 0	Vollständig vorhanden (15 Treffer)	0C 70 0B 50 00 00 10 0B 0F 00	00 A2 00 00 00 28 51 69 21 00
Textnachricht 1	nicht feststellbar	-	-
Textnachricht 2	nicht feststellbar	-	-
Textnachricht 3	nicht feststellbar	-	-
Textnachricht 4	nicht feststellbar	-	-
Textnachricht 5	nicht feststellbar	-	-
Textnachricht 6	nicht feststellbar	-	-
Textnachricht 7	nicht feststellbar	-	-
Textnachricht 8	nicht feststellbar	-	-
Textnachricht 9	nicht feststellbar	-	-
Textnachricht 10	nicht feststellbar	-	-

Tabelle A.10: Ergebnisse BA2_RAM_g_IG.dmp

Vollständige Tabelle zu `BA2_RAM_e_IG.dmp`:

Suchbegriff	Feststellbar	10 Hex-Werte vor	10 Hex-Werte nach
Instagram	Vollständig vorhanden (399 Treffer)	`61 67 72 61 6D 2E 63 6F 6D 2F`	`22 01 04 3B 01 19 68 74 74 70`
Nutzername lokaler Nutzer	Vollständig vorhanden (16 Treffer)	`75 73 65 72 6E 61 6D 65 22 11`	`22 07 77 65 62 73 69 74 65 22`
Nutzername Chatpartner	nicht feststellbar	-	-
Nutzer-ID lokaler Nutzer	Vollständig vorhanden (76 Treffer)	`22 75 73 65 72 49 44 22 3A 22`	`22 7D 5D 2C 5B 22 6F 64 73 3A`
Nutzer-ID Chatpartner	nicht feststellbar	-	-
Textnachricht 0	Vollständig vorhanden (13 Treffer)	`04 00 16 9B 02 00 B0 29 00 00`	`7B 00 8C FF FF D0 04 D0 51 1B`
Textnachricht 1	nicht feststellbar	-	-
Textnachricht 2	nicht feststellbar	-	-
Textnachricht 3	nicht feststellbar	-	-
Textnachricht 4	Teils vorhanden (1 Treffer)	`2C 22 54 65 78 74 22 3A 20 22`	`5C 6E 5C 6E 22 2C 22 54 65 78`
Textnachricht 5	nicht feststellbar	-	-
Textnachricht 6	nicht feststellbar	-	-
Textnachricht 7	nicht feststellbar	-	-
Textnachricht 8	nicht feststellbar	-	-
Textnachricht 9	nicht feststellbar	-	-
Textnachricht 10	nicht feststellbar	-	-

Tabelle A.11: Ergebnisse BA2_RAM_e_IG.dmp

Vollständige Tabelle zu `BA2_RAM_m_IG.dmp`:

Suchbegriff	Feststellbar	10 Hex-Werte vor	10 Hex-Werte nach
Instagram	Vollständig vorhanden (46 Treffer)	61 67 72 61 6D 2E 63 6F 6D 2F	00 30 02 04 4F 08 23 68 74 74
Nutzername lokaler Nutzer	nicht feststellbar	-	-
Nutzername Chatpartner	nicht feststellbar	-	-
Nutzer-ID lokaler Nutzer	Vollständig vorhanden (23 Treffer)	64 73 5F 75 73 65 72 5F 69 64	2E 69 6E 73 74 61 67 72 61 6D
Nutzer-ID Chatpartner	nicht feststellbar	-	-
Textnachricht 0	Vollständig vorhanden (22 Treffer)	17 12 5B 0B 19 14 18 11 1C 60	72 1C 14 0E 39 0F 1C 13 EE 18
Textnachricht 1	nicht feststellbar	-	-
Textnachricht 2	nicht feststellbar	-	-
Textnachricht 3	nicht feststellbar	-	-
Textnachricht 4	nicht feststellbar	-	-
Textnachricht 5	nicht feststellbar	-	-
Textnachricht 6	nicht feststellbar	-	-
Textnachricht 7	nicht feststellbar	-	-
Textnachricht 8	nicht feststellbar	-	-
Textnachricht 9	nicht feststellbar	-	-
Textnachricht 10	nicht feststellbar	-	-

Tabelle A.12: Ergebnisse BA2_RAM_m_IG.dmp

Vollständiger JSON-Inhalt aus `BA1_RAM_e_IG.dmp`:

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Dekodierter Text
AA457F60	22	3A	5B	7B	22	6F	70	22	3A	22	61	64	64	22	2C	22	":[{"op":"add","
AA457F70	70	61	74	68	22	3A	22	2F	64	69	72	65	63	74	5F	76	path":"/direct_v
AA457F80	32	2F	74	68	72	65	61	64	73	2F	33	34	30	32	38	32	2/threads/340282
AA457F90	33	36	36	38	34	31	37	31	30	33	30	30	39	34	39	31	3668417103009491
AA457FA0	32	38	35	32	33	34	34	33	38	34	36	34	34	37	31	30	2852344384644710
AA457FB0	37	2F	69	74	65	6D	73	2F	33	31	31	33	31	31	37	38	7/items/31131178
AA457FC0	31	36	32	37	35	32	39	32	38	38	35	36	39	38	37	36	1627529288569876
AA457FD0	32	39	31	36	38	36	32	33	36	31	36	22	2C	22	76	61	29168623616","va
AA457FE0	6C	75	65	22	3A	22	7B	5C	22	69	74	65	6D	5F	69	64	lue":"{\"item_id
AA457FF0	5C	22	3A	5C	22	33	31	31	33	31	31	37	38	31	36	32	\":\"31131178162
AA458000	37	35	32	39	32	38	38	35	36	39	38	37	36	32	39	31	7529288569876291
AA458010	36	38	36	32	33	36	31	36	5C	22	2C	5C	22	75	73	65	68623616\",\"use
AA458020	72	5F	69	64	5C	22	3A	38	32	38	30	31	37	36	33	32	r_id\":828017632
AA458030	34	34	2C	5C	22	74	69	6D	65	73	74	61	6D	70	5C	22	44,\"timestamp\"
AA458040	3A	31	36	38	37	36	32	34	35	34	39	38	30	34	35	30	:168762454980450
AA458050	31	2C	5C	22	69	74	65	6D	5F	74	79	70	65	5C	22	3A	1,\"item_type\":
AA458060	5C	22	74	65	78	74	5C	22	2C	5C	22	63	6C	69	65	6E	\"text\",\"clien
AA458070	74	5F	63	6F	6E	74	65	78	74	5C	22	3A	5C	22	37	30	t_context\":\"70
AA458080	37	38	34	30	39	34	33	35	38	36	35	36	31	30	35	30	7840943586561050
AA458090	31	5C	22	2C	5C	22	73	68	6F	77	5F	66	6F	72	77	61	1\",\"show_forwa
AA4580A0	72	64	5F	61	74	74	72	69	62	75	74	69	6F	6E	5C	22	rd_attribution\"
AA4580B0	3A	66	61	6C	73	65	2C	5C	22	66	6F	72	77	61	72	64	:false,\"forward
AA4580C0	5F	73	63	6F	72	65	5C	22	3A	6E	75	6C	6C	2C	5C	22	_score\":null,\"
AA4580D0	69	73	5F	73	68	68	5F	6D	6F	64	65	5C	22	3A	66	61	is_shh_mode\":fa
AA4580E0	6C	73	65	2C	5C	22	6F	74	69	64	5C	22	3A	5C	22	37	lse,\"otid\":\"7
AA4580F0	30	37	38	34	30	39	34	33	35	38	36	35	36	31	30	35	0784094358656105
AA458100	30	31	5C	22	2C	5C	22	69	73	5F	62	74	76	5F	73	65	01\",\"is_btv_se
AA458110	6E	64	5C	22	3A	66	61	6C	73	65	2C	5C	22	69	73	5F	nd\":false,\"is_
AA458120	61	65	5F	64	75	61	6C	5F	73	65	6E	64	5C	22	3A	66	ae_dual_send\":f
AA458130	61	6C	73	65	2C	5C	22	74	65	78	74	5C	22	3A	5C	22	alse,\"text\":\"
AA458140	48	61	73	74	20	64	75	20	42	69	6C	64	65	72	20	6F	Hast du Bilder o
AA458150	64	65	72	20	56	69	64	65	6F	73	20	76	6F	6E	20	48	der Videos von H
AA458160	75	6E	64	65	77	65	6C	70	65	6E	2C	20	64	69	65	20	undewelpen, die
AA458170	77	69	72	20	74	61	75	73	63	68	65	6E	20	6B	5C	5C	wir tauschen k\\
AA458180	75	30	30	66	36	6E	6E	65	6E	3F	5C	22	7D	22	7D	5D	u00f6nnen?\"}"}]

Abbildung A.1: Auszug RAM-Dump JSON-Datei

Literaturverzeichnis

[1] IT-Service-Network. „Instant Messenger | Definition & Erklärung“, IT-Service-Network. (2023), Adresse: https://it-service.network/it-lexikon/instant-messenger (besucht am 06. 05. 2023).

[2] L. Ceci. „Mobile messaging users worldwide 2025 | Statista“. eMarketer, Hrsg., Statista. (2022), Adresse: https://www.statista.com/statistics/483255/number-of-mobile-messaging-users-worldwide/ (besucht am 06. 05. 2023).

[3] S. Dixon. „Germany number of Instagram users 2022 | Statista“, Statista. (2022), Adresse: https://www.statista.com/statistics/1021975/instagram-users-germany/ (besucht am 06. 05. 2023).

[4] Statista. „Threema - Nutzer 2022 | Statista“, Statista. (2023), Adresse: https://de.statista.com/statistik/daten/studie/445619/umfrage/nutzer-des-schweizer-messaging-dienstes-threema/ (besucht am 06. 05. 2023).

[5] Bundeskriminalamt. „Cyberkriminalität, Polizeilich erfasste Fälle bis 2021 | Statista“. Statista, Hrsg. (2023), Adresse: https://de.statista.com/statistik/daten/studie/295265/umfrage/polizeilich-erfasste-faelle-von-cyberkriminalitaet-im-engeren-sinne-in-deutschland/?locale=de (besucht am 04. 05. 2023).

[6] T. Schrader, „Gender-Hinweis Hausarbeit: Vorlage und wohin er gehört“, *Scribbr*, Jg. 2022, 11. Aug. 2022. Adresse: https://www.scribbr.de/hausarbeit/gender-hinweis-hausarbeit-vorlage/ (besucht am 09. 05. 2023).

[7] S. Fuchs, „Analyse der Nutzungsspuren des Web Clients von WhatsApp und Telegram im Arbeitsspeicher, Bachelorthesis“, deu. Adresse: https://monami.hs-mittweida.de/frontdoor/index/index/docId/13059.

[8] D. Barradas, T. Brito, D. Duarte, N. Santos und L. Rodrigues, „Forensic Analysis of Communication Records of Web-based Messaging Applications from Physical Memory“, in *Proceedings of the 14th International Joint Conference on e-Business and Telecommunications*, (Madrid, Spain), SCITEPRESS - Science and Technology Publications, 2017, S. 43–54, ISBN: 978-989-758-259-2. DOI: 10.5220/0006396100430054. Adresse: https://pdfs.semanticscholar.org/3aa3/5033ee706aab19c64bee4e6ef157120a1136.pdf (besucht am 04. 05. 2023).

[9] Y. -T. Chang, M. -J. Chung, C. -F. Lee, C. -T. Huang und S. -J. Wang, „Memory Forensics for Key Evidence Investigations in Case Illustrations“, in *2013 Eighth Asia Joint Conference on Information Security*, 2013, S. 96–101. DOI: 10.1109/ASIAJCIS.2013.22.

[10] Ben Lutkevich. „Computerforensik (IT-Forensik)“, ComputerWeekly.de. (2022), Adresse: https://www.computerweekly.com/de/definition/Computer-Forensik-IT-Forensik (besucht am 13. 05. 2023).

[11] M. Büchel und P. Hirsch, *Internetkriminalität, Phänomene - Ermittlungshilfen - Prävention*. Kriminalistik-Verl., 2014, 164 S., ISBN: 978-3-7832-0026-3.

[12] Bundesamt für Sicherheit in der Informationstechnik, „Leitfaden IT-Forensik“, Jg. 2011, 2011. Adresse: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Leitfaden_IT-Forensik.pdf?__blob=publicationFile&v=1 (besucht am 04. 06. 2023).

[13] A. Geschonneck, *Computer-Forensik, Computerstraftaten erkennen, ermitteln, aufklären*, 5., aktualisierte und erw. Aufl. dpunkt.verl., 2011, 366 S., ISBN: 978-3-89864-774-8.

[14] DWDS. „Artefakt Definition, Schreibung, Definition, Bedeutung, Synonyme, Beispiele | DWDS“. DWDS, Hrsg. (2021), Adresse: https://www.dwds.de/wb/Artefakt (besucht am 04. 05. 2023).

[15] Lydia Wimmer, „Die Gestaltung digitaler Artefakte - Designtheoretische Ansätze in der Human-Computer Interaction“, *Cuvillier Verlag*, S. 15–16, 2009. Adresse: https://cuvillier.de/uploads/preview/public_file/2228/9783869550442.pdf (besucht am 04. 05. 2023).

[16] Markus Hunn und Tom Spring. „Welche Online-Aktivitäten erzeugen digitale Spuren/Daten auf einem Gerät?“ Wirtschaftsinformatik reloaded, Hrsg., n|w Fachhochschule Nordwestschweiz. (2021), Adresse: https://www.fhnw.ch/plattformen/iwi/2021/11/18/welche-online-aktivitaeten-erzeugen-digitale-spuren-daten-auf-einem-geraet/ (besucht am 04. 05. 2023).

[17] Matthias Schmidt. „Digitale Forensik in a big Nutshell“, Institute for Digital Business - HWZ. (2020), Adresse: https://hwzdigital.ch/digitale-forensik-in-a-big-nutshell/ (besucht am 04. 05. 2023).

[18] DWDS. „Persistenz – Schreibung, Definition, Bedeutung, Synonyme, Beispiele | DWDS“, DWDS - Digitales Wörterbuch der deutschen Sprache. (2023), Adresse: https://www.dwds.de/wb/Persistenz (besucht am 08. 06. 2023).

[19] ITWissen.info. „Persistenz“, ITWissen.info. (2016), Adresse: https://www.itwissen.info/Persistenz-persistence.html (besucht am 08. 06. 2023).

[20] P. Mandl, *Grundkurs Betriebssysteme, Architekturen, Betriebsmittelverwaltung, Synchronisation, Prozesskommunikation, Virtualisierung* (Springer eBook Collection), ger, 5., aktualisierte Auflage. Wiesbaden: Springer Vieweg, 2020, 356 S., Mandl, Peter (VerfasserIn), ISBN: 9783658305475. DOI: 10.1007/978-3-658-30547-5.

[21] GfdS. „Was sind Emojis? | GfdS“, GfdS - Gesellschaft für deutsche Sprache e.V. (2015), Adresse: https://gfds.de/was-sind-emojis/ (besucht am 06. 05. 2023).

[22] J. Degenhard. „Global: WhatsApp users 2019-2028 | Statista“, Statista. (2023), Adresse: https://www.statista.com/forecasts/1145337/whatsapp-users-in-the-world (besucht am 06. 05. 2023).

[23] Ryte Wiki. „Instant Messenger einfach erklärt – Ryte Wiki“, Ryte Wiki. (2021), Adresse: https://de.ryte.com/wiki/Instant_Messenger#Funktionen_von_Instant_Messengern (besucht am 06. 05. 2023).

[24] ITWissen.info. „Web-Client“, ITWissen.info. (2020), Adresse: https://www.itwissen.info/Web-Client-web-client.html (besucht am 08. 06. 2023).

[25] Materna Virtual Solution. „Ende-zu-Ende-Verschlüsselung (Glossar IT-Sicherheit)“. Materna Virtual Solution, Hrsg., Materna Virtual Solution. (2022), Adresse: https://www.virtual-solution.com/glossar/ende-zu-ende-verschluesselung/ (besucht am 09. 05. 2023).

[26] Bornemann AG. „Ende-zu-Ende-Verschlüsselung“, Bornemann AG. (2021), Adresse: https://bornemann.net/wiki/ende-zu-ende-verschluesselung/ (besucht am 16. 05. 2023).

[27] P. Schmitz und S. Luber, „Was ist Ende-zu-Ende-Verschlüsselung (E2EE)?“, *Security-Insider*, Jg. 2018, 27. Juni 2018. Adresse: https://www.security-insider.de/was-ist-ende-zu-ende-verschluesselung-e2ee-a-727147/ (besucht am 09. 05. 2023).

[28] Google. „Google Play-Store Threema“, Google. (2023), Adresse: https://play.google.com/store/search?q=threema&c=apps&hl=de&gl=US (besucht am 06. 05. 2023).

[29] Apple. „Threema Apple App-Store“, Apple. (2023), Adresse: https://apps.apple.com/de/app/threema-der-sichere-messenger/id578665578 (besucht am 06. 05. 2023).

[30] Threema. „The Threema Story“, Threema. (2023), Adresse: https://threema.ch/de/about (besucht am 06. 05. 2023).

[31] Threema. „Funktionen und Bedienung. Mehr als sicheres Messaging – Threema“, Threema. (2023), Adresse: https://threema.ch/de/funktionen (besucht am 09. 05. 2023).

[32] Threema. „Was ist eine Threema-ID?“, Threema. (2023), Adresse: https://threema.ch/de/faq/threema_id (besucht am 10. 05. 2023).

[33] Threema. „Was bedeuten die drei farbigen Punkte neben einem Kontakt? – Threema“, Threema. (2023), Adresse: https://threema.ch/de/faq/levels_expl (besucht am 09. 05. 2023).

[34] Instagram. „Instagram Direct Messenger | Video Chat & Send DMs | About Instagram“, Meta. (2023), Adresse: https://about.instagram.com/features/direct (besucht am 06. 05. 2023).

[35] Landsiedel-Seminare. „Was ist Kommunikation? Definition, Arten und Modelle“, Landsiedel. (2023), Adresse: https://www.landsiedel-seminare.de/coaching-welt/wissen/lexikon/kommunikation.html (besucht am 11. 05. 2023).

[36] L. Lazar, „Sender-Empfänger Modell – Schritt für Schritt erklärt (+Beispiel)“, *Nachhilfe-Team.net*, Jg. 2021, 28. Dez. 2021. Adresse: https://www.nachhilfe-team.net/studitipps/sender-empfaenger-modell/ (besucht am 16. 05. 2023).

[37] C. Niesen, „Abhörskandal: Alles Wichtige zur NSA-Affäre“, *DER SPIEGEL*, Jg. 2017, 16. Feb. 2017. Adresse: https://www.spiegel.de/politik/deutschland/nsa-affaere-worum-geht-es-a-1134779.html (besucht am 11. 05. 2023).

[38] S. Kersken, *Handbuch für Fachinformatiker, Der Ausbildungsbegleiter ; [EDV-Grundlagen, Programmierung, Mediengestaltung ; praxisorientiertes Lehr- und Nachschlagewerk ; für Fachinformatiker der Bereiche Anwendungsentwicklung und Systemintegration* (Galileo Computing), ger, 2., erw. Aufl. Bonn: Galileo-Press, 2005, 1076 S., ISBN: 3-89842-668-8.

[39] M. Wernert, *Internetkriminalität, Grundlagenwissen, erste Maßnahmen und polizeiliche Ermittlungen*, ger, 3., aktualisierte Auflage. Stuttgart u. a.: Boorberg, 2017, 213 S., Wernert, Manfred (VerfasserIn), ISBN: 978-3-415-06009-8.

[40] A. S. Tanenbaum und T. Austin, *Rechnerarchitektur, Von der digitalen Logik zum Parallelrechner* (Always learning), ger, 6., aktualisierte Auflage. Hallbergmoos: Pearson, 2014, 799 S., Tanenbaum, Andrew S. (VerfasserIn) Austin, Todd (VerfasserIn), ISBN: 978-3-86894-238-5. DOI: 4238.

[41] L. Kuhlee und V. Völzow, *Computer-Forensik-Hacks* (Hacks series), ger, 1. Aufl. Beijing und Köln: O'Reilly, 2012, 322 S., ISBN: 978-3-86899-121-5.

[42] ITWissen.info. „Aufbau des Von Neumann Rechners“, ITWissen.info. (2014), Adresse: https://www.itwissen.info/lex-images/Aufbau-des-Von-Neumann-Rechners_en.png (besucht am 18. 05. 2023).

[43] Wissensplattform. „Von-Neumann-Architektur“, Wissensplattform. (2018), Adresse: https://wissensplattform-schueler.de/von-neumann-architektur/ (besucht am 18. 05. 2023).

[44] U. Rembold und P. Levi, *Einführung in die Informatik für Naturwissenschaftler und Ingenieure*, ger, 3., vollst. überarb. und erw. Aufl. München und Wien: Hanser, 1999, 610 S., ISBN: 3446181571.

[45] P. Schnabe. „DRAM - Dynamic RAM“, Elektronik-Kompendium.de. (2023), Adresse: https://www.elektronik-kompendium.de/sites/com/0701281.htm (besucht am 31. 05. 2023).

[46] ITWissen.info. „Virtueller Speicher (VS)“, ITWissen.info. (2020), Adresse: https://www.itwissen.info/Virtueller-Speicher-VS-virtual-storage-VS.html (besucht am 31. 05. 2023).

[47] ComputerWeekly.de. „Memory Management Unit (MMU)“, Computerweekly. (2022), Adresse: https://www.computerweekly.com/de/definition/Memory-Management-Unit-MMU (besucht am 08. 06. 2023).

[48] D. Labudde und M. Spranger, Hrsg., *Forensik in der digitalen Welt, Moderne Methoden der forensischen Fallarbeit in der digitalen und digitalisierten realen Welt*, ger, 1. Aufl. 2017, Labudde, Dirk (HerausgeberIn) Spranger, Michael (HerausgeberIn), Berlin, Heidelberg: Springer Berlin Heidelberg, 2017, 326 S., ISBN: 9783662538012. Adresse: http://nbn-resolving.org/urn:nbn:de:bsz:31-epflicht-1584151.

[49] volatilityfoundation. „The Volatility Foundation - Open Source Memory Forensics“, volatilityfoundation. (2023), Adresse: https://www.volatilityfoundation.org/ (besucht am 08. 06. 2023).

[50] Exterro. „FTK® Imager - Exterro“, Exterro. (2023), Adresse: https://www.exterro.com/ftk-imager (besucht am 08. 06. 2023).

[51] Magnet Forensics. „MAGNET DumpIt for Windows - Magnet Forensics“, Magnet Forensics. (2023), Adresse: https://www.magnetforensics.com/resources/magnet-dumpit-for-windows/ (besucht am 08. 06. 2023).

[52] GitHub. „GitHub - ufrisk/MemProcFS: MemProcFS“, GitHub. (2023), Adresse: https://github.com/ufrisk/MemProcFS (besucht am 08. 06. 2023).

[53] Robert Sheldon. „Flüchtiger Speicher (Volatile Memory)“. Computerweekly, Hrsg. (2022), Adresse: https://www.computerweekly.com/de/definition/Fluechtiger-Speicher-Volatile-Memory (besucht am 04. 05. 2023).

[54] C. Willer, *PC-Forensik, Daten suchen und wiederherstellen* (Computer & Literatur), ger, Dt. Orig.-Ausg., 1. Aufl. Böblingen: C & L Computer und Literaturverl., 2012, 509 S., ISBN: 978-3-936546-60-6.

[55] IONOS Digital Guide. „hiberfil.sys: Löschen und Deaktivieren der Ruhezustandsdatei“, IONOS Digital Guide. (2020), Adresse: https://www.ionos.de/digitalguide/server/konfiguration/hiberfilsys-loeschen-und-deaktivieren/ (besucht am 26. 05. 2023).

[56] IONOS Digital Guide. „pagefile.sys: Alle Informationen zur Auslagerungsdatei von Windows“, IONOS Digital Guide. (2020), Adresse: https://www.ionos.de/digitalguide/server/konfiguration/pagefilesys/ (besucht am 26. 05. 2023).

[57] IT-Service-Network. „Was ist Hardware? – Definition im IT-Lexikon“, IT-Service-Network. (2023), Adresse: https://it-service.network/it-lexikon/hardware (besucht am 24. 05. 2023).

[58] D. Barrett und G. Kipper, *Virtualization and forensics, A digital forensic investigators guide to virtual environments*, eng. Amsterdam und Heidelberg: Syngress, 2010, 254 S., ISBN: 978-1-59749-557-8.

[59] Robert Sheldon. „Virtuelle Maschine - Virtual Machine“, Computerweekly. (2023), Adresse: https://www.computerweekly.com/de/definition/Virtuelle-Maschine-Virtual-Machine-VM (besucht am 25. 05. 2023).

[60] J. Ehneß und S. Luber, „Was ist eine Virtuelle Maschine (VM)?“, *Storage-Insider*, 16. Aug. 2019. Adresse: https://www.storage-insider.de/was-ist-eine-virtuelle-maschine-vm-a-842096/ (besucht am 25. 05. 2023).

[61] Oracle. „Downloads – Oracle VM VirtualBox“, Oracle. (2023), Adresse: https://www.virtualbox.org/wiki/Downloads (besucht am 23. 05. 2023).

[62] ComputerWeekly.de. „Was ist MD5? - Definition von WhatIs.com“, Computerweekly. (2016), Adresse: https://www.computerweekly.com/de/definition/MD5 (besucht am 20. 06. 2023).

[63] AimesElement. „Grau Und Weiß Grube Bulle Liegen Deiner Gras Zeigt Pfote Stockfoto und mehr Bilder von Hund - iStock“. (2016), (besucht am 24. 06. 2023).

[64] C. Bux, „Shar Pei“, *zooplus SE*, Jg. 2017, 8. Aug. 2017. Adresse: https://www.zooplus.de/magazin/hund/hunderassen/shar-pei (besucht am 24. 06. 2023).

[65] News Center Microsoft Deutschland. „Die Geschichte von Windows | News Center Microsoft“, Microsoft. (2023), Adresse: https://news.microsoft.com/de-de/features/windows-geschichte/ (besucht am 28. 05. 2023).

[66] Wikipedia. „Microsoft Windows 10“. de. Wikipedia, Hrsg. Creative Commons Attribution-ShareAlike License Page Version ID: 233741062, Wikipedia. (2023), Adresse: https://de.wikipedia.org/w/index.php?title=Microsoft_Windows_10&oldid=233741062 (besucht am 28. 05. 2023).

[67] W. Pryjda, „Energie sparen oder Ruhezustand: Wo ist der Unterschied?“, *WinFuture.de*, Jg. 2022, 13. Mai 2022. Adresse: https://winfuture.de/special/windows11/faq/Energie-sparen-oder-Ruhezustand-Wo-ist-der-Unterschied-252.html (besucht am 28. 05. 2023).

[68] Microsoft. „Windows 10 herunterladen“, Microsoft. (2023), Adresse: https://www.microsoft.com/de-de/software-download/windows10 (besucht am 26. 05. 2023).

[69] StatCounter. „Meistgenutzte Browser weltweit - April 2023 | Statista“, Statista. (2023), Adresse: https://de.statista.com/statistik/daten/studie/158095/umfrage/meistgenutzte-browser-im-internet-weltweit/ (besucht am 28. 05. 2023).

[70] P. Stelzel-morawietz, „Browsertest: Chrome, Firefox, Edge und Opera im Vergleich“, *PC-WELT*, Jg. 2021, 8. Mai 2021. Adresse: https://www.pcwelt.de/article/1168193/browsertest-firefox-chrome-edge-im-vergleich.html (besucht am 09. 06. 2023).

[71] Andrea Fortuna. „How to extract a RAM dump from a running VirtualBox machine“, Andrea Fortuna. (2017), Adresse: https://andreafortuna.org/2017/06/23/how-to-extract-a-ram-dump-from-a-running-virtualbox-machine/ (besucht am 22. 06. 2023).

[72] File-Recovery.com. „JPG Signature Format: Documentation & Recovery Example“, File-Recovery.com. (2023), (besucht am 01. 07. 2023).

[73] W. Storr, „ODER-Gatter Tutorial“, *Basic Electronics Tutorials and Revision*, Jg. 2018, 8. Okt. 2018. Adresse: https://www.electronics-tutorials.ws/de/logische/oder-gatter.html (besucht am 14. 07. 2023).

Eidesstattliche Erklärung

Hiermit versichere ich – Finn Hohlfeld – 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, 16. August 2023 [redacted]

Ort, Datum