HOCHSCHULE MITTWEIDA
UNIVERSITY OF APPLIED SCIENCES

Bachelorarbeit

Herr
Leander Hoßfeld

IT-Forensische Sicherung und qualitative Bewertung von ermittlungsrelevanten Daten aus Fitnesstrackern/Fitness-Smartwatches ohne Zugriffsmöglichkeiten auf das ursprünglich gekoppelte Smartphone

MIAS
Modernes Fortbildungsprogramm für technische Mitarbeiter und Harmonisierung wissenschaftlicher Abschlussarbeiten in Kriminaltechnischen Instituten der Sicherheitsbehörden

Die vorliegende Arbeit wurde in der Zeit vom 07.07.2022 bis zum 26.09.2022 unter der Betreuung von Herrn Prof. Ronny Bodach und Herrn Dipl. Inf. Andreas Sommer im Landeskriminalamt Thüringen (TLKA) in Erfurt durchgeführt. Die vorliegende Arbeit wurde im Rahmen des EU-Projektes MiAS (Fördernummer: IZ25-5793-2019-45) durchgeführt und kofinanziert.

Das Projekt MiAS wird aus Mitteln des Fonds für die Innere Sicherheit der Europäischen Union kofinanziert (Fördernummer: IZ25-5793-2019-45).

Mittweida, 2022

Fakultät: Angewandte Computer- und Biowissenschaften

Bachelorarbeit

IT-Forensische Sicherung und qualitative Bewertung von ermittlungsrelevanten Daten aus Fitnesstrackern/Fitness-Smartwatches ohne Zugriffsmöglichkeiten auf das ursprünglich gekoppelte Smartphone

Autor:
Herr

Leander Hoßfeld

Studiengang:
Allgemeine und Digitale Forensik

Seminargruppe:
FO19w4-B

Erstprüfer:
Herr Prof. Ronny Bodach

Zweitprüfer:
Herr Dipl. Inf. Andreas Sommer

Einreichung:
Mittweida, 26.09.2022

Verteidigung/Bewertung:
Mittweida, 2022

Faculty: Applied Computer Sciences and Biosciences

Bachelor Thesis

IT forensic backup and qualitative evaluation of investigation-relevant data from fitness trackers/fitness smartwatches without access to the originally paired smartphone

author:
Mr.

Leander Hoßfeld

course of studies:
General and Digital Forensic Science

seminar group:
FO19w4-B

first examiner:
Mr. Prof. Ronny Bodach

second examiner:
Mr. Dipl. Inf. Andreas Sommer

submission:
Mittweida, 26.09.2022

defence/ evaluation:
Mittweida, 2022

Bibliografische Beschreibung:

Leander Hoßfeld:

IT-Forensische Sicherung und qualitative Bewertung von ermittlungsrelevanten Daten aus Fitnesstrackern/Fitness-Smartwatches ohne Zugriffsmöglichkeiten auf das ursprünglich gekoppelte Smartphone. - 2022. - 18, 90, 16 S.

Mittweida, Hochschule Mittweida, University of Applied Sciences, Fakultät: Angewandte Computer- und Biowissenschaften, Bachelorarbeit, 2022.

Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung von männlichen und weiblichen Sprechformen verzichtet. Sämtliche allgemeine Personenbezeichnungen gelten gleichwohl für beiderlei Geschlecht.

Referat:

Die vorliegende Bachelorarbeit befasst sich mit der Sicherung und qualitativen Bewertung von ermittlungsrelevanten Daten, die auf Fitnesstrackern/Fitness-Smartwatches ausgewählter Hersteller abgelegt sind. Das Ziel dieser Arbeit besteht darin, zu untersuchen, unter welcher Konstellation die abgelegten Daten forensisch gesichert werden können, wenn keine Zugriffsmöglichkeit zum ursprünglich gekoppelten Smartphone besteht. Die Untersuchung erstreckt sich dabei auf die Simulation von Verbindungsumgebungen zwischen Fitnesstrackern/Fitness-Smartwatch und Android-Gerät sowie dem Auslesen und Interpretieren vorhandener Speicherchips.

Abstract:

This bachelor thesis deals with the backup and qualitative evaluation of investigation-relevant data that are stored on fitness trackers/fitness smartwatches from selected manufacturers. The aim of this thesis is to investigate under which constellation the stored data can be forensically secured if there is no access to the originally paired smartphone. The investigation covers the simulation of connection environments between fitness trackers/fitness smartwatches and Android devices as well as the reading and interpretation of existing memory chips.

Danksagungen

Im Rahmen meines zwölfwöchigen Bachelorpraktikums am Landeskriminalamt Thüringen in Erfurt von März bis Mai 2022 entstand der Wunsch, eine Bachelorarbeit mit Unterstützung des Dezernates 43 – Forensische IuK zu verfassen.

Zunächst möchte ich mich daher beim Landeskriminalamt Thüringen, insbesondere bei den Sachverständigen im Dezernat 43 – Forensische IuK bedanken, die mich im gesamten Zeitraum sowohl bei der Recherche als auch Durchführung der Untersuchungen unterstützt haben. Durch das kollegiale Arbeitsklima konnte das Bachelorprojekt mit hilfreichen Ratschlägen, Hinweisen sowie kritischen Diskussionen verbessert werden. Ein besonderer Dank gilt stellvertretend meinem Zweitbetreuer Herrn Dipl. Inf. Andreas Sommer (Erfurt), der mir das Thema vorgeschlagen hat und mich mit vielen interessanten Ideen, die in der IT-Forensik eine wesentliche Bedeutung haben, letzten Endes für derartige Fragestellungen begeistern konnte.

Ferner möchte ich mich bei meinem Vater, Prof. Dr. Uwe Hoßfeld (Jena), für die zahlreichen Gespräche und Hinweise zum Themengegenstand bedanken, der trotz vieler Verpflichtungen in Familie und Beruf, Zeit dafür gefunden hat.

Ein weiterer Dank gilt Frau Prof. Dr. phil. Henriette Haas (Montreux, Schweiz) für ihre kritischen Hinweise zum Manuskript.

Am Schluss möchte ich mich bei meinem Erstbetreuer, Herrn Prof. Ronny Bodach (Mittweida), für die stets kompetente Betreuung während des Bearbeitungszeitraumes bedanken. Die Möglichkeit, jederzeit Fragen zu stellen sowie Zwischenstände zum Einschätzen einzusenden, trugen einen Großteil zur Optimierung der Arbeit bei.

Inhalt

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

BSI	Bundesamt für Sicherheit in der Informationstechnik
RAM	Random Access Memory
TAP	Test Access Port
MEMS	Mikroelektromechanische Systeme
PPG	Photoplethysmographie
SSH	Secure Shell
SFTP	Secure File Transfer Protocol
FTP	File Transfer Protocol
FTPS	File Transfer Protocol over TLS
SoC	System-on-a-Chip
CPU	Central Processing Unit
PzP	Punkt-zu-Punkt-Verbindung
ROM	Read-Only Memory
EEPROM	Electrically Erasable Programmable Read-Only Memory
Mgt.	Management
AMOLED	Active Matrix Organic Light Emitting Diode
GPS	Global Positioning System
UHD	Ultra High Definition
HDMI	High Definition Multimedia Interface
LPDDR4	Low-Power Double Data Rate 4
SDRAM	Synchronous Dynamic Random Access Memory
LAN	Local Area Network
SATA	Serial Advanced Technology Attachment
APK	Android Package
IDE	Integrated Development Environment

WSON	Plastic Small-outline No-lead Package
SPI	Serial Peripheral Interface
DIL	Dual in-line Package
CTR	Counter Mode
AES	Advanced Encryption Standard
ADB	Android Debug Bridge
XML	Extensible Markup Language
LED	Light Emitting Diode
CSV	Comma-seperated values
ECDH	Elliptic-curve Diffie-Hellman
DSGVO	Datenschutz-Grundverordnung
BLOB	Binary Large Object

1 Einleitung

Digital assistierende Technologien erleben derzeit einen Boom. Durch die Digitalisierung und die damit einhergehende breite Verfügbarkeit von Endgeräten wie Smartphones und Wearables sowie deren Akzeptanz in der Gesellschafft, wächst die Zahl der von Menschen benutzten technischen Geräte stetig. Zu den wohl am meist verbreiteten Wearables gehören Smartwatches und Fitnesstracker [1]. Der weltweite Absatz von Wearables hat sich seit dem Jahre 2014 mehr als verzehnfacht. Sprach man 2014 noch von einem Absatz von 28,8 Millionen, so sind es im Jahre 2021 bereits 534 Millionen Geräte weltweit. 3,2 Millionen Geräte wurden davon 2021 allein in Deutschland abgesetzt [2]. Grenzt man die Zahlen nur auf Fitnesstracker ein, so wurden 2017 rund 36 Millionen Fitnesstracker verkauft. Die Prognose ist auch hier ein stetig wachsender Absatz von 51,73 Millionen Geräten bis Ende 2022 [3]. Der Boom ist nicht nur für die Firmen, sondern auch für die IT-Forensik ein großer Gewinn. Fitnesstracker sowie Smartwatches synchronisieren und speichern relevante digitale Daten in gekoppelten Smartphones oder Cloud-Diensten. Sie überwachen und erfassen die Körperfunktionen und zeichnen Bewegungsmuster der Menschen auf, wie z.B. Herzfrequenzen, Schritte und ggf. Positionsdaten mit Zeitbezügen [1].

Wie Literaturrecherchen zeigen, gehen erste Fallbeispiele bis in die 2010er Jahre zurück: In einem ersten aus dem Jahre 2018 gelang es Ermittlern aus den USA, mithilfe von Daten aus einem *Fitbit*-Fitnesstracker, schnell einen Verdächtigen in Rahmen eines Mordfalles zu überführen. Der Verdächtige „[…] gab bei einer Befragung an, seine Stieftochter am Nachmittag des 8. Septembers besucht zu haben. Als er gegangen sei, habe sie noch gelebt. Das Video einer Überwachungskamera zeigt aber, dass der Mann erst kurz nach halb vier Navarras Haus verlässt – nachdem das Fitness-Armband der Frau den Anstieg und den endgültigen Stopp des Herzschlags aufzeichnete“ [4]. In einem weiteren aktuellerem Fallbeispiel aus Griechenland vom Mai 2021 überführten Ermittler einen mutmaßlichen Täter durch die Vitaldaten des Fitnesstrackers seiner Frau [5]. Eine Sicherung und anschließende Auswertung des Fitnesstrackers der jungen Frau zeigte, „[…] dass sie in der betreffenden Nacht früher gestorben war, als der Mann angegeben hatte. Auch sei ihr Puls zuvor normal gewesen […]“ [5], obwohl dieser bei einem derartigen Überfall sehr hoch hätte sein müssen, wie griechische Medien unter Berufung auf Polizeikreise berichteten [5].

Durch die Untersuchung der oben genannten Geräte können somit Aussagen in Strafverfahren unterstützend zu anderen Beweismitteln auf ihre Glaubwürdigkeit und einzelne Aktivitäten von Personen nachvollzogen werden. Damit erschließen sich in der IT-Forensik neue Aufgabengebiete, die mit Blick auf die Digitalisierung und der einhergehenden Verbreitung von Fitnesstrackern sowie Smartwatches, neue Themenfelder und Handlungsmöglichkeiten für den IT-Forensiker eröffnen.

1.1 Problemstellung

Um die Daten aus Fitnesstrackern/Fitness-Smartwatches nutzen zu können, ist vor allem eine Betrachtung der gespeicherten Daten im Smartphone aus forensischer Sicht sinnvoll, wie eine ähnliche Bachelorarbeit bereits zeigte [6]. Fehlt jedoch bei einer Sicherstellung das Smartphone, sind relevante Daten der Fitnesstracker/Fitness-Smartwatches für die Ermittler dort nicht mehr einsehbar. Aus den oben erwähnten Fallbeispielen ergeben sich perspektivisch somit nachfolgende Fragen:

1. Sind auf den Fitnesstrackern/Fitness-Smartwatches selbst ermittlungsrelevante Daten abgelegt?

2. Wenn ja, wie können diese forensisch gesichert werden?

3. Was ergibt ein Vergleich exemplarisch ausgewählter Hersteller?

4. Ist es möglich, eine entsprechende Handlungsempfehlung für zukünftige derartige Fragestellung für den IT-Forensiker zu erarbeiten?

1.2 Zielsetzung

Das Ziel der folgenden Arbeit besteht darin, zu untersuchen, ob und wenn ja, unter welcher Konstellation die auf Fitnesstrackern/Fitness-Smartwatches abgelegten Daten forensisch gesichert werden können, wenn keine Zugriffsmöglichkeit zum ursprünglich gekoppelten Smartphone besteht. Die Untersuchung erstreckt sich dabei auf:

1. Die Erzeugung von Verbindungsumgebungen zwischen Fitnesstrackern/Fitness-Smartwatch und Simulationsgeräten (*Android*) mit dem Ziel, dass Synchronisations- und Speicherverhalten sowie die Zugangsmöglichkeiten der Geräte für den IT-Forensiker darzustellen;

2. Die Extraktion sowie Interpretation ermittlungsrelevanter Daten aus vorhandenen Speicherchips.

Weiterhin soll eine Handlungsempfehlung für die digitale Forensik im Falle einer Einzelsicherung erstellt werden.

1.3 Aufbau der Arbeit

Die nachfolgende Arbeit besteht aus vier Hauptteilen. Nachdem zunächst in einer Einleitung auf die Problemstellung und Zielsetzung eingegangen wurde, folgt ein erstes theoretisches Teilkapitel über die benutzten Grundlagen (IT-Forensik, Wearables, Elektronische Bauelemente, Secure-Shell-Protocol). Daran schließt sich das dritte Teilkapitel über „Material und Methoden“ an. Neben dem Untersuchungsdesign werden hier Fragen der Hard- und

Software analysiert, das Untersuchungsbetriebssystem *LineageOS* vorgestellt, die IT-Forensische Sicherung der Daten, Mikrochips und Adapter sowie die Extraktion der ermittlungsrelevanten Daten thematisiert. Das vierte und fünfte Teilkapitel ist den Ergebnissen der Analysen und der entsprechenden Diskussion gewidmet. Die Bachelorarbeit wird durch ein Fazit und einen Ausblick letztendlich abgerundet. Ein Literaturverzeichnis sowie ein weiterführender, umfassender, hauptsächlich bebilderter Anhang ergänzen die Arbeit entsprechend.

2 Grundlagen

Um ein tiefgründiges Verständnis für die in der Arbeit besprochene Thematik und deren angewandte Methodiken zu erlangen, ist es zunächst notwendig, einige essenzielle Grundlagen vorzustellen.

2.1 IT-Forensik

Die Begrifflichkeit IT-Forensik, als ein Teilgebiet der allgemeinen Forensik, setzt sich aus den Worten „Informationstechnologie“ und „Forensik“ zusammen. „Forensisch“ entspringt dabei dem lateinischen Wort *forensis* (dt. = zum Forum gehörig, auf dem Forum befindlich) [7]. Im alten Rom stellte das Forum den Markt- und Gerichtsplatz der Stadt dar, auf dem Untersuchungen, Gerichtsverfahren, Urteilsverkündigungen sowie der Vollzug der Urteile durchgeführt wurden. Dadurch weist die IT-Forensik einen Bezug zum Gericht auf [8]. Der Begriff „forensisch“ bedeutet folglich „für den Gebrauch vor Gericht“. Das charakteristische Ziel der IT-Forensik ist somit die Nutzung von informationstechnischen Daten als Beweis in Gerichtsverfahren. Eine einheitliche Definition des Begriffs die darüber hinausgeht existiert jedoch nicht [7]. Als Beispiel für die Heterogenität des Begriffes seien folgende Definitionen aufgeführt:

> Nach Heinson [7, S. 17] wird der Begriff IT-Forensik als „[…] die Sicherung und Analyse von Daten aus IT-Systemen mit wissenschaftlichen Methoden, um damit vor Gericht Sachverhalte zu beweisen“ definiert.
>
> Das Bundesamt für Sicherheit in der Informationstechnik (BSI) [9, S. 13] hingegen schlägt in seinem *Leitfaden „IT-Forensik“* die Definition des Begriffes als eine „[…] streng methodisch vorgenommene Datenanalyse auf Datenträgern und in Computernetzen zur Aufklärung von Vorfällen unter Einbeziehung der Möglichkeiten der strategischen Vorbereitung insbesondere aus der Sicht des Anlagenbetreibers eines IT-Systems“ vor.

2.1.1 Forensische Untersuchung

Oberstes Ziel für jeden IT-Forensiker ist die Beständigkeit der gewählten Methoden, Hilfsmittel und Ergebnisse vor Gericht. Während der gesamten Untersuchung muss jeglicher Manipulationsverdacht ausgeschlossen werden. Die Resultate müssen eine große Evidenz besitzen, sodass auch Außenstehende, die nicht über denselben Wissens- bzw. Erfahrungsstand verfügen, vollstände Gewissheit erlangen können [10]. An eine forensische Untersuchung sind demnach spezielle Anforderungen zu stellen.

Nach Geschonneck [10] ergeben sich sechs Anforderungen:

1. **Akzeptanz:** Die angewandten Methodiken und Schritte müssen von der Fachwelt beschrieben und anerkannt sein. Bei neuen Verfahren und Werkzeugen sollten idealerweise professionelle Ermittler bereits damit vertraut sein, wenn diese auf Konferenzen und Publikationen keine Erwähnung gefunden haben;
2. **Glaubwürdigkeit:** Bei Bedarf sollten bei den verwendeten Methoden Funktionalität und Robustheit nachgewiesen werden können. Besonders bei komplexeren Werkzeugen und Methoden ist dies besonders wichtig, wenn die Wirkungsweise vom Ermittler nicht verstanden und plausibel erklärt werden kann;
3. **Wiederholbarkeit:** Alle im Ermittlungsprozess verwendeten Methoden und Hilfsmittel müssen von Dritten bei Anwendung wiederholbar sein und am Ende bei gleicher Schrittfolge, gleiche Ergebnisse liefern;
4. **Integrität:** Während des gesamten Ermittlungsprozesses muss sichergestellt werden, dass die Spuren unverändert bleiben. Die Integrität der Beweismittel muss jederzeit demonstriert werden können;
5. **Ursache und Auswirkung:** Die Methodiken, die für die Ermittlung gewählt wurden, erfordern es zu jeder Zeit, Verbindungen zwischen Personen, Ereignissen und Beweisspuren herzustellen;
6. **Dokumentation:** Im Ermittlungsprozess ist es erforderlich, jeden Schritt angemessen zu dokumentieren.

Neben den hier aufgeführten Anforderungen ist es ebenfalls notwendig, eine gut strukturierte und logische Abfolge der einzelnen Prozessschritte einer forensischen Untersuchung zu definieren. Das BSI [9] unterteilt in seinem *Leitfaden „IT-Forensik“* dahingehend die Vorgehensweise einer forensischen Untersuchung in sechs Abschnitte:

1. **Strategische Vorbereitung (SV):** Im Rahmen dieses Abschnittes werden alle Maßnahmen vor dem eigentlichen Eintreten bzw. in Erwartung eines Vorfalls getroffen. Beispiel: Aktivierung von Logdiensten zur Protokollierung der Umstände eines Vorfalls;
2. **Operationale Vorbereitung (OV):** Hierbei sind alle Maßnahmen einzuordnen, die zwar nach Eintreten eines Vorfalls, aber vor der eigentlichen Datensammlung erfolgen. Beispiel: Identifikation potenzieller Datenquellen wie mobiler Datenträger oder externer Geräte;
3. **Datensammlung (DS):** Auf die Identifikation potenzieller Datenquellen folgt im Rahmen dieses Abschnittes die Erzeugung von Abbildern (Images). Sämtliche erzeugte Abbilder müssen dabei mittels kryptographischer Verfahren abgesichert werden, um die Integrität des Beweismittels sicherzustellen;
4. **Untersuchung (US):** In diesem Abschnitt werden alle Maßnahmen zusammengefasst, die aus den erzeugten Abbildern forensisch wertvolle Daten extrahieren können. Beispiel: Extraktion relevanter Bilddateien aus dem Abbild einer Festplatte;
5. **Datenanalyse (DA):** Die extrahierten Daten werden im Rahmen dieses Abschnittes nun einer Detailanalyse unterzogen. Hierzu zählen Maßnahmen, die in der Lage

sind, aufgrund von vorgefundenen Inhalten, Verbindungen zwischen mehreren Spuren herzustellen und eventuell auf eine Urheberschaft zu schließen. Beispiel: Auswertung von Logdateien;

6. **Dokumentation (DO):** Alle gefundenen Einzelergebnisse werden im Rahmen dieses Abschnittes nun in einer Gesamtbetrachtung zusammengefasst. Man spricht von der sogenannten abschließenden Dokumentation. Im Gegensatz dazu, verläuft die parallele Dokumentation. Ihre Aufgabe besteht aus der Protokollierung der gewonnenen Daten und durchgeführten Prozesse wie z.B.: Name und Version des verwendeten Programms, Kommandozeilenparameter des Aufrufs sowie die Motivation zur Auswahl bestimmter Werkzeuge.

2.1.2 Forensische Datensicherung

Im Buch *Forensik in der digitalen Welt* [11, S. 118] heißt es: „Jede digital-forensische Analyse beginnt mit der Datensicherung." In der Regel ist die Sicherung digitaler Spuren mit der Erstellung eines korrekten forensischen Abbildes, auch Image genannt, verbunden. Dieser Schritt ist jedoch nicht unproblematisch. Jede Nachlässigkeit kann in dieser Phase zu Manipulationsverdacht führen und nicht mehr rückgängig gemacht werden. Im schlimmsten Falle ist die Sicherung nicht mehr gerichtsverwertbar [11]. In der IT-Forensik unterscheidet man grundsätzlich zwischen zwei Untersuchungsformen in Bezug auf Datensicherungen: a.) Post-mortem-Analyse und b.) Live-Forensik [9].

Bei der **Post-mortem-Analyse** (Offline-Forensik) wird ein Vorfall nachträglich aufgeklärt. Im Wesentlichen geschieht dies durch die Untersuchung von Datenträgerabbildern auf persistente also nichtflüchtige Spuren. Die wichtigsten Untersuchungsinhalte sind dabei die Gewinnung und Analyse von gelöschten, umbenannten sowie anderweitig verschlüsselten und versteckten Dateien aus Massenspeichern [9]. Diese Untersuchungsmethodik wird oft auch **physikalische Datensicherung** genannt. Der Massenspeicher wird dabei vollständig dupliziert und es entsteht ein Datenträgerabbild (Image). In der Regel wird dafür jeder einzelne Sektor gelesen und gesichert. Dies betrifft auch Bereiche, die vom Betriebssystem als „frei" angesehen werden [12]. Mit dem erstellten Image erhält der Forensiker somit eine „[…] 1:1 Kopie des Datenträgers, an welchem verschiedene Untersuchungsschritte mehrfach ausgeführt werden können, ohne die Originaldaten zu verändern" [9, S. 26].

Die **Live-Forensik** (Online-Forensik) umfasst hingegen Maßnahmen, die man bereits während der Laufzeit des Vorfalls vornimmt. Hierbei wird vor allem versucht, nicht persistente, also flüchtige Daten, zu gewinnen und anschließend zu untersuchen [9]. Diese beinhalten unter anderem Informationen über bestehende Netzwerkverbindungen, gestartete Prozesse sowie mögliche Hauptspeicherinhalte [12]. Die dabei oft angewandte Untersuchungsmethodik wird **logische Datensicherung** genannt und bildet das Gegenteil zur bereits beschriebenen physikalischen. Hierbei ist anzumerken, dass die Datensicherung hier immer unter Zuhilfenahme des originalen Beweismittels, direkt aus dem laufenden System, geschieht. Ein besonderes Augenmerk liegt dabei vor allem auf Daten, die nur während

einer offenen Sitzung erhoben werden können, da sie andernfalls nicht mehr zugänglich sind. Zu diesen Daten gehören: Cloud Speicher, Messenger Inhalte, offene verschlüsselte Bereiche, Inhalte von Datenbanken sowie Online E-Mail Postfächer [12].

2.1.3 Gesonderte Vorgehensweisen und Überlegungen bei der Datensicherung von Mobilgeräten

Abseits von der klassischen Definition und Vorgehensweise forensischer Datensicherungen, stellt die Überlegung in Bezug auf Mobilgeräte, auch Mobilfunkforensik genannt, eine besondere Herausforderung dar. Unabhängig davon, welche Methode für die unterschiedlichen Geräte gewählt wird, ist es auch hier unerlässlich, die Integrität der Daten sicherzustellen, sie also möglichst unverändert zu lassen. Da die Daten von Mobilgeräten aufgrund ihrer kompakten Bauweise häufig selbst mobil, also nicht persistent sind, ist die Sicherstellung der Integrität hier problematisch, weshalb Untersuchungen häufig noch während des Betriebes durchgeführt werden müssen. Jede Interaktion während des Betriebes kann dadurch zu einer Veränderung der Daten führen, wodurch aber auch flüchtige Beweise, siehe Teilkapitel 2.1.2, gesammelt werden können. Trotz der Problemstellung sollte der IT-Forensiker zunächst versuchen, Methoden anzuwenden, die die Integrität eines Gerätes weniger gefährden, also nicht in die Daten eingreifen. Man spricht hierbei von nicht-invasiven forensischen Methoden [13]. Die Abbildung 1 stellt die Methodenauswahl der Mobilfunkforensik in Form einer Pyramide dar. Mit jeder Ebene in Richtung Spitze erhöhen sich die Invasivität, die benötigten Vorkenntnisse, die Analysedauer sowie die technische Herausforderung der gewählten Methode.

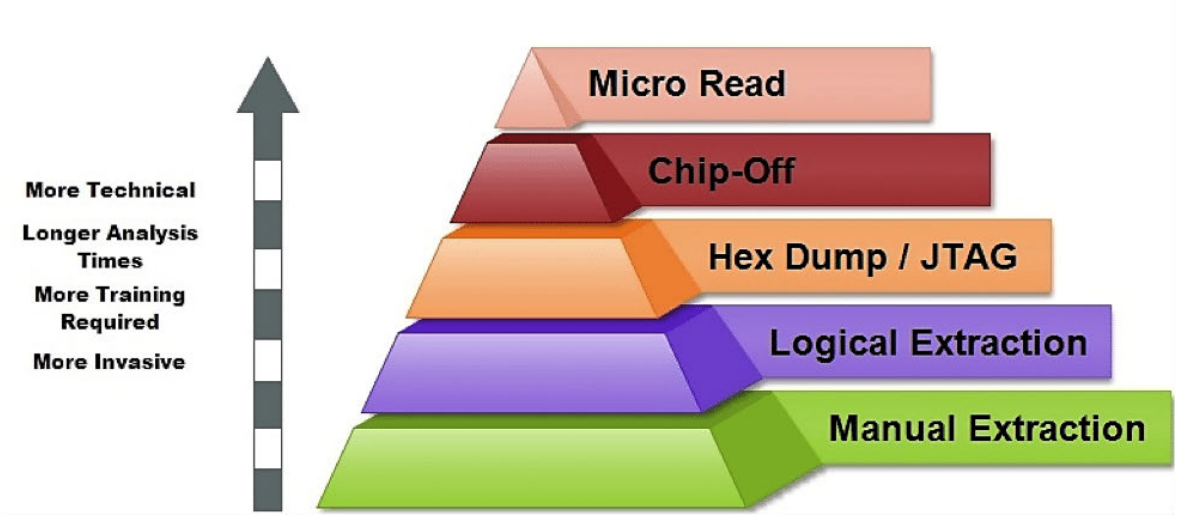


Abbildung 1: Methoden-Klassifikations-Pyramide der Mobilfunkforensik [13]

Nicht-invasive forensische Methoden lassen sich wie folgt aufgliedern:

1. **Manuelle Extraktion (*Manual Extraction*):** In dieser Methode durchsucht der IT-Forensiker die Daten des Mobilgerätes lediglich über Tastatur oder Touchscreen. Dabei werden alle relevanten Informationen fotografisch dokumentiert;

2. **Logische Extraktion (*Logical Extraction*):** Bei diesem Verfahren wird eine Verbindung zwischen dem Mobilgerät und der forensischen Arbeitsstation über ein USB-Kabel, *Bluetooth* etc. hergestellt. Anknüpfend an den Verbindungsaufbau sendet die Arbeitsstation Befehlsanfragen an das Gerät, woraufhin das Gerät selbst aus seinem Speicher Daten zurücksendet;
3. **JTAG-Verfahren:** In dieser Methode stellt der IT-Forensiker eine Verbindung zu den Test-Access-Ports (TAPs) eines Gerätes her und weist den Prozessor an, die auf den vorhandenen Speicherchips gespeicherten Rohdaten auf die Arbeitsstationen zu übertragen;
4. **Hex-Dump:** Bei diesem Verfahren wird die forensische Arbeitsstation mit dem Gerät verbunden und anschließend ein unsignierter Code oder Bootloader in das Gerät getunnelt, welche dann jeweils Anweisungen zum Extrahieren des Speichers vom Mobilgerät enthalten. Die resultierende Datenextraktion liegt im Binärformat vor [13].

In Fällen einer schweren Beschädigung müssen die Flash-Speicherchips des Gerätes manuell entfernt und gesichert werden [14]. Die dabei angewandten Methoden werden als invasive forensische Methoden bezeichnet und unterteilen sich in folgende Arten:

1. **Chip-Off:** Aufgrund der Methodenrelevanz in der vorliegenden Bachelorarbeit wird dieser Methode ein extra Teilkapitel 2.1.4 gewidmet;
2. **Micro Read:** Bei dieser Methode wird durch die Linsen eines Elektronenmikroskops ein manueller Rundumblick geworfen und die Daten auf dem Speicherchip, genauer die physikalischen *Gates*, analysiert [13].

2.1.4 Chip-Off-Analyse

Bei der Chip-Off-Analyse versucht der IT-Forensiker, Speicherchips physisch aus dem Gerät zu entfernen und mittels spezieller Hardware die Daten aus dem Chip zu extrahieren [14]. Wie die Abbildung 1 bereits gezeigt hat, ist die Untersuchungsmethodik eine technische Herausforderung. Schon das Herauslöten der Chips ist kostspielig und erfordert eine besondere Schulung. Der IT-Forensiker muss sich hierfür spezielle Geräte beschaffen, die das Erhitzen und Herauslöten der Speicherchips ermöglichten [13]. Sind alle Vorbereitungen getroffen, muss unter einer bestimmten Temperatur das Lötmittel zum Schmelzen gebracht werden, welches den Chip mit der Leiterplatte verbindet. Die Temperatur sollte jedoch nie deutlich höher als nötig sein, da dies unter Umständen zu Datenfehlern führen kann. Unter Beachtung der genannten Punkte kann der Chip anschließend abgezogen werden [14]. Im nächsten Schritt müssen die Bits und Bytes der Rohdaten, die man aus dem Speicher extrahieren kann, noch geparst, wenn nötig entschlüsselt und interpretiert werden. Ein kleiner Fehler in diesen drei Schritten kann ebenfalls zu irreparablen Schäden des Speicherchips führen, wodurch die Daten unwiderruflich verloren wären [13]. Experten raten daher nur zum Chip-Off, wenn: a.) bereits alternative Extraktionsmethoden versucht wurden; b.) der aktuelle Zustand des Gerätespeichers erhalten werden soll und c.) der Speicherchip das einzige, nicht zerstörte Element des Gerätes ist [13].

2.2 Wearables

Der Schirmbegriff Wearables bezeichnet am Körper getragene Kleinstcomputer oder Computersysteme, welche eine Datenerfassung und -verarbeitung ermöglichen [1]. Dazu zählen Elemente wie Uhren, Handschuhe, Brillen etc., die Computersysteme beinhalten und dem tragenden bei seiner Tätigkeit, ohne Beeinträchtigung der Flexibilität und Aufmerksamkeit, unterstützen sollen [15]. Wearables werden häufig dafür verwendet, anhand diverser Sensoren Körperdaten zu erfassen. Dabei bieten die Geräte die Möglichkeit, dem Anwender die Daten unmittelbar anzuzeigen oder auszugeben. Durch die Ausstattung mit kabelloser Kommunikationstechnik stellen diese somit flexible Lösungen, im Gegensatz zu anderen Geräteklassen, wie beispielsweise Smartphones, bereit. Solche Geräte sind insbesondere Fitnesstracker und Smartwatches [1].

2.2.1 Abgrenzung Fitnesstracker/Fitness-Smartwatch

Fitnesstracker und Smartwatches gehören zu den am meist verbreiteten Wearables. Sie werden am Handgelenk getragen und unterscheiden sich im Wesentlichen durch ihren Funktionsumfang. Beiden Geräten ist zunächst gemein, dass sie sowohl umwelt- als auch körperbezogene Daten erfassen können [1]. Dazu zählen etwa erfasste Schritte, detektiertes Schlafverhalten sowie der Kalorienverbrauch [15]. Aufgrund begrenzter Rechenkapazität geschieht die Auswertung der erfassten Rohdaten bei Fitnesstrackern meistens nicht auf dem Gerät selbst, sondern über ein gekoppeltes Tablet oder Smartphone, welche die auszuwertenden Daten durch eine App an entfernte Server zur Aufbereitung übermitteln [1].

Smartwatches hingegen gelten als Weiterentwicklung der Fitnesstracker und stellen dem Nutzer zusätzlich Funktionen bereit, die es ermöglichen, aktuelle Informationen aus seiner Umgebung zu senden. So erhält dieser seine eingehenden Anrufe, Nachrichten, Termine oder E-Mails nicht mehr nur über das Smartphone, sondern auch auf die Smartwatch [15]. Des Weiteren können über die Geräte auch Navigations- oder Kommunikationsanwendungen genutzt werden [1]. Informationsabfragen mittels Sprachbefehlen, Navigationsdienste sowie die intelligente Kommunikation zu anderen Geräten, wie z.B. der Kamera im Flur, sind nur wenige Auszüge der Funktionsbreite, die die Smartwatch vom Fitnesstracker abgrenzt [15].

Für die Begriffe Fitnesstracker und Smartwatch existieren eine Reihe an synonymen Bezeichnungen. In Bezug auf Fitnesstracker spricht Seyrkammer [15] von „Fitnessbändern“, währenddessen Luthe et al. [1] den Begriff „Gesundheitstracker“ verwendeten. Merkel [16] erwähnt im Kontext beider Begriffe die Bezeichnungen „Activitytracker“ und „Sportuhr“. Zuletzt spricht die Zeitung WELT [17] von „Fitness-Smartwatches“. Um Verwechslungen zu vermeiden und eine einheitliche Begriffsverwendung einzuführen, werden in der folgenden Bachelorarbeit ausschließlich die Begriffe **Fitnesstracker** und **Fitness-Smartwatch** verwendet.

2.2.2 Funktionsweise

Um die Funktionsweise von Fitnesstrackern und Fitness-Smartwatches zu verstehen, muss man zunächst erläutern, welche Sensoren in den Geräten verbaut sind und wie diese Daten aufzeichnen und interpretieren. In der Regel befinden sich in Fitnesstrackern und Fitness-Smartwatches mehrere Sensoren. Zu den am meisten verbreiteten gehören: Bewegungssensoren, optische Sensoren, barometrische Sensoren sowie GPS-Empfänger [18]. Welche Messergebnisse die Sensoren liefern, zeigt die Abbildung 2. In Bezug auf die vorliegende Bachelorarbeit, die ermittlungsrelevante Daten untersuchen soll, werden im Folgenden nur die Schritte sowie die Herzfrequenz betrachtet.

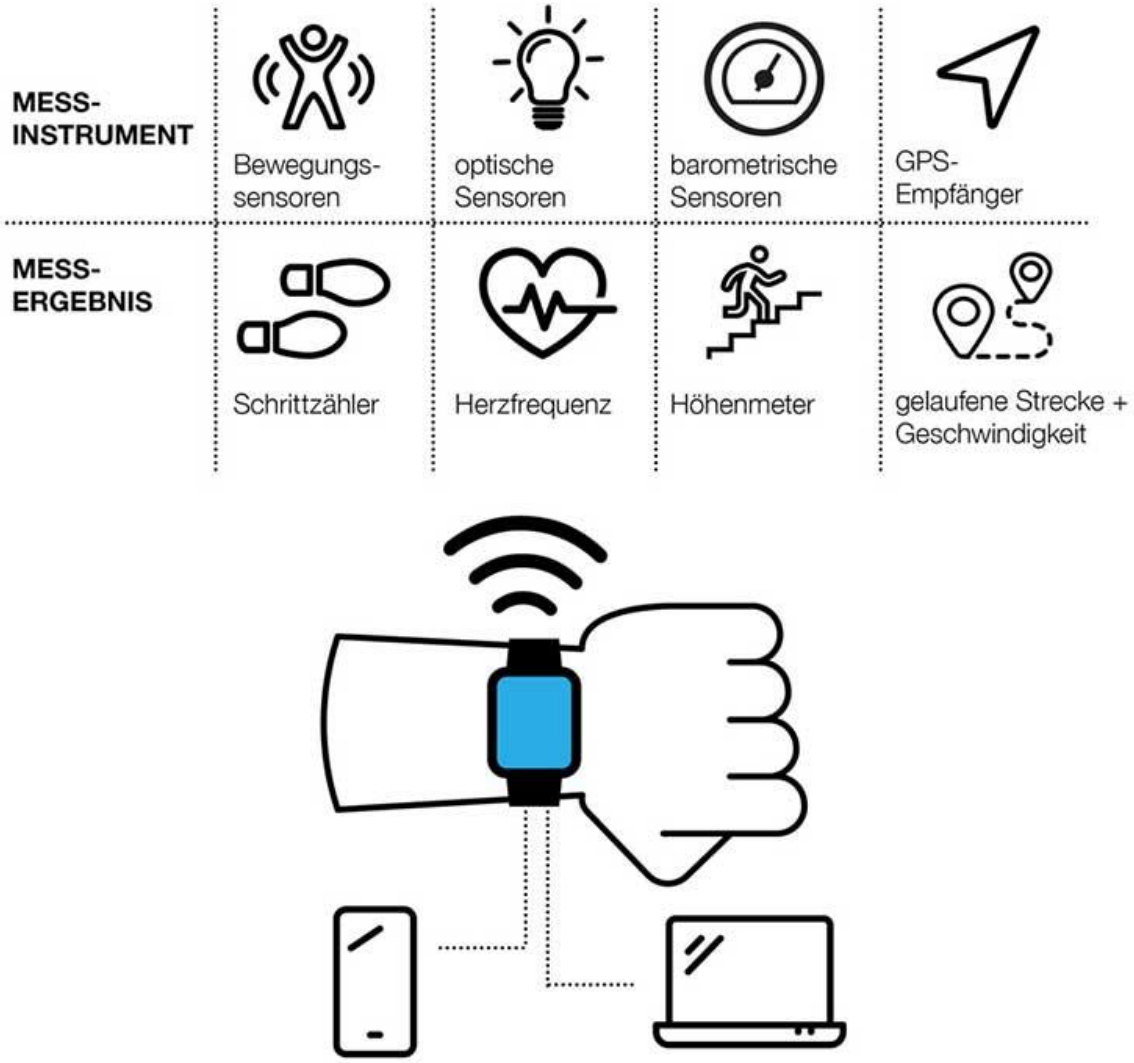


Abbildung 2: Messinstrumente und -ergebnisse von Fitnesstrackern/Fitness-Smartwatches [19]

Bewegungssensoren ermitteln die Bewegungen einer Person und befinden sich in jedem Fitnesstracker und jeder Fitness-Smartwatch. Es handelt sich dabei um kleinste Elemente, die sich auf den Elektronikbausteinen des Gerätes befinden und in den Bereich der Mikroelektromechanischen Systeme (MEMS) gehören. Man unterscheidet zwischen zwei

Sensoren: Beschleunigungssensoren und Gyroskop-Sensoren. Beschleunigungssensoren dienen der Erfassung linearer Bewegungen bzw. der Beschleunigung in allen drei Ebenen. Gyroskop-Sensoren hingegen erfassen die Rotationsbewegungen analog zur Erfassung der Beschleunigungssensoren ebenfalls in allen drei Ebenen eines dreidimensionalen Raums [18]. Die Abbildung 3 veranschaulicht den dreidimensionalen Raum zuzüglich der Rotationsbewegungen.

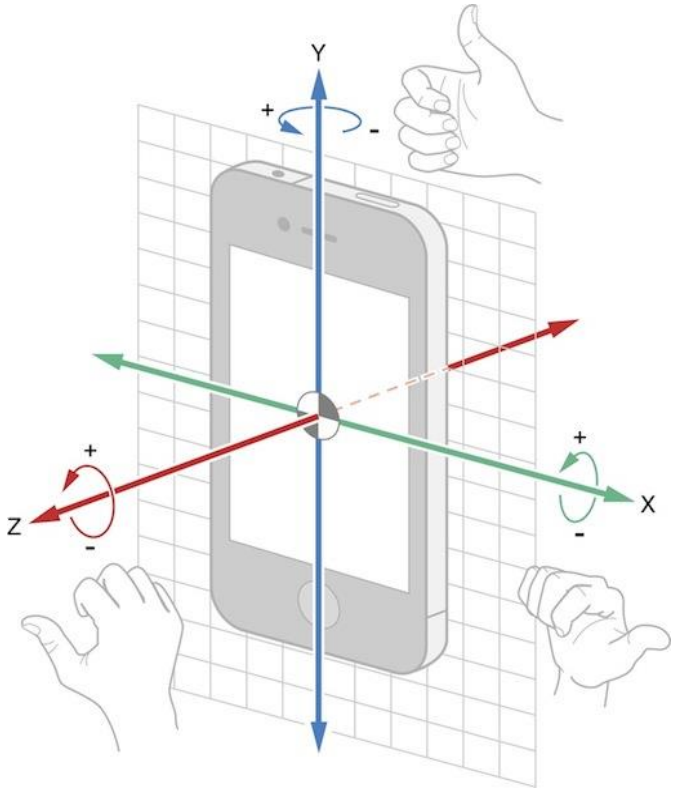


Abbildung 3: Dreidimensionaler Raum mit Rotationsbewegungen [20]

Mithilfe der aus den beiden Sensoren gewonnenen Messdaten können bspw. Bewegungen vollständig beschrieben werden. Wie dies geschieht, obliegt den einzelnen Herstellern, die mittels spezieller Algorithmen und Strategien der Musterkennung aus den Messwerten Rückschlüsse auf die Art der Bewegung zulassen [21].

Durch die sogenannte Photoplethysmographie (PPG) ist es schon seit längerer Zeit möglich, die Herzfrequenz mittels Licht zu messen. Auch in Fitnesstrackern und Fitness-Smartwatches findet sich die Technologie in Form von **optischen Sensoren** wieder. Die Geräte mit optischer Pulsmessung verfügen dabei in der Regel über eine kleine Lichtquelle, die an der Innenseite des Armbands angebracht ist. Von der Lichtquelle ausgehend, ist das Licht intensiv genug, um so weit in die Haut einzudringen, dass die in den oberen Hautschichten befindlichen Blutgefäße erreicht werden. Am Blutgefäß wird dann ein Teil des Lichts reflektiert und von einem weiterem am Armband befindlichen Sensor, dem Photodetektor, registriert [22]. Die Abbildung 4 verbildlicht den Vorgang der optischen Messung.

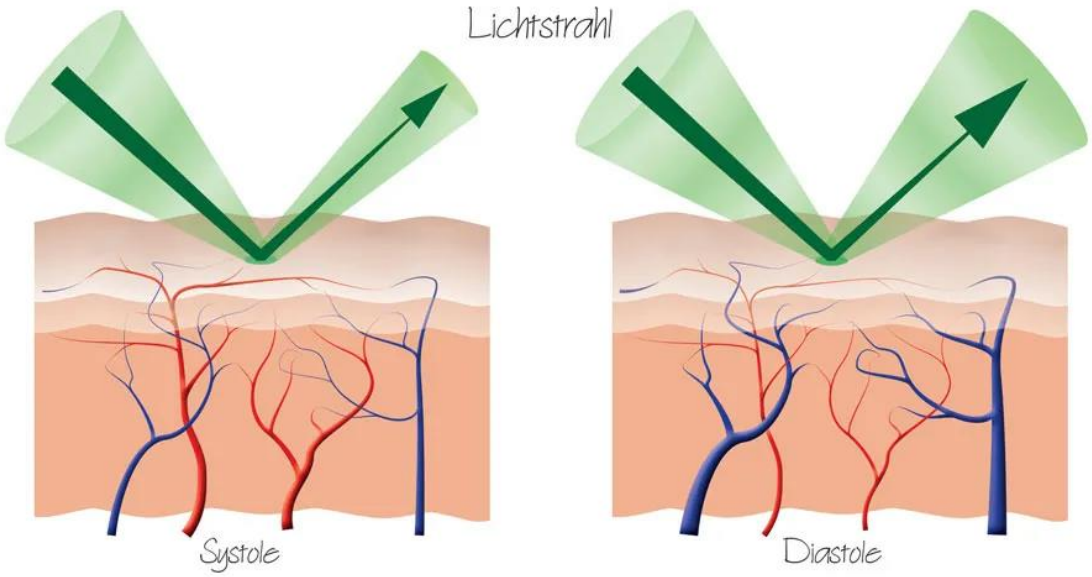


Abbildung 4: Optische Pulsmessung (schematisch) [22]

Der Photodetektor macht sich dabei die biologischen Eigenschaften des Herzmuskels zu Nutze. Man unterscheidet beim Herzschlag zwischen dem Zusammenziehen (Systole) und dem Entspannen des Herzmuskels (Diastole). Während bei der Systole Blut durch die Gefäße zu den Organen gedrückt wird und somit Blutfluss und Gefäßdurchmesser zunehmen, fließt bei der Diastole das Blut durch die Gefäße wieder zum Herzen zurück, wodurch Blutdruck und Gefäßdurchmesser abnehmen. Zusätzlich nutzt der Detektor die Farbe Rot von Blut, weil diese die roten Anteile des Lichts reflektiert, wohingegen grüne und blaue Farbanteile absorbiert werden. Eine große Menge Blut absorbiert also mehr Anteile von grünem und blauem Licht (Systole) als eine geringe (Diastole). Diese Veränderungen in den Anteilen des reflektierenden Lichts werden vom Photodetektor über die Zeit gemessen. Mit diesem Wissen kann nun aus der Zeitspanne zwischen den minimal gemessenen Grünanteilen sowohl der Herzzyklus als auch der Puls detektiert werden [22].

2.2.3 Marktübersicht

Durch die Digitalisierung und die daraus folgende Verbreitung von Wearables gibt es auf dem Weltmarkt eine Reihe an renommierten Herstellern die versuchen, ihre Fitnesstracker und Fitness-Smartwatches mit den unterschiedlichsten Farben, Formen und Funktionen zu verkaufen. Für die vorliegende Bachelorarbeit wurden dahingehend Marktanteile hinsichtlich der Absatzstärken einzelner Hersteller analysiert. Die Statistik in der Abbildung 5 zeigt die Marktanteile am weltweiten Absatz von Wearables nach Herstellern sortiert. Beim Betrachten der Statistik fällt auf, welche Hersteller die größten konstanten Marktanteile und welche im Laufe der Jahre an Anteilen verloren haben. Während *Xiaomi* von 2015 bis 2021 einen mehr oder minder konstanten Marktanteil aufweist, verlieren seit einiger Zeit Hersteller wie *Fitbit* oder *Garmin* vollständig ihre Position am Weltmarkt. Neben der Kategorie *Andere*, die bis 2019 die größten Anteile aufwiesen, verzeichnete *Apple* ab 2015 bis 2020 ein

konstantes Wachstum und stellte sich 2020 sogar als Marktführer heraus. Im Jahr 2021 lagen die größten Marktanteile bei der Kategorie *Andere* gefolgt von *Apple* und *Xiaomi*.

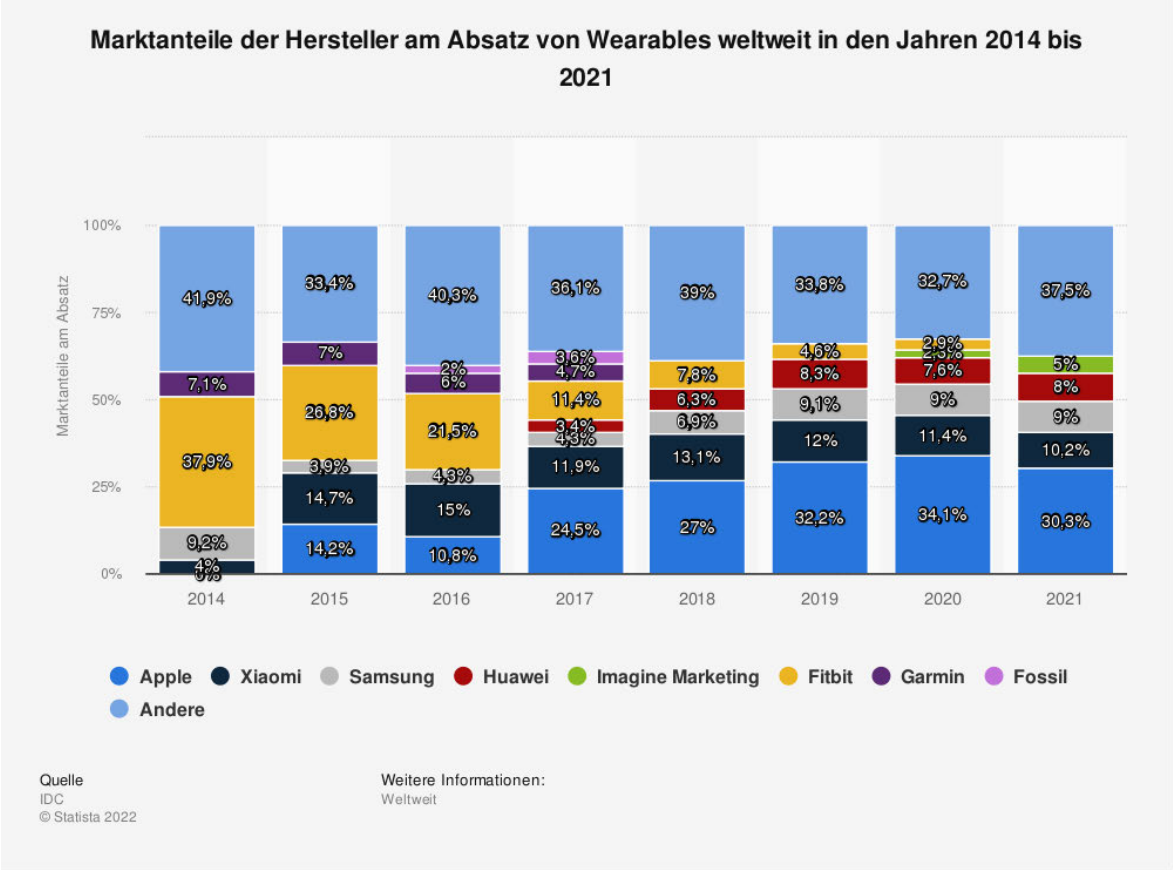


Abbildung 5: Marktanteile der Hersteller am Absatz von Wearables weltweit in den Jahren 2014 bis 2021 [23]

2.3 Elektronische Bauelemente

Dieses Teilkapitel gibt einen Überblick über die Grundlagen der elektronischen Bauelemente, die im Rahmen der Bachelorarbeit eine wichtige Rolle einnahmen. Es werden nachfolgend Begrifflichkeiten erklärt und Funktionsweisen erläutert.

2.3.1 System-on-a-Chip

Durch die immer besseren Fertigungsverfahren der Chiptechnik und der dadurch größeren Anzahl an Transistoren pro Chip ist es möglich geworden, ein komplettes System auf einem Chip zu entwickeln, welches viele verschiedene Funktionen vereint. Ein System, welches früher in mehreren Chips auf einer Platine untergebracht war, kann somit in einem einzigen Chip integriert werden. Solch ein auf einem Chip integriertes System wird System-on-a-Chip (SoC) genannt. Ein SoC bringt viele Vorteile. Neben einem niedrigen Energieverbrauch ist die erhöhte Kommunikationsgeschwindigkeit der Schaltungen aufgrund der Integrationsdichte vieler Komponenten von großem Vorteil. Die Kontrolle des

Gesamtsystems sowie die Ausführung des Softwareteils wird bei einem SoC durch spezielle Prozessoren (CPUs) übernommen. Diese unterscheiden sich gegenüber herkömmlichen in Computern verbauten CPUs in einigen Aspekten. Neben einem niedrigen Energieverbrauch, der in Mobilgeräten unerlässlich ist, sind die CPUs in SoC´s nicht auf Leistung ausgelegt, da andere Komponenten die eigentlichen Aufgaben übernehmen [24]. Die Komponenten eines SoC sind dabei über einen internen Bus oder eine Punkt-zu-Punkt-Verbindung (PzP) miteinander und somit auch mit der CPU verbunden [25]. Die Abbildung 6 veranschaulicht das Konzept eines SoC. Über den internen Bus werden dabei die Einzelkomponenten wie Prozessor, Speicher (ROM, EEPROM, Flash etc.), Arbeitsspeicher (RAM) und Funktionen wie Energiemanagement miteinander verbunden und durch die CPU gesteuert.

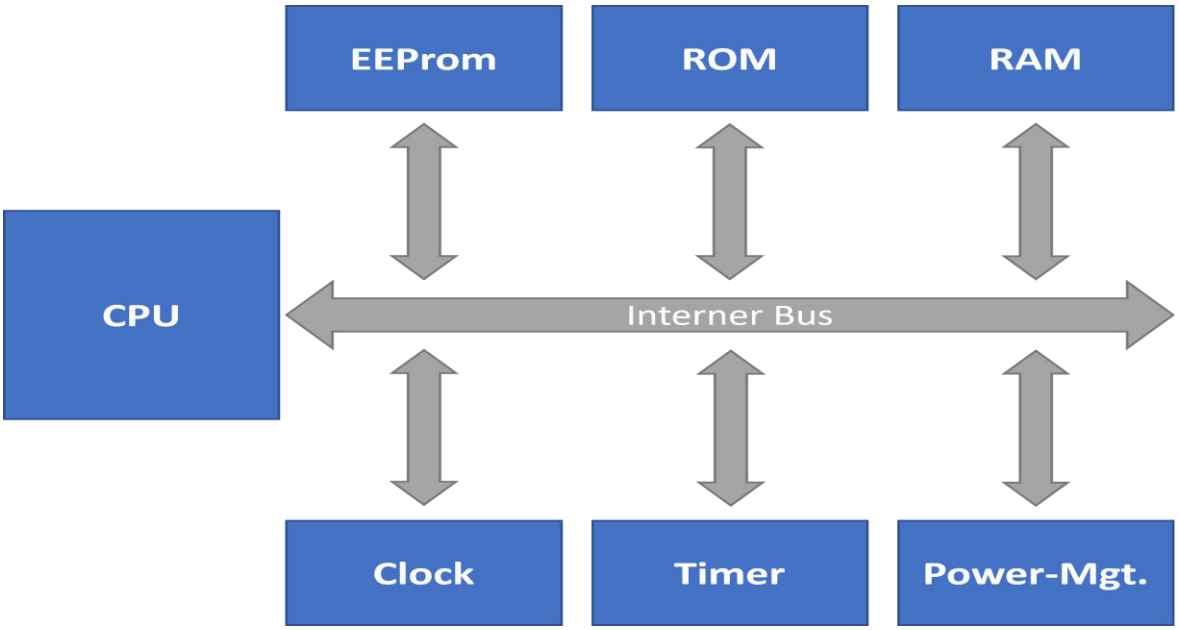


Abbildung 6: System-on-a-Chip Konzept (Eigene Darstellung basierend auf [25])

2.3.2 Flash-Speicher

Aus der technischen Entwicklung lässt sich ableiten, dass längerfristig Speicher mit direktem Zugriff bisher bestehende Speicher mit mechanischen Zugriffstechniken wie Bänder oder Platten ablösen werden. Die üblichste Bauform für Speicher mit direktem Zugriff sind sogenannte Halbleiterspeicher. Der sogenannte Flash-Speicher ist solch ein persistenter Halbleiterspeicher, der eine Lebensdauer von 10 Jahren mit vielen tausenden Lese-Schreibvorgängen erlaubt [26]. Grundlegend stellen die Eigenschaften von Flash-Speichern einen Kompromiss zwischen anderen Speichertechnologien wie z.B. EEPROM-Speichern (Electrically Erasable Programmable Read-Only Memory) in Bezug auf Kosten und Funktionalität dar. Ein Flash benutzt, wie ein EEPROM, eine elektrische Löschtechnik, die es ermöglicht, den Speicher innerhalb weniger Sekunden zu löschen. Der Unterschied besteht nun darin, dass bei Flash-Speichern immer nur bestimmte Blöcke bzw. Sektoren anstatt des kompletten Speichers mit einmal gelöscht werden können. Sektoren stellen dabei oft ein Viertel / ein Achtel / ein Sechzehntel etc. der Gesamtkapazität dar. Ein Löschen auf

Byte-Ebene ist bei Flash-Speichern grundsätzlich nicht möglich [27]. Hinzu kommt, dass sich Flash-Speicher im Gegensatz zu EEPROM-Speichern durch eine hohe Speicherdichte und schnelle Schreibvorgänge auszeichnen. Zum Abspeichern größerer Datenmengen sind diese also optimal geeignet [28]. Grundlegend wird zwischen zwei verschiedenen Speichertypen unterschieden: dem NOR-Flash-Speicher und dem NAND-Flash-Speicher.

Bei **NOR-Speichern** ermöglicht die Anordnung von Bit- und Word-Leitung die bitweise Ansteuerung der *Gates*, also der Speicherzellen. Beim Lesevorgang von Speicherzellen können diese durch die vielen Anordnungen der Leitungen zügig gelesen werden. Im Gegensatz zum Lesen ist das Beschreiben der Zellen jedoch ein zeitliches Problem, da jede Zelle bitweise angesteuert und beschrieben werden muss. Zusammengefasst zeichnet sich die NOR-Speichertechnologie durch schnelle Lesezeiten und langsame Schreibzeiten aus und ist dort geeignet, wo schnelles Lesen unabdingbar ist, beispielsweise in Programmspeichern von SoC´s [28].

Im Gegensatz zu NOR-Speichern können bei **NAND-Speichern** die einzelnen Speicherzellen nicht direkt gelesen werden, sondern immer nur im Verbund als ganze Zelle. Diese Serienschaltung der Speicherzellen hat zur Folge, dass der Ladungsträgerfluss zum Aufbau beim Lesevorgang wesentlich mehr Zeit in Anspruch nimmt als bei NOR-Speichern. NAND-Speicher sparen zudem eine Menge an Anschlüssen untereinander, so dass sie deutlich kleiner ausfallen als NOR-Speicher und die Schreibvorgänge deutlich schneller ablaufen als beim bitweisen Beschreiben. Zusammengefasst werden NAND-Speicher überall da eingesetzt, wo eine hohe Speicherdichte und Schreibgeschwindigkeit benötigt wird und die Lesegeschwindigkeit nicht im Vordergrund steht, beispielsweise in SD-Karten oder Memorysticks [28].

In der Abbildung 7 können die Funktionsweisen beider Speichertypen anschaulich betrachtet werden.

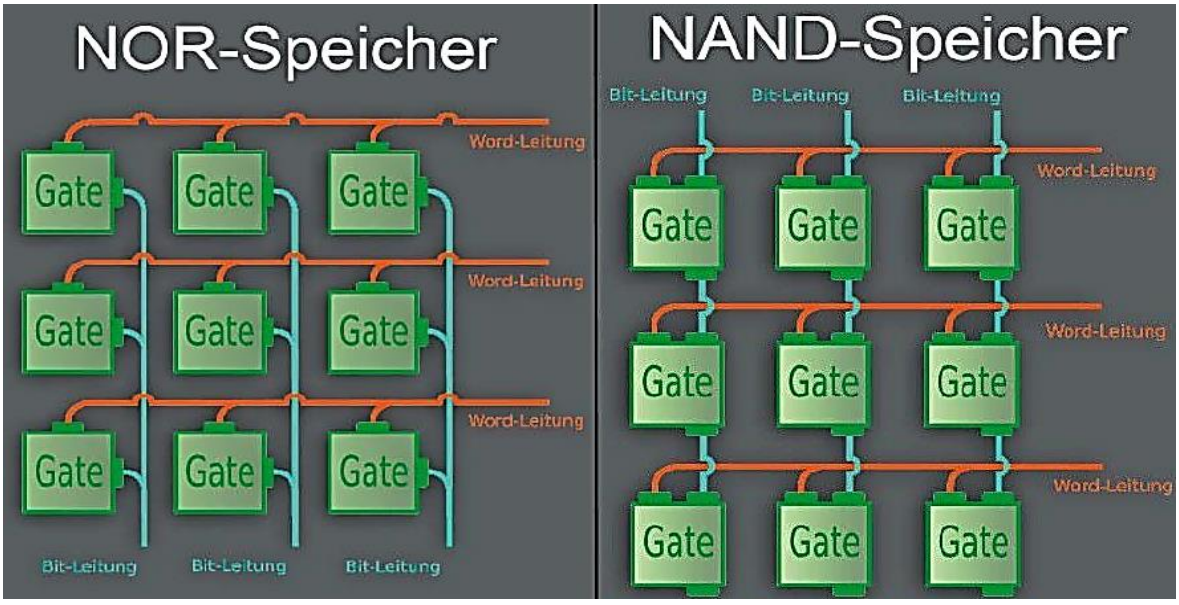


Abbildung 7: NOR- vs. NAND-Flash-Speicher [29]

2.4 Secure-Shell-Protocol

Das „***S**ecure-**SH**ell-Protocol“* (SSH) ist ein zum Administrieren von Unix-basierten Servern eingesetztes Netzwerkprotokoll. Die Abkürzung SSH setzt sich dabei aus den Wörtern *Secure* (engl. = *secure,* dt. = sicher) und *Shell* (engl. = *shell,* dt. = Schale oder Muschelschale) zusammen. In der Informatik wird der Begriff für die äußere „Schale“ eines Betriebssystems über die der Nutzer mit diesem kommunizieren kann, verwendet. Die ursprünglich 1995 erschienene Version von SSH1.0 wurde über die Jahre von SSH1.3 und SSH1.5 weiterentwickelt und schließlich durch SSH2.0 ersetzt, mit welchem heutzutage alle modernen Anwendungen arbeiten [30].

2.4.1 Funktionsweise

SSH wird hauptsächlich in geschlossenen Administratorumgebungen eingesetzt, in der jeder Admin nur eine definierte Anzahl an Servern zu betreuen hat [30]. Für die Kommunikation benutzt SSH ein paket-orientiertes binäres Protokoll, welches auf Port 22, einem offiziell dafür reservierten Port, auf Verbindungen wartet [31]. Für einen sicheren Verbindungsaufbau werden bei SSH typischerweise öffentliche Schlüssel und Passwörter benutzt [30]. Die Authentifikation findet sowohl Server- als auch Client seitig statt. Man unterscheidet zwischen der Server- und Client-Authentifikation.

Server-Authentifikation: Der SSH-Client eines Nutzers identifiziert einen Server über dessen öffentlichen Schlüssel und digitale Signatur. Hierbei benötigt der Client den zum administrierten Server passenden öffentlichen Schlüssel, um damit die ausgetauschte Signatur während des Verlaufs eines Handshakes zu verifizieren. Ist der vom Server während des Handshakes gesendete öffentliche Schlüssel beim Client in der Liste der vertrauenswürdigen Schlüssel gespeichert, so läuft die Authentifikation des Servers ohne Mithilfe des Nutzers ab. Andernfalls muss der Client entscheiden, ob der neue Schlüssel in die Liste aufgenommen wird oder nicht. Der Server selbst authentifiziert sich dann durch die digitale Signierung wichtiger Parameter des Handshakes, die auch den ausgehandelten Schlüssel beeinflussen [30].

Client-Authentifikation Gegenüber einem Server authentifiziert sich der Client über ein verschlüsselt übertragenes Passwort oder über einen öffentlichen Schlüssel mit entsprechender digitaler Signatur. Für die erfolgreiche Client-Authentifikation müssen sowohl Passwort als auch öffentlicher Schlüssel manuell auf den administrierenden Servern eingetragen werden [30].

Anstelle der Authentifizierung über öffentlichen Schlüssel und Passwort, kann der Verbindungsaufbau auch über Schlüsselpaare erfolgen. Ein SSH-Schlüsselpaar besteht aus einem öffentlichen- und einem privaten Schlüssel. Da diese immer zusammen generiert werden, passt jeder öffentliche Schlüssel auch nur zu dem privaten Schlüssel, mit dem er zusammen erzeugt wurde. Der öffentliche Schlüssel wird dabei wie bei der bereits zuvor erläuterten Methode, auf dem System hinterlegt, wo sich ein Client hin verbinden möchte. Ein

Client mit privatem Schlüssel hat folglich nur Zugang zu den Systemen, wo der passende öffentliche Schlüssel hinterlegt ist. Der private Schlüssel nimmt somit eine zentrale Rolle ein und sollte besonders geschützt werden [32].

2.4.2 Secure File Transfer Protocol

Das sogenannte *Secure File Transfer Protocol* (SFTP) ist das Standard-Dateiübertragungsprotokoll für die Verwendung mit dem SSH-, genauer SSH2.0-Protokoll. Es sorgt für eine sichere Dateiübertragung, die über einen vertraulichen Datenstrom abgewickelt wird. Neben der Datenübertragung, für welches das Protokoll in erster Linie dient, kann es auch zum allgemeinen Zugang auf das Dateisystem eines FTP-Servers (File Transfer Protocol-Server) verwendet werden [33]. SFTP ist eine verschlüsselte Alternative zum FTP und wird zusätzlich wie auch SSH2.0 auf Port 22 angeboten [34]. Das Protokoll läuft über einen sicheren Kanal, in denen keinerlei Informationen im Klartext übertragen werden. Solche Informationen sind beispielsweise Kennwörter oder Dateiinformationen [33].

Die grundlegende Funktionsweise kann in Abbildung 8 nachvollzogen werden. Wie zu erkennen, ist die Verbindung zwischen dem FTP-Client und FTP-Server verschlüsselt (engl. = *encryption*, dt. = Verschlüsselung; engl. = *decryption*, dt. = Entschlüsselung). Ausschließlich über diese verschlüsselte Verbindung, auch SSH-Tunnel genannt, werden die Daten von und zu dem Client transportiert. Um die Identität des Servers bei einer SFTP-Verbindung sicherzustellen, übermittelt der FTP-Server vor dem Verbindungsaufbau einen kryptografischen Fingerprint seines öffentlichen Server-Schlüssels, welchen er mittels seines privaten Schlüssels generiert hat. Verbindet sich ein Client erstmalig mit dem Server, so ist der Schlüssel dem Client-Programm noch nicht bekannt und muss dahingehend vom Nutzer bestätigt werden. Der bestätigte Schlüssel wird dann lokal gespeichert und kann somit bei jedem neuen Verbindungsaufbau für die Verifizierung des Servers verwendet werden, um auszuschließen, dass jemand „mitlauscht“ [33].

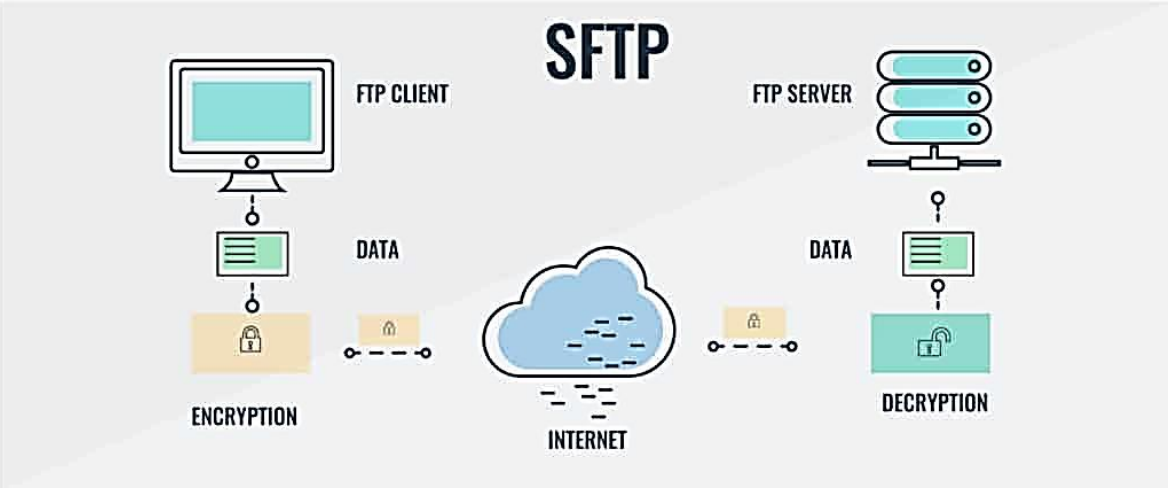


Abbildung 8: Funktionsweise SFTP [35]

3 Material und Methoden

In diesem Kapitel soll auf die verwendeten Materialen und angewandten Methoden geblendet werden. Beginnend mit dem Versuchsaufbau wird systematisch im Anschluss versucht, die benutzte Hard- und Software in Bezug auf die angewandten Methoden zu beschreiben. Ferner wird das Untersuchungsbetriebssystem *LineageOS* vorgestellt, die IT-Forensische Sicherung der Daten, Mikrochips und Adapter sowie die Extraktion der ermittlungsrelevanten Daten thematisiert.

3.1 Versuchsaufbau

Bevor auf die Materialen und Methoden näher eingegangen wird, ist es angebracht, einen groben Überblick über den Versuchsaufbau zu geben. Man unterscheidet zwischen zwei verschiedenen Aufbauausführungen. Die Abbildung 9 veranschaulicht die erste, für das Teilkapitel 3.5.1 notwendige Ausführung des Versuchsaufbaus. Der Arbeitsplatz besteht zum einen aus einem Untersuchungsgerät in Form eines Laptops (links) mit entsprechender Software und Peripherie, zum anderen aus zwei *Raspberry Pi's* (mittig), die für die Untersuchung *Android* Geräte simulieren. Diese sind mit einem entsprechenden Bildschirm und weiterem Zubehör ausgestattet. Als letzter zu erwähnender Versuchsgegenstand sind die jeweils zu untersuchenden Fitnesstracker/Fitness-Smartwatches (rechts) zu nennen.

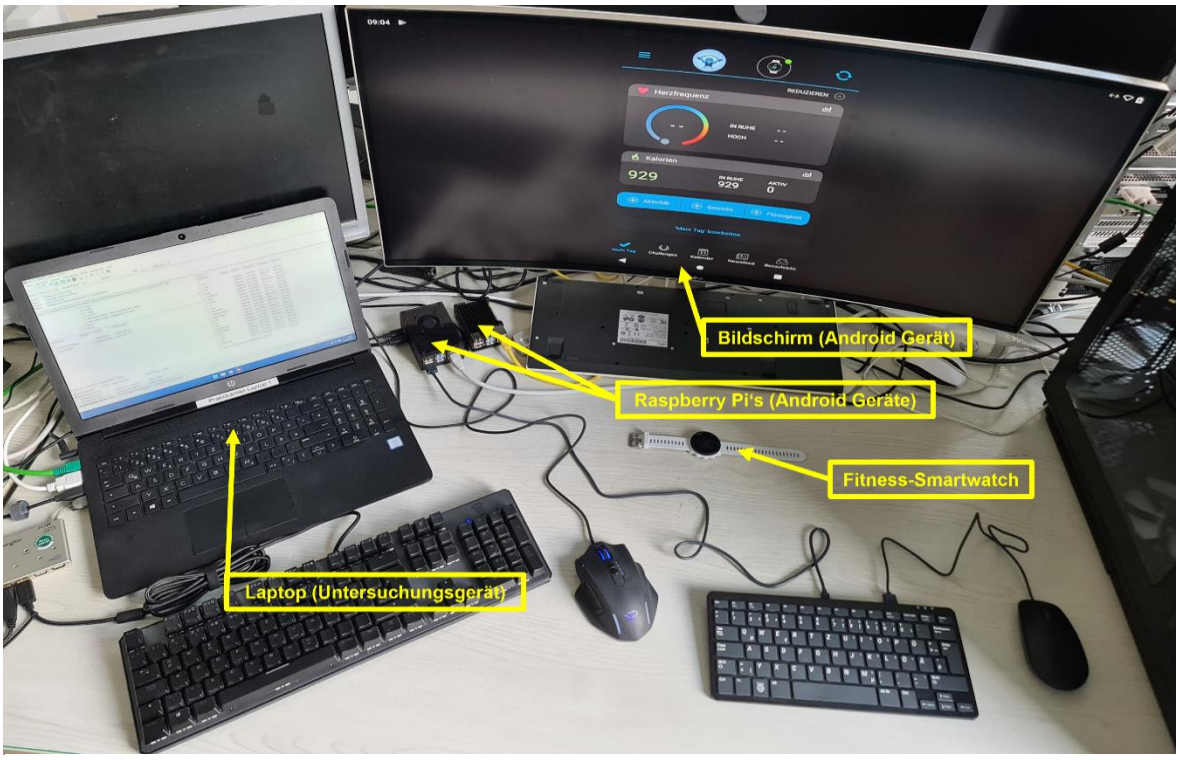


Abbildung 9: Versuchsaufbau – Logische Sicherung - SFTP (Eigene bearbeitete Aufnahme, Juni 2022)

Im Gegensatz zur Abbildung 9 veranschaulicht die Abbildung 10 die zweite, für das Teilkapitel 3.5.2 notwendige Ausführung des Versuchsaufbaus. Neben einem Stereomikroskop mit entsprechender Kaltlichtquelle (rechts) sind ebenfalls eine Heißluftstation (links hinten), Vergrößerungslampe (links vorne), hitzeresistente Unterlage (mittig hinten) sowie Feintools (rechts) und der zu untersuchende Fitnesstracker (mittig vorne) am Arbeitsplatz gegeben.

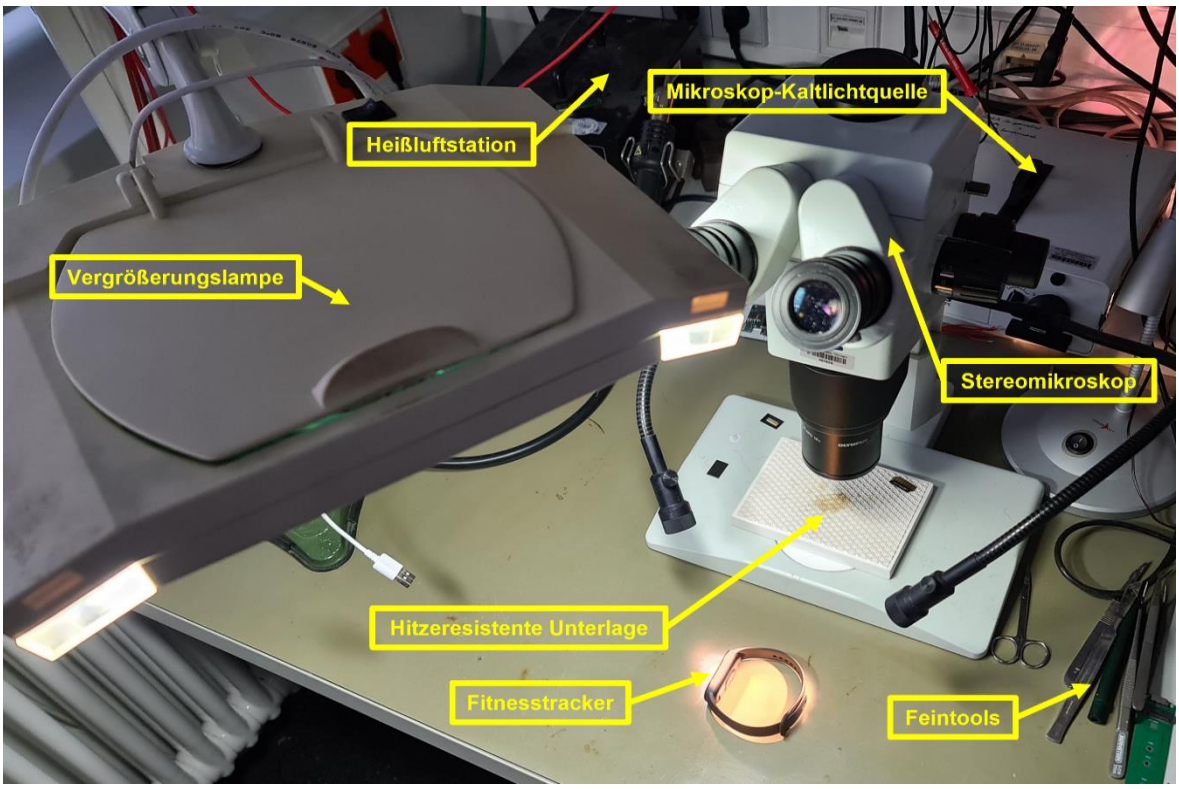


Abbildung 10: Versuchsaufbau – Chip-Off-Analyse (Eigene bearbeitete Aufnahme, Juni 2022)

3.2 Hardware

Zunächst gibt dieses Teilkapitel einen Überblick über die während des Bachelorprojektes verwendete Hardware. Es werden zudem Geräte vorgestellt und ihre Funktionen betrachtet.

Xiaomi Mi Smart Band 6

Das *Xiaomi Mi Smart Band 6* ist ein Fitnesstracker der chinesischen Firma *Xiaomi*. Er wurde am 30. April 2021 in Europa vorgestellt und ist das erste Untersuchungsobjekt [36]. Der 12,8g schwere Fitnesstracker besteht im Wesentlichen aus einer Display-Einheit und einem Silikonarmband, in welchen das Gehäuse eingesetzt ist und wieder herausgenommen werden kann. Das Display ist ein 1,56 Zoll großes AMOLED (Active Matrix Organic Light Emitting Diode) Display mit einem 152 x 486 Pixel großen Touchscreen. Als Verbindungstechnologie kommt *Bluetooth* 5.0 zum Einsatz. Laut Herstellerangaben hält der eingebaute 125mAh Akku bis zu 14 Tage. Die Display Einheit ist zudem gegen einen Wasserdruck von bis zu 5 ATM (506,625 kPa) geschützt. Wichtige Funktionen des Fitnesstrackers sind:

Musiksteuerung, Schrittzähler, Schlafüberwachung, Pulsmesser, Wecker, Nachrichtenerinnerungen, Anrufablehnung, Sporttracking mit 30 Sportmodi, Blutsauerstoffmessung etc. [37]. In der Abbildung 11 ist der verwendete Fitnesstracker von allen Seiten abgebildet.

Abbildung 11: *Xiaomi Mi Smart Band 6* (Eigene zusammengeschnittene Aufnahmen, Mai 2022)

Fitbit Inspire 2

Das zweite Untersuchungsobjekt ist ein Fitnesstracker der US-amerikanischen Firma *Fitbit*. Er wurde am 25. September 2020 weltweit vorgestellt und trägt den Namen *Fitbit Inspire 2* [38]. Ähnlich wie das erste Untersuchungsobjekt, bietet der Fitnesstracker viele Spezifikationen und Funktionen. Laut Herstellerangaben ist ein Dreiachsiger Beschleunigungssensor, ein optischer Herzfrequenzmesser (vgl. Teilkapitel 2.2.2) sowie ein Vibrationsmotor verbaut. Die Akkulaufzeit beträgt bis zu 10 Tage. In Bezug auf die Wasserfestigkeit ist der Fitnesstracker bis zu einer Tiefe von 50 Meter tragbar. Wichtige Funktionen sind unter anderem: kontinuierliche Herzfrequenzmessung, Ruhefrequenz, Aufzeichnung der Hauttemperatur, Bewegungserinnerung, Schlafaufzeichnung, Wecker, Stoppuhr sowie verschiedene Sportmodi wie Schwimm- oder Lauftracking [39]. Die Abbildung 12 veranschaulicht den untersuchten Fitnesstracker von allen Seiten.

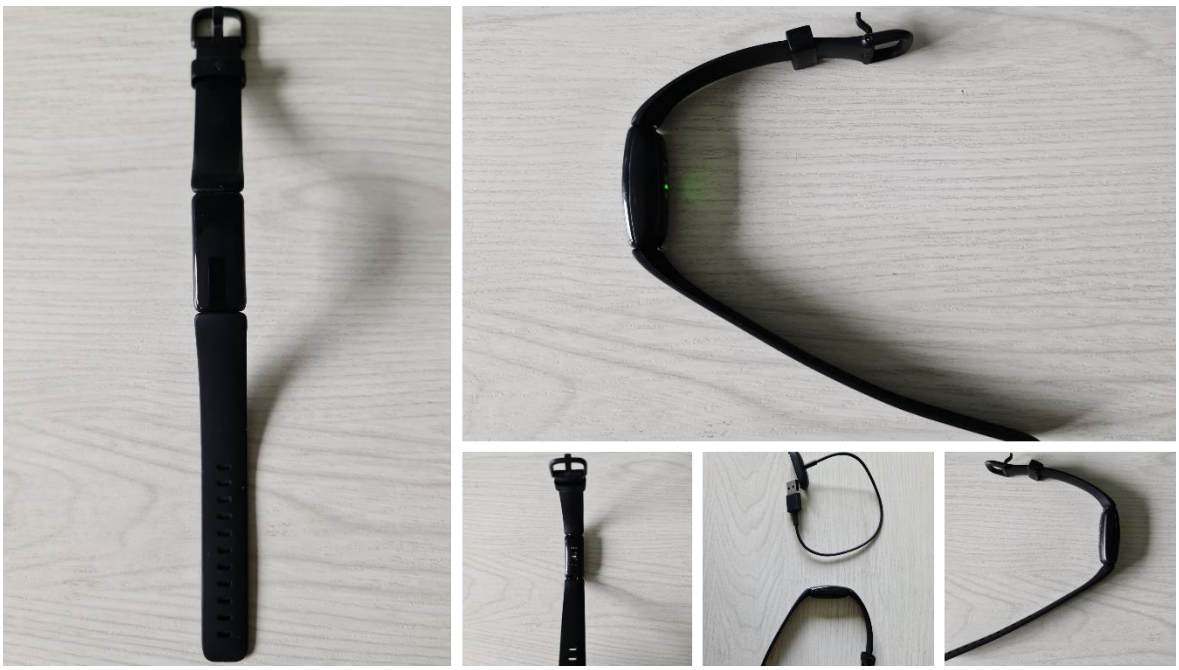


Abbildung 12: *Fitbit Inspire 2* (Eigene zusammengeschnittene Aufnahmen, Mai 2022)

Garmin Forerunner 55

Als drittes und einziges Untersuchungsobjekt ist die *Garmin Forerunner 55* des US-amerikanischen Unternehmens *Garmin* eine Fitness-Smartwatch. Diese wurde am 2. Juni 2021 weltweit vorgestellt und unterscheidet sich durch ihre Spezifikationen und Funktionen deutlich von den bereits vorgestellten Fitnesstrackern [40]. Als einzige besitzt die Fitness-Smartwatch einen GPS-Sensor, mit dem die Funktionsanzahl deutlich erweitert werden kann. Laut dem Hersteller wird das 1,04 Zoll große Display mit einer Auflösung von 208 x 208 Pixeln durch ein chemisch verstärktes Glas geschützt. Die Batterielaufzeit beträgt bis zu zwei Wochen mit Ausnahme des GPS-Modus, bei welchem die Uhr nur eine Laufzeit von bis zu 20 Stunden aufweist. Wie das *Xiaomi Mi Smart Band 6* besitzt die *Garmin Forerunner 55* eine Wasserdichtigkeit von 5 ATM (506,625 kPa). Ausgehend vom Teilkapitel 2.2.1 zeichnet sich die *Garmin Forerunner 55* als Fitness-Smartwatch durch eine Reihe Smartphone ähnlicher Funktionen (Kalender-, Wetter-, Musik-, Telefonsuchfunktion etc.) aus. Die Fitness-Smartmatch besitzt aber auch typische Uhrfunktionen, wie z.B.: Uhrzeit- und Datumsanzeige, Wecker, Timer, Stoppuhr. Besonders hervorzuheben sind die Gesundheitsüberwachungsfunktionen die neben der Herzfrequenz- sowie der Atemfrequenzmessung auch eine Schlafüberwachung umfassen. Als größte Funktionsbreite bietet die *Garmin Forerunner 55* unzählige Sportfunktionen wie: Schwimmfunktionen, Radfahrfunktionen, Laufunktionen etc., die mittels des GPS-Sensor feingranular aufgezeichnet werden können [41]. Die Fitness-Smartwatch ist in der Abbildung 13 von allen Seiten abgebildet.

Abbildung 13: *Garmin Forerunner 55* (Eigene zusammengeschnittene Aufnahmen, Mai 2022)

Raspberry Pi 4 Model B

Der *Raspberry Pi 4 Model B* ist hingegen ein kleiner Einplatinencomputer, welcher sich für verschiedene Aufgaben anbietet. Er kann zum einen als Desktop-Ersatz für beispielsweise einfache Office-Anwendungen, zum anderen als Server, Konsole sowie Dateisystemträger für verschiedenste Projekte verwendet werden. Über zwei Micro-HDMI-Ports (High Definition Multimedia Interface) kann man bis zu zwei UHD-Monitore (Ultra-High-Definition) anschließen. Als Prozessor besitzt der *Raspberry Pi 4 Model B* einen 1,5GHz schnellen *ARM-Cortex-A72 Quad Core*. Beim Arbeitsspeicher wird zwischen 1, 2, 4 oder 8 GB LPDDR4 (Low-Power Double Data Rate 4) SDRAM (Synchronous Dynamic Random Access Memory) unterschieden. Integriert sind zudem ein ac-WLAN- und *Bluetooth*-5.0-Adapter. Die Anschlussmöglichkeiten erstrecken sich über vier USB-Buchsen (2 x USB 3.0, 2 x USB 2,0), eine USB-Typ-C-, Ethernet-LAN- (Local Area Network) sowie Micro-SD-Karten-Schnittstelle. Über die letztere wird das auf der Micro-SD-Karte befindliche Betriebssystem, Skript etc. mit der Hardware in Verbindung gebracht [42]. Der Aufbau sowie die Anschlussmöglichkeiten sind nochmals in der Abbildung 14 veranschaulicht. In der Abbildung 9 sind zudem die im Rahmen der Untersuchung verwendeten *Raspberry Pi´s* zu sehen.

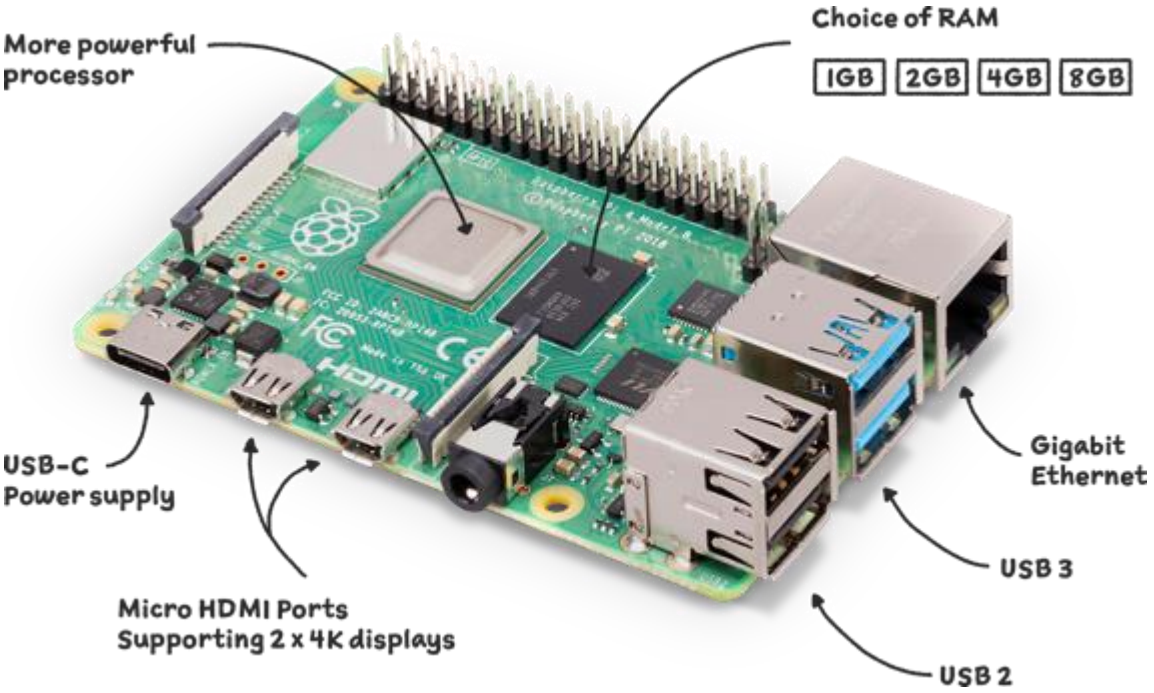


Abbildung 14: Aufbau - *Raspberry Pi 4 Model B* [43]

HP Laptop – *15-da0402ng*

Der für die Untersuchung verwendete Laptop ist ein 15,6 Zoll Notebook (vgl. Abbildung 9) des US-amerikanischen Herstellers *HP Inc*. Er verfügt über ein Intel Core i5-8250U (3,4GHz), 8 GB DDR4 SDRAM sowie einer 1 TB HDD mit SATA Schnittstelle. Externe Anschlussmöglichkeiten sind in Form eines SD-Kartenlesers, 2 x USB 3.1 Gen 1, 1 x USB 2.0, 1 x HDMI, 1 x RJ-45 sowie eines kombinierten Kopfhörer/Mikrofon Anschlusses gegeben [44].

Olympus SZX9 Forschungsstereomikroskop

Für das Betrachten kleiner Objekte, die mit dem bloßen Auge nicht sichtbar sind, wird das Forschungsstereomikroskop vom Typ SZX9 des japanischen Herstellers *Olympus* verwendet. Es besitzt einen Gesamtvergrößerungsbereich von 6,3x bis 57x und ist somit ideal für die medizinische, biologische und vor allem die forensische Forschung geeignet [45]. Die Ausleuchtung des Vergrößerungsbereiches übernahm die dazugehörige Kaltlichtquelle *HIGHLIGHT 3100* von *Olympus*, wie die Abbildung 10 bereits veranschaulichte.

TOOLCRAFT AT850D Heißluftstation

Zum Löten/Entlöten von Mikrobauteilen sowie zum Erwärmen von Kunststoffen wird die *TOOLCRAFT AT850D* Heißluftstation verwendet (Abbildung 10). Mit Hilfe der Station ist es schnell möglich, Luft-Temperaturbereiche von 100 bis 480 Grad Celsius einzustellen und diese konstant zu halten, um somit entsprechend den Herstelleranforderungen die Bauteile zu behandeln. Durch eine Hochleistungs-Membranpumpe mit hohem Druck ist es ferner möglich, mittels verschiedener Düsen, ein Fördervolumen von bis zu 23 l/min einzustellen.

Die Station verfügt zudem über eine digitale Anzeige, die die Soll- und Ist-Temperatur anzeigt [46].

Interflux IF 8300

Unterstützend zum Löten/Entlöten mittels der vorgestellten Heizstation wird das „no-clean“, halogen- und kolophoniumfreie Lötflussmittelgel des belgischen Herstellers *Interflux* verwendet. Die Rückstände nach dem Löten sind transparent und minimal, so dass keine Reinigung erforderlich ist („no-clean“). Das Flussmittelgel ist in verschiedenen Viskositäten verfügbar, die jeweils unterschiedliche Flammpunkte und Dichten aufweisen. Das *IF 8300* kann mittels drucken, dosieren, tauchen oder mit einer dazugehörigen Bürste auf das Objekt aufgetragen werden [47].

BeeProg2

Der *BeeProg2* ist ein professionelles Programmiergerät der slowakischen Firma *Elnec*, welches im Rahmen der Untersuchung für das Einlesen der Speicherchips verwendet wird. Das Programmiergerät wurde speziell auf die schnellere Programmierung von Speicherchips wie NAND-Speicher (vgl. Teilkapitel 2.3.2) entwickelt und unterstützt zudem alle Arten von programmierbaren Chips vom EEPROM bis zum Microcontroller. Passen die Chips nicht direkt in das 48-Pin-Gehäuse, so gibt es eine Reihe an Adaptern, die für spezielle Gehäuseformen erhältlich sind (vgl. Teilkapitel 3.6.3) [48].

3.3 Software

Im folgenden Teilkapitel wird ein Überblick über die im Bachelorprojekt verwendete Software gegeben.

Raspberry Pi Imager

Um Micro-SD-Karten für einen *Raspberry Pi 4 Model B* mit einem entsprechenden Betriebssystem zu beschreiben, ist es nötig, auf spezielle Tools zurückzugreifen, die dies umsetzen können. Im Rahmen der Untersuchung wurde das *Raspberry Pi* eigene Imaging-Dienstprogramm mit dem Namen *Raspberry Pi Imager* (Version 1.7.2) verwendet. Die freie Software ermöglicht durch seine übersichtliche grafische Oberfläche eine leichte Bedienung. Eine weitere Besonderheit ist, dass das Tool in den Betriebssystemen *Windows, macOS* und *Linux* verwendet werden kann und somit Betriebssystem spezifische Methodiken auf Micro-SD-Karten zuzugreifen sowie diese zu beschreiben, in einem Programm vereint sind [49].

DB Browser for SQLite

Die freie Software *DB Browser for SQLite* ist ein visuelles, qualitativ hochwertiges Tool zum entwerfen, erstellen und bearbeiten verschiedenster Datenbankendateien, die mit *SQLite* kompatibel sind. Das Tool zielt dabei auf Benutzerfreundlichkeit für einfache Endbenutzer als auch Entwickler ab, die die genannten Aufgaben mit Datenbanken erledigen möchten.

Die Oberfläche ähnelt dabei einer Art Tabellenkalkulationsprogramm und ist somit keine visuelle *Shell* für *SQLite*. Der Anspruch der Entwickler war dabei, das Tool auch ohne Kenntnisse für *SQLite* und der dazugehörigen Befehle einfach anwenden zu können [50]. Im Rahmen der Untersuchung wurde das Tool (Version 3.12.2) vor allem zum Durchsuchen von Datenbankdateien verwendet.

PyCharm

PyCharm ist eine sogenannte *Integrated Development Environment* (engl. Abk. = *IDE*; *dt*. = integrierte Entwicklungsumgebung) der Firma *JetBrains*. Die Entwicklungsumgebung ist für die Programmiersprache *Python* entwickelt wurden und existiert in einer quelloffenen Community Edition sowie einer proprietären Professional Edition [51]. Erstere (Version 2022.1.3) wurde im Rahmen der Untersuchung zum Schreiben eines hilfreichen Python Skriptes verwendet, welches in der Anlage Teil 3 zu finden ist. Dabei verfügt die IDE über einige nützliche Funktionen, die während der Programmierung hilfreich waren: Code-Refaktorierung nach *PEP 8* [52], Codevervollständigung, Code-Inspektion, Code-Navigation sowie Fehlerhervorhebung in Echtzeit mit Lösungsvorschlägen. Zudem verfügt *PyCharm* über ein eingebautes *Terminal* zum Ausführen von Befehlen (Installieren von Paketen, Ausführen von Skripten etc.), einen integrierten *Python-Debugger* zum Nachvollziehen von Funktionsweisen und Fehlern sowie einem *Test-Runner* zum Testen von Konfigurationen [51].

FileZilla

Das Tool *FileZilla* ist ein schneller, zuverlässiger und plattformübergreifender FTP-, FTPS- und SFTP-Client. Die Software ist frei, quelloffen und mit einer intuitiven grafischen Benutzeroberfläche sowie vielen nützlichen Funktionen ausgestattet. Zu den Funktionen der Software gehören unter anderem: einfache Bedienung, FTP/FTPS/SFTP Unterstützung, plattformübergreifende Nutzung, IPv6-Unterstützung, Verfügbarkeit in vielen Sprachen sowie die Übertragung und Wiederaufnahme von Dateien größer als 4 GB [53]. Neben der normalen Version gibt es eine *FileZilla Pro* Version, die zusätzlich Protokolle für *Dropbox, Microsoft OneDrive, Google Drive, Amazon S3* etc. unterstützt [54]. Im Rahmen der Untersuchung stellte sich *FileZilla* (Version 3.60.1) als hilfreiches Tool zum Dateizugriff sowie Datenübertragung über SSH mittels SFTP heraus.

PG4UW

PG4UW ist ein gemeinsames Steuerprogramm für alle Programmierer der Firma *Elnec* [55]. In Bezug auf die Untersuchung wird die Software in Verbindung mit dem *BeeProg2* (vgl. Teilkapitel 3.2) verwendet. Das Steuerprogramm ist eine 32-Bit-Anwendung für *Microsoft Windows XP* bis *Windows 11* (32-Bit und 64-Bit). Das Zielgerät (Adapter + Speicherchip) kann in der Software nach seiner Klasse, dem Hersteller oder durch die Eingabe eines Teils des Herstellernamens und/oder einer Teilenummer ausgewählt werden. Neben den gerätebezogenen Standardbefehlen wie Lesen, Programmieren, Leerzeichenprüfung und Verifizieren sind ebenfalls einige Testfunktionen wie Einschubtests und Signatur-Byte-Prüfung

implementiert. Das Steuerprogramm erlaubt zudem Datenmanipulationen innerhalb/zwischen Dateien und Puffern sowie eine automatische Dateiformaterkennung und -konvertierung. Die Funktionsbreite wird durch Sonderfunktionen wie dem sofortigen Start nach Einsetzen des Chips in den Sockel abgerundet. Die Bedienung ist durch die grafische Oberfläche mit Pull-Down-Menü, durch Hotkeys sowie einer Online-Hilfe vereinfacht möglich [55].

VISUAL NAND RECONSTRUCTOR

VISUAL NAND RECONSTRUCTOR (VNR) ist eine benutzerfreundliche und intuitive Software mit vereinheitlichten Funktionen zur Datenwiederherstellung sowie -analyse von NAND-Speichern der polnischen Firma *ruSolut*. Das Tool verfügt über eine integrierte Datenbank mit NAND-Chip- und Kontroller-Konfigurationsdaten und bietet somit eine Lösung für die meisten bisher bekannten Chips. Integrierte automatische Analysemodi vereinfachen die Datenwiederherstellung der zu untersuchenden NAND-Flash-Speicher. Einzigartig und relevant für die Untersuchung sind die Modi der Datenvisualisierung, die mittels mehrstufiger Bildstrukturbeschreibung das *Reverse Engineering* wesentlich erleichtern. Zuletzt verfügt das Tool auch über einen speziellen *Scrambler* der mittels eines *XOR*-Extraktionsmodus die Entschlüsselung von Daten aus verschlüsselten Chips unterstützen kann [56].

HxD

HxD ist ein kostenloser und schneller Hex-Editor, der neben der Verarbeitung beliebiger Dateien egal welcher Größe, auch das direkte Bearbeiten von Datenträgern sowie die Veränderung von Arbeitsspeichern (RAM) unterstützt. Durch die leicht zu bedienende grafische Oberfläche werden dem Nutzer übersichtlich Funktionen wie: Suchen und Ersetzen, Export in diverse Dateiformate, Einfügen von Byte-Mustern, Prüfsummen/Digests, Zusammenfügen oder Aufspalten von Dateien, einen „Datei-Reißwolf“ und vieles mehr angeboten. Hauptvorteil des Editors ist seine Schnelligkeit im Umgang mit den zu analysierenden Dateien [57].

binwalk

Das Tool *binwalk* ist ein unter *Linux* und *Windows* ausführbares Werkzeug zum Durchsuchen von Binärabbildern (.bin-Dateien) nach ausführbaren Code und eingebetteten Dateien. Es wurde insbesondere für die Identifizierung von Code und Dateien aus Firmware-Images konzipiert [58]. Das Tool ist in der Programmiersprache *Python* geschrieben und benötigt zum Ausführen daher die jeweilige Version. Welche Version benötigt wird, wie die Installation abläuft etc. kann auf der *GitHub*-Seite der Entwickler nachgelesen werden [59].

3.4 LineageOS

Um Fitnesstracker und Fitness-Smartwatches untersuchen zu können, ist es nötig, eine Untersuchungsumgebung aufzubauen, um die Verbindung zu Mobilgeräten nachzustellen. Für die Untersuchung wird daher der aus Teilkapitel 3.2 vorgestellte *Raspberry Pi 4 Model B* entsprechend mit einem Betriebssystem verknüpft, welches mit den Fitnesstrackern/Fitness-Smartwatches kompatibel ist. Dabei ist es naheliegend, ein Betriebssystem zu wählen, welches speziell für mobile Geräte entwickelt wurde. Für die Untersuchung fällt hier die Wahl auf das Betriebssystem *Android*. Das *Android*-Betriebssystem ist eine vollständig anpassbare mobile, freie und quelloffene Betriebssystem-Plattform und eignet sich dadurch sehr gut für Untersuchungen auf den unterschiedlichsten Medien [60]. Während die Frage nach dem Betriebssystem beantwortet wurde, bleibt noch offen, welche *Android* Version zu wählen ist. Die Abbildung 15 zeigt, welche *Android* Version am meisten genutzt wird. Die Statistik veranschaulicht die Anteile der verschiedenen *Android*-Versionen, gemessen an der Internetnutzung der Geräte, die im April 2022 ein *Android*-Betriebssystem installiert hatten. Es wird deutlich, dass sich *Android 11.0* mit 34,63% im Gegensatz zum neuen *Android 12.0* mit 11,77% mit einer Differenz von 22,86% an die Spitze absetzt. Der dazwischen liegende Vorgänger *Android 10.0* mit 23,26% kommt mit einer Differenz von 11,37% ebenfalls nicht in die Nähe der Spitze. Für die Untersuchung wird daher *Android 11.0* verwendet.

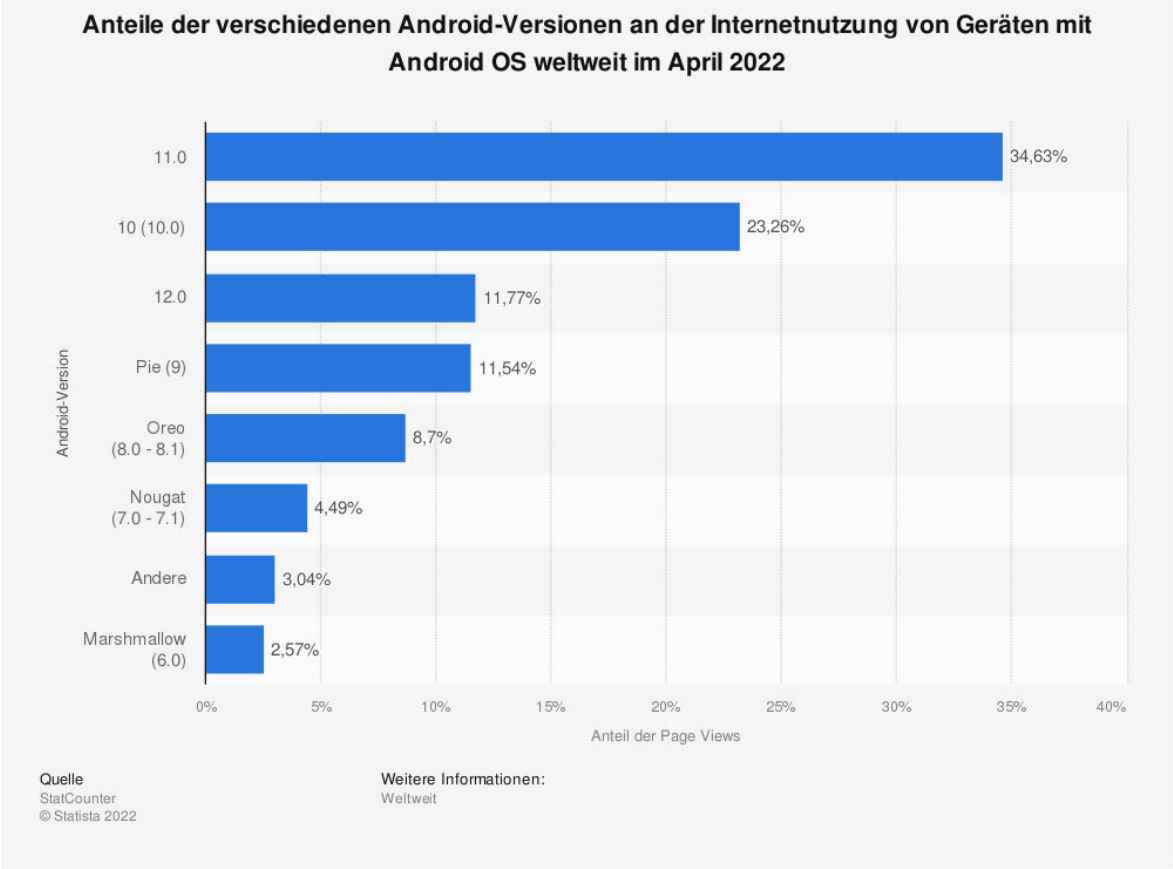


Abbildung 15: Anteile der verschiedenen *Android*-Versionen an der Internetnutzung von Geräten mit *Android* OS weltweit im April 2022 [61]

Mit Blick auf das Teilkapitel 3.2 wird deutlich, dass zur Untersuchung kein mobiles Endgerät in Form eines Smartphones oder Tablets, sondern ein Einplatinencomputer verwendet wird. Diesen Umstand muss man für die Einrichtung des *Android*-Betriebssystems beachten und ein extra für den *Raspberry Pi 4 Model B* ausgelegtes *Android* installieren. Für die Untersuchung wird auf das sogenannte *LineageOS* zurückgegriffen. *LineageOS* setzt sich aus dem englischen Wort *lineage* (dt. = Abstammung) und der Abkürzung *OS* (engl. = *operating system)* zusammen [62]. Es ist eine *Custom ROM*, eine Art alternatives Betriebssystem, welches den Nutzern verschiedene Möglichkeiten bietet, das System nach ihren Interessen zu verändern. *LineageOS* hat derzeit Ausführungen für 29 Geräte, von denen jede unterschiedliche Versionen aufweisen [60]. Speziell für den *Raspberry Pi* 4 wird durch den Entwickler Tuomas Kontio ein nicht kommerzielles, freies *Android 11* Betriebssystem mit dem Namen *LineageOS 18.1* zur Verfügung gestellt. Um die *Custom ROM* zu nutzen, wird ein Arbeitsspeicher von mindestens 2 GB benötigt [63]. Die Installation erfolgt über drei Schritte:

1. Herunterladen des Images im ZIP-Dateiformat über die Entwicklerseite;
2. mittels des Tools *Raspberry Pi Imager* das Image auf eine Micro-SD-Karte schreiben;
3. den *Raspberry Pi 4 Model B* starten und den Installationsanweisungen von *LineageOS 18.1* auf einem angeschlossenen Bildschirm folgen.

Nach erfolgreicher Installation kann *LineageOS 18.1* wie ein *Android 11* auf dem *Raspberry Pi 4 Model B* genutzt werden. Als einzige Besonderheit ist zu beachten, dass der Einplatinencomputer als *Android* Tablet interpretiert wird und man mit Blick auf die Teilkapitel 3.4.1 und 3.4.2 mit Einschränkungen in Bezug auf die App-Verfügbarkeit rechnen muss.

Zwar wird der *Android*-Quellcode unter einer Open-Source-Lizenz veröffentlicht, paradoxerweise werden jedoch die meisten *Android*-Geräte mit einer Kombination aus freien/offenen Quellcode und proprietärer (herstellergebundener) Firmware ausgeliefert. Dies gilt insbesondere für die Firmware, die für den Zugriff auf die sogenannten *Google Play Services* erforderlich ist. Die *Google Play Services*, allgemein als *Google Mobile Services* (GMS) bekannt, kontrollieren mobile Geräte auf Systemebene und sind Teil des *Google*-Apps-Pakets [60]. Da *LineageOS* frei sowie quelloffen ist und somit keine proprietäre Firmware enthält, erfordert dieser Umstand für die Untersuchung eine gesonderte Behandlung, da einige Apps aus dem *Google*-Apps-Paket benötigt werden (vgl. Teilkapitel 3.4.2).

3.4.1 The Open GApps Project

LineageOS bietet Nutzern die Möglichkeit, dass gebündelte proprietäre *Google* Apps-Paket nachträglich zu installieren. Im Rahmen der Untersuchung wurde dafür das Paket des *Open GApps Project* verwendet. Das *Open GApps Project* ist ein Open-Source-Projekt zur automatischen Generierung aktueller *Google*-Apps-Pakete. Dabei werden alle *Android*-Versionen unterstützt und die *Google* Apps regelmäßig aktualisiert. Wie auch bei *LineageOS*

handelt es sich um ein Projekt, welches ausschließlich für den persönlichen Gebrauch frei verwendet werden darf [64]. Die Installation ist auch hier in wenigen Schritten auf dem *Raspberry Pi 4 Model B* abgeschlossen:

1. Herunterladen des App-Paketes im ZIP-Dateiformat über die Entwicklerseite;
2. Verschieben der ZIP-Datei auf die Micro-SD-Karte des *Raspberry Pi 4 Model B* (Interner Speicher des *LineageOS*);
3. *LineageOS* im Recovery-Modus starten;
4. im Recovery-Menü die ZIP-Datei auswählen und installieren;
5. Löschen des Dalvik-Caches über das Recovery-Menü;
6. *LineageOS* aus dem Recovery-Menü neustarten [63].

Wenn die Installation erfolgreich verlaufen ist, erscheint das *Google Play Store* Icon und man kann die App wie gewohnt nutzen. Zur vollständigen Nutzung des *Google Play Store* wird ein *Google-Account* benötigt. Im Rahmen der Untersuchung wurden dahingehend vor der Nutzung des *Play Stores* entsprechende Konten erstellt. Die Abbildung 16 veranschaulicht die Benutzeroberfläche bzw. den Startbildschirm des verwendeten *LineageOS 18.1* mit installiertem *Open GApps* Paket (rechtes Icon), aktiviertem Terminal (linkes Icon) und dem Internetbrowser (Icon in der Mitte).

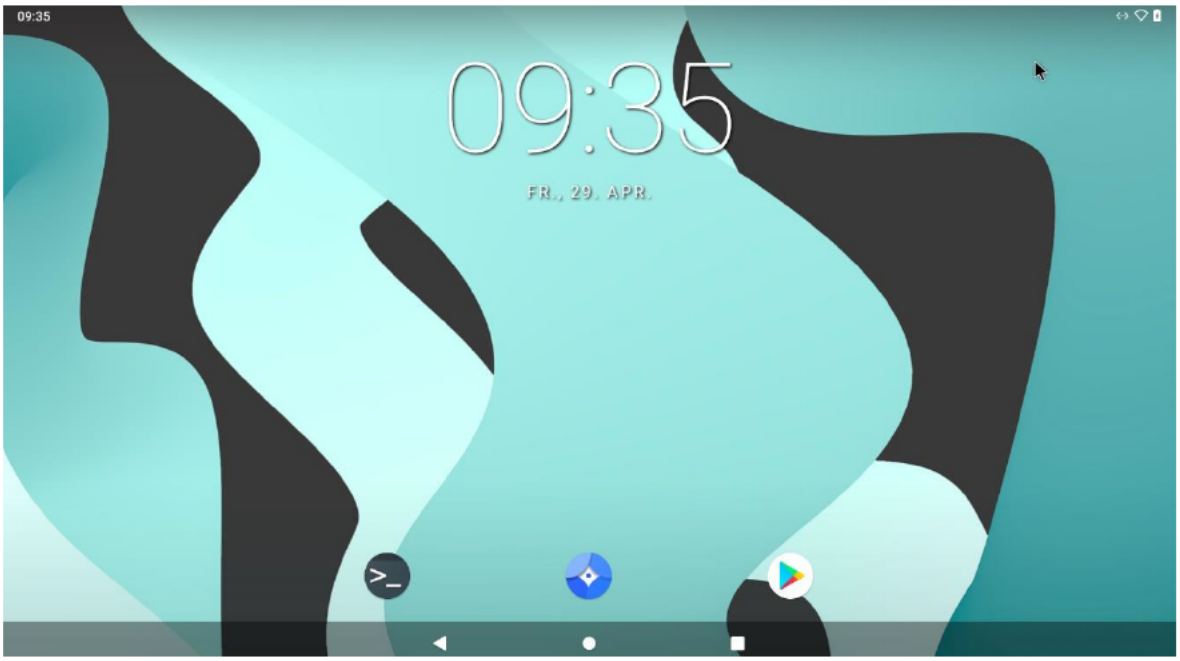


Abbildung 16: Startbildschirm *LineageOS 18.1* (Screenshot, Mai 2022)

Nach der Einrichtung des Betriebssystems mit dem *Google*-Apps-Paket wird als letzter Punkt im nachfolgenden Teilkapitel auf die für die Fitnesstracker und Fitness-Smartwatches relevanten Apps geblendet.

3.4.2 Fitness-Apps

Mit Blick auf das Teilkapitel 3.2 müssen für die Untersuchung die Fitness-Apps der Hersteller *Xiaomi, Fitbit* und *Garmin* installiert werden. Neben der Installation wird für die Nutzung der App auch ein entsprechender Account erstellt. Im Rahmen der Untersuchung wurde dafür der erstellte *Google-Account* verwendet. Bei allen Apps sind die Standardeinstellungen beibehalten. Die zu den Fitnesstrackern/Fitness-Smartwatches gehörenden Apps sind:

1. *Xiaomi Mi Smart Band 6* = ***Zepp Life;***
2. *Fitbit Inspire 2* = ***fitbit;***
3. *Garmin Forerunner 55* = ***Garmin Connect™.***

Bei der Installation der Fitnessapplikationen muss beachtet werden, dass der *Raspberry Pi 4 Model B* als Tablet interpretiert wird und somit Unterschiede in der Verfügbarkeit der Apps im Gegensatz zu Smartphones bestehen können. Ein Blick in den *Google Play Store* verrät, dass alle Apps, außer *Zepp Life* heruntergeladen und installiert werden können. Für die Installation von *Zepp Life* ist folglich eine manuelle Installation notwendig, indem man die APK-Datei (Android Package File) der App herunterlädt und auf dem Gerät speichert. Die APK-Datei wird somit abseits des *Google Play Stores* installiert und genutzt. Die Abbildung 17 gibt einen Gesamtüberblick über die grafischen Oberflächen der drei Fitness-Apps. Links abgebildet, die App *Zepp Life*, in der Mitte die App *fitbit* und rechts die App *Garmin Connect™*.

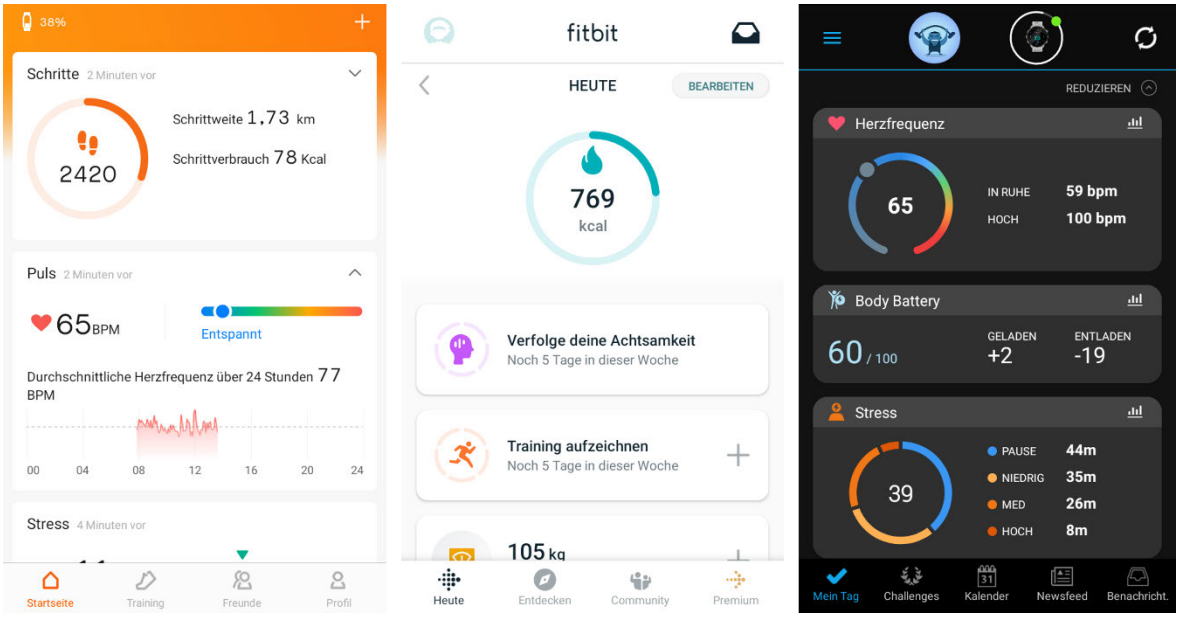


Abbildung 17: Übersicht Fitness-Apps (Zusammengeschnittene Screenshots, Juni 2022)

3.5 IT-Forensische Sicherung der Daten

Ein Ziel der Untersuchung war es (vgl. Teilkapitel 1.2), Verbindungsumgebungen zwischen Fitnesstrackern/Fitness-Smartwatch und einem Simulationsgerät (*Raspberry Pi 4 Model B*)

aufzubauen, um dadurch das Synchronisations- und Speicherverhalten sowie die Zugangsmöglichkeiten der Geräte für den Ermittler darzustellen. Um die gesetzten Ziele zu erreichen, ist es notwendig abzuwägen, welche Daten aus dem Simulationsgerät relevant sind und welche nicht. Nach Jacoby [6] ist eine Betrachtung der Fitnessapplikationsdaten sinnvoll. Auf Grundlage dieser Forschungsarbeit konnte festgestellt werden, dass sich die Fitnessapplikationsdaten der drei Hersteller alle im Verzeichnis `/data/data` des Simulationsgerätes befinden. Eine Suche nach dem Herstellernamen führte schließlich zu den benötigten Fitnessapplikationsdaten in den Pfaden:

1. *Zepp Life* = `/data/data/com.xiaomi.hm.health`
2. *fitbit* = `/data/data/com.fitbit.FitbitMobile`
3. *Garmin Connect™* = `/data/data/com.garmin.Android.apps.connectmobile`

Im Folgenden muss entschieden werden, welche Methodik sich als die sinnvollste für die Sicherung der Fitnessapplikationsdaten herausstellt.

Eine erste Möglichkeit ist die vollständige forensische Sicherung (Physikalische Sicherung, vgl. Teilkapitel 2.1.2) des Simulationsgerätes mit einer anschließenden Extraktion der Fitnessapplikationsdaten. Zur Durchführung würde man für jede Sicherung die Micro-SD-Karte des *Raspberry Pi 4 Model B* entnehmen, diese mittels forensischer Tools sichern und die benötigten Daten „per Hand“ extrahieren. Mit Blick auf die Untersuchungsziele (vgl. Teilkapitel 1.2) ist dieses Verfahren aufgrund der Häufigkeit der zu erstellenden Sicherungen mit einem großen Aufwand verbunden. Da die Sicherung gezielt auf Daten einzelner Applikationen abzielen soll, also nur auf bestimmte Verzeichnisse, ist eine vollständige forensische Sicherung zudem ebenfalls mit einem unnötigen Mehraufwand verbunden. Die erste Möglichkeit wird daher **ausgeschlossen**.

Eine zweite Möglichkeit ist die Sicherung der Fitnessapplikationsdaten über die sogenannte *Android Debug Bridge* (ADB). In diesem logischen Sicherungsverfahren ist das Mobiltelefon zunächst im laufenden Betrieb mithilfe eines USB-Kabels mit dem Untersuchungsgerät verbunden. Anschließend wird über die Kommandozeile des Untersuchungsgerätes ein Zugriff auf die *Shell* des Simulationsgerätes erlangt, worüber dann die benötigten Befehle ausgeführt werden können um die Fitnessapplikationsdaten zu sichern [6]. Da dieses Verfahren jedoch schon Bestandteil einer Bachelorarbeit war [6] und in dieser Untersuchung ein anderes, optimiertes Verfahren gesucht wird, muss die zweite Möglichkeit ebenfalls **ausgeschlossen** werden.

Eine dritte Möglichkeit ist die logische Sicherung über SSH mittels des SFTP, die nachfolgend **favorisiert** wurde.

3.5.1 Logische Sicherung - SFTP

Die logische Sicherung über eine SSH-Verbindung mittels des SFTP stellte sich in der Untersuchung als die einfachste, schnellste und unkomplizierteste Methodik heraus. Bevor auf

die Vorteile der dritten Möglichkeit geblendet werden kann, muss zunächst beschrieben werden, wie solch eine Verbindung aufgebaut wird und die Sicherung durchzuführen ist. An dieser Stelle sei erneut auf den Versuchsaufbau in Abbildung 9 verwiesen.

Grundvorrausetzung für die Sicherung ist die Vereinigung aller aktiven Geräte im selben Netzwerk, die miteinander kommunizieren sollen. Im Rahmen der Untersuchung wurden dafür das Untersuchungs- und Simulationsgerät (*HP*-Laptop und *Raspberry Pi 4 Model B)* mittels eines Netzwerkkabels in das Netzwerk eingebunden und bei jedem Start automatisch mit einer neuen Heimnetzwerkadresse (*Private Network Ip Address*) versehen, über die die Geräte miteinander kommunizieren können. Die Grundlage für das Aufbauen einer SSH-Verbindung ist damit geschaffen.

Auf dem Simulationsgerät (*Raspberry Pi 4 Model B*) ist der SSH-Service standardmäßig deaktiviert. Im ersten Schritt der logischen Sicherung muss der SSH-Service folglich aktiviert werden. Der farbige Rahmen in der Abbildung 18 zeigt den dafür zuständigen Einstellungspunkt in den Systemeinstellungen des *Raspberry Pi*. Setzt man den Schalter auf der rechten Seite der Einstellungen (im farbigen Rahmen rechts), so aktiviert sich der im Simulationsgerät integrierte SSH-Server, der ab sofort unter der privaten Heimnetzwerkadresse 10.1.7.247 über den Port 22 (10.1.7.247**:22**) erreichbar ist. Unter der Einstellungsunterüberschrift „Remote access*“* kann neben dem SSH-Service auch beispielsweise die bereit ausgeschlossene Möglichkeit der ADB aktiviert werden.

Abbildung 18: Aktivierung des SSH-Service im *Raspberry Pi 4 Model B* (Bearbeiteter Screenshot, Juli 2022)

Nach der Aktivierung des SSH-Service auf dem Simulationsgerät bestehen nun seitens des Untersuchungsgerätes (*HP-Laptop*) viele Möglichkeiten, mit dem *Raspberry Pi 4 Model B* zu kommunizieren. Eine Möglichkeit, die sich als schnell, einfach und zuverlässig herauskristallisiert hat, ist die Einrichtung eines SFTP-Clients auf dem Untersuchungsgerät. Im Rahmen der Untersuchung wurde dafür die Software *FileZilla* verwendet. Ausgehend von Teilkapitel 2.4 ist bekannt, dass für die Authentifizierung und den Verbindungsaufbau

zwischen Untersuchungs- und Simulationsgerät entweder Passwörter oder Schlüssel verwendet werden können. Für die Untersuchung wurde die Authentifizierung über öffentlichen und privaten Schlüssel gewählt (Public-Key-Authentifizierung).

Bezugnehmend zu Teilkapitel 2.4 muss beachtet werden, dass ein öffentlicher und privater Schlüssel immer zusammen erzeugt werden und folglich ein Client (Untersuchungsgerät) mit einem privaten Schlüssel immer nur Zugang zu einem Server (Simulationsgerät) erlangen kann, wenn auf diesem der dazugehörige öffentliche Schlüssel hinterlegt ist. Beim Aktivieren des SSH-Service auf dem Simulationsgerät wird auf diesem ein neues Verzeichnis `~/.ssh` erzeugt, in dem unter anderem der private Schlüssel des Servers zu finden ist. Vor einer erfolgreichen Public-Key-Authentifizierung muss also der zur Erstellung des öffentlichen Server-Schlüssels verwendete, private Schlüssel aus dem Verzeichnis extrahiert und in *FileZilla* für die Authentifizierung abgespeichert werden. Mittels des privaten Schlüssels authentifiziert sich der SFTP-Client nun vollautomatisiert gegenüber dem Simulationsgerät und eine Verbindung kann ohne Kennworteingabe aufgebaut werden. Ein weiterer Vorteil neben dem schnellen Verbindungsaufbau ist der uneingeschränkte Systemzugriff (Root-Zugang) den man nach einem erfolgreichen Zugang bekommt. Es ist somit möglich, frei durch das System zu navigieren und die benötigten Daten zu sichern.

Ein erfolgreicher Verbindungsaufbau, ist in der Abbildung 19 veranschaulicht. Zum Verbindungsaufbau (gelbes Rechteck) wird neben der Heimnetzwerkadresse des Servers, der für den Root-Zugang benötigte Benutzername „root“ und der anzusprechende Port 22 benötigt. Ein Kennwort ist aufgrund der Public-Key-Authentifizierung nicht relevant. Sind der hinterlegte private Schlüssel und die Angaben in den Feldern korrekt, so ist der Verbindungsaufbau abgeschlossen und der Verzeichnisinhalt vom Wurzelverzeichnis des SSH-Servers (Simulationsgerät) wird erfolgreich angezeigt. Das blaue Rechteck in der Abbildung 19 zeigt auf der rechten Seite das Wurzelverzeichnis des Simulationsgerätes, in welchem man sich nun mit vollen Zugriffsrechten bewegen kann. Auf der linken Seite ist das jeweilige lokal ausgewählte Verzeichnis abgebildet, in welchen man sich ebenfalls bewegen kann. Für die Datensicherung vom Simulationsgerät kann nun per „Drag and Drop“ der gewünschte Fitnessapplikationsdaten-Ordner auf die linke Seite in eine gewünschte lokale Ordnerstruktur gezogen werden. Über *FileZilla* (SFTP) wird das gewünschte Paket nun an das gewählte Ziel kopiert.

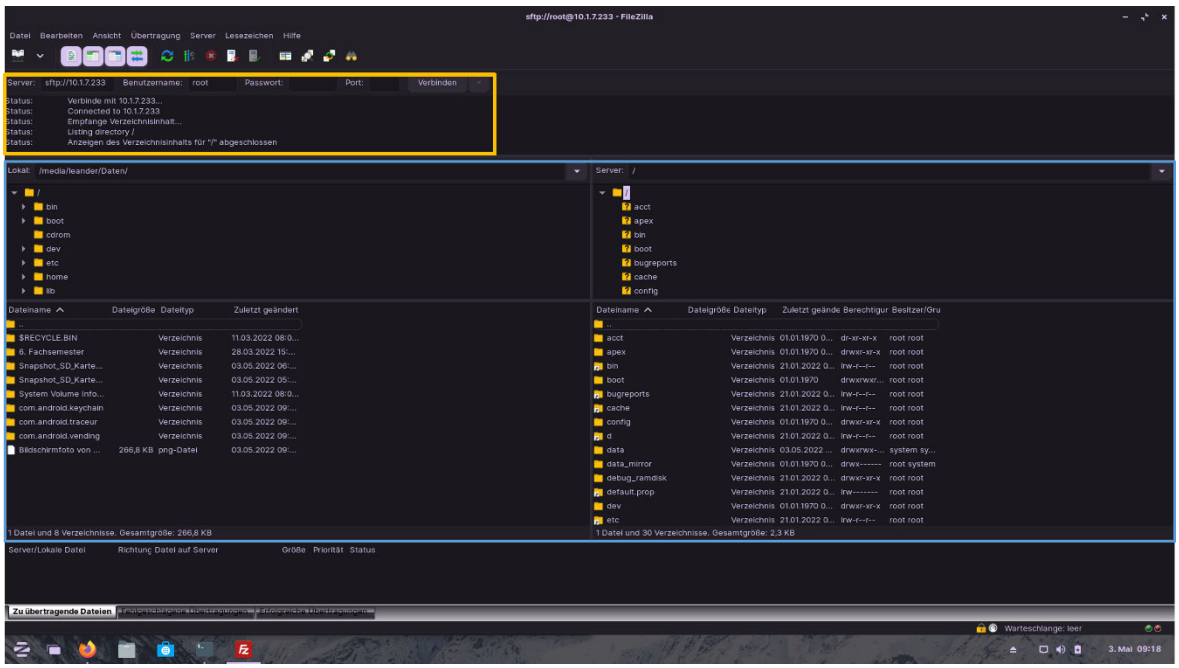


Abbildung 19: Verbindungsaufbau *FileZilla* (Bearbeiteter Screenshot, Juli 2022)

3.5.2 Chip-Off-Analyse

Im Rahmen der Zielsetzung (vgl. Teilkapitel 1.2) führte man als zweite Sicherungsmethodik eine sogenannte Chip-Off-Analyse (vgl. Teilkapitel 2.1.4) bei den Fitnesstrackern *Xiaomi Mi Smart Band 6* und *Fitbit Inspire 2* durch. Aufgrund der hohen technischen Herausforderung und der großen Zerstörungsgefahr verzichtete man auf eine Chip-Off-Analyse bei der Fitness-Smartwatch *Garmin Forerunner 55*. Im Folgenden wird auf die Vorgehensweise dieser hochkomplexen Sicherungsmethodik geblendet.

3.5.2.1 Xiaomi Mi Smart Band 6

Als erstes Untersuchungsobjekt wurde das *Xiaomi Mi Smart Band 6* einer Chip-Off-Analyse unterzogen. Zunächst wird auf Anlage Teil 1 verwiesen, in welcher unterstützend zum beschriebenen Vorgang, anschaulich nachvollzogen werden kann, wie die Chip-Off-Analyse abgelaufen ist.

Im ersten Schritt der Chip-Off-Analyse muss sich zunächst ein Überblick über das zu untersuchende Objekt gemacht werden. Der Fitnesstracker wird dafür unter die von der Kaltlichtquelle *HIGHLIGHT 3100 (Olympus)* zur Verfügung gestellten Beleuchtung genauer betrachtet. Dabei fiel auf, dass der Fitnesstracker von einem Silikonmantel inklusive Armband umgeben war, welcher das eigentliche Gehäuse zum Tragen am Handgelenk fixierte.

Im folgenden Schritt wurde das Gehäuse des Fitnesstracker vom Silikonmantel getrennt. Bei der Betrachtung des Einzelgehäuses suchte man anschließend nach Möglichkeiten, möglichst zerstörungsfrei in das Innere des Fitnesstracker zu gelangen. Die Suche nach Kanten und Einschlüssen war dahingehend sehr hilfreich, da man feststellte, dass das

Display als einziges Bauteil nicht fest mit dem Gehäuse verschmolzen war. Hier bestand also eine Möglichkeit, durch die Kanten am Rand des Displays in das Innere zu gelangen.

Bei einem ersten Versuch das Display mittels Feintools zu lösen, stellte man fest, dass dieses mit Kleber am Gehäuse befestigt ist. Zum Ablösen des Klebers, erhitzte man den Displayrand mittels der *TOOLCRAFT AT850D* Heißluftstation. Nach einer Minute beendete man den Heißluftvorgang und entfernte das Display vorsichtig mit einem Skalpell (Feintool) vom Gehäuse. Dabei fiel auf, dass das Displaykabel mit einer Steckerverrieglung am Mainboard des Fitnesstrackers verankert war. Nach Entfernung der Schaumstoffpads, die die Anschlüsse vor äußeren Einflüssen schützen sollen, löste man das Display vom Mainboard.

Im nächsten Schritt versuchte man, dass Mainboard vom Gehäuse zu trennen. Dieses war mittels zwei Schrauben am Gehäuse befestigt. Zudem gab es noch Schaumstoffpads, eine Steckerverrieglung des optischen Sensors sowie eine *Bluetooth*-Antenne, die vor der Herausnahme entfernt werden mussten. Nach der Entfernung aller genannten Bauteile unter dem *Olympus SZX9* Forschungsstereomikroskop konnte das Mainboard vom Gehäuse getrennt werden. Auf der Vorderseite des Mainboards befand sich eine Schutzabdeckung, die die voraussichtlich darunter befindliche Mikroelektronik schützen soll. Die Rückseite wurde durch den Akkumulator sowie den Vibrationsmotor des Fitnesstrackers bedeckt.

Auf der Suche nach Mikrochips wurde im nächsten Schritt der Akkumulator vom Mainboard abgelötet und ein Chip mit der Aufschrift „winbond 25Q256JWPM“ frei gelegt. Erste Betrachtungen unter dem *Olympus SZX9* sowie Vergleichsrecherchen (Detaillierter im Teilkapitel 3.6) ergaben, dass es sich um ein Flash-Speicherchip handeln muss.

Die Suche nach dem Speicherchip war nunmehr abgeschlossen und es wurde im letzten Schritt der Chip vom Mainboard abgelötet. Dieser Schritt erfordert einen großen Erfahrungsschatz und bildete eine technisch anspruchsvolle Herausforderung im Analyseverfahren. Um den Chip mit einer gleichmäßigen Temperaturverteilung an allen Lötstellen ablöten zu können, strich man den Chip mit dem Lötflussmittel *IF 8300 (Interflux)* ein und erhitzte dieses mittels der *TOOLCRAFT AT850D* Heißluftstation auf ca. 300°C. Bei diesem Vorgang ist stets eine Schutzbrille zu tragen, da beim Erhitzen bestimmte Bestandteile des Lötflussmittels verdampfen, die für das menschliche Auge gefährlich sein können. Nach einer halben Minute hatte sich das erhitzte Lötflussmittel so weit verlaufen, dass der Chip mittels einer Pinzette einfach herausgenommen werden konnte. Zum Schutz vor äußeren Einwirkungen wurde der Chip unverzüglich in ein Schutzgehäuse gelegt. Das Chip-Off-Verfahren war nun abgeschlossen.

Zusammengefasst kann gesagt werden, dass das Chip-Off-Verfahren nicht zerstörungsfrei durchführbar ist.

Um weitere Chips zu finden, entfernte man in einem Zusatzschritt die Schutzkappen von beiden Seiten des Mainboards. Die Abbildung 20 veranschaulicht das freigelegte Mainboard von beiden Seiten. Dabei stellte man einen weiteren auffälligen Chip mit der Aufschrift „dialog DA14697“ fest. Anschaulich dargestellt ist ebenfalls die Lötstelle, auf welcher der „winbond 25Q256JWPM“ angelötet war. Welche Funktionen die festgestellten Chips „winbond 25Q256JWPM“ und „dialog DA14697“ erfüllen und ob sie relevant für die Untersuchung sind, wird im Teilkapitel 3.6 geklärt.

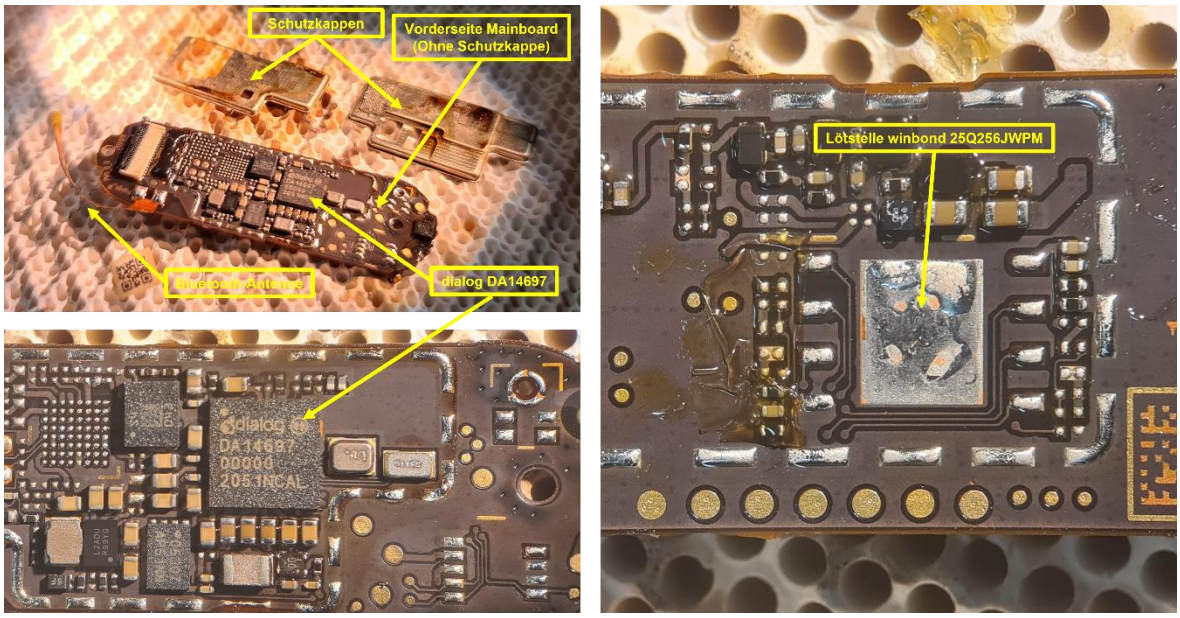


Abbildung 20: Freigelegtes Mainboard vom *Xiaomi Mi Smart Band 6* (Eigene bearbeitete und zusammengeschnittene Aufnahmen, Juli 2022)

3.5.2.2 Fitbit Inspire 2

Das zweite einer Chip-Off-Analyse unterzogene Untersuchungsobjekt war der Fitnesstracker *Fitbit Inspire 2*. Auch hier wird zu Beginn auf die Anlage Teil 2 verwiesen, in welcher ebenfalls unterstützend zur verbalen Beschreibung, die Chip-Off-Analyse anschaulich betrachtet werden kann. Zunächst lässt sich festhalten, dass sich der Ablauf hier nicht deutlich von der Chip-Off-Analyse des *Xiaomi Mi Smart Band 6* unterscheidet.

Im ersten Schritt wurde sich auch hier zunächst ein Überblick über das Untersuchungsobjekt verschafft. Die Kaltlichtquelle *HIGHLIGHT 3100 (Olympus)* half erneut, dass Untersuchungsobjekt genug auszuleuchten. Bei der näheren Betrachtung viel auf, dass der Fitnesstracker im Gegensatz zum *Xiaomi Mi Smart Band 6* nicht aus einem Silikonmantel und dem dazugehörigen Gehäuse besteht, sondern aus einem oberen und unterem Silikonarmband und dem dazugehörigen Gehäuse. Auch hier galt die weitere Aufmerksamkeit dem eigentlichen Gehäuse des Fitnesstracker.

Im nächsten Schritt wurde also erneut nach Kanten und Einschlüssen gesucht, die es erlauben, in das Gehäuse einzudringen. Dabei stellte sich eine deutliche Kante unterhalb des Displays als nützlich dar, über welche man zunächst versuchte, mittels Feintools

einzudringen. Entgegen der Erwartung aus dem vorherigen Chip-Off-Verfahren gelang es erstaunlicherweise gut, dass vermutliche Display mittels einer Zange und eines Skalpells herauszulösen. Dabei stellte sich überraschenderweise das vermutete Display lediglich als eine Linse des darunterliegenden Displays heraus.

Im nächsten Schritt wurde die Linse entfernt und das darunter liegende Display freigelegt. Beim Display stellte man fest, dass dieses am Mainboard festgeklebt war. Hinzu kam, dass das Mainboard selbst am Gehäuse nicht verschraubt, sondern verschweißt war. Ein zerstörungsfreies Auseinanderlegen der einzelnen Komponenten ist somit endgültig ausgeschlossen.

Darauffolgend löste man im nächsten Schritt das Display mittels eines Skalpells vom Mainboard und das Mainboard selbst durch ein Durchtrennen der Schweiß-Haltepunkte. Was sich als Ergebnis aus dem Gehäuse herauslöste war ein Verbund aus einem Akkumulator mit Kunststoffhalterung, dem Mainboard und dem darauf angeschlossenen Display.

Im vorletzten Schritt wurden nun alle Bestandteile vom Mainboard getrennt. Neben dem Ablöten der Akkumulator-Kontakte wurde das Displaykabel vom Mainboard abgesteckt und Schaumstoffkontakte entfernt. Auf der Rückseite des Mainboards befanden sich nach dem Entfernen aller externen Bestandteile außer dem optischen Sensor und der Steckerverriegelung des Display-Kabels keine relevanten Komponenten mehr, weswegen ausschließlich die Vorderseite betrachtet wurde.

Auf dieser verdeckte eine Schutzkappe die darunter vermutete Mikroelektronik. Entgegen der Erwartung konnte auch in diesem Schritt die Schutzkappe ohne Eingriff von Heißluft, mittels Feintools abgetrennt werden, woraufhin nun die Vorderseite des Mainboards frei lag. Auffällig waren hier zwei große Chips mit den Aufschriften „CY8C68237FM9-BLE“ und „A0330NU12835“ die in der Abbildung 21 veranschaulicht sind.

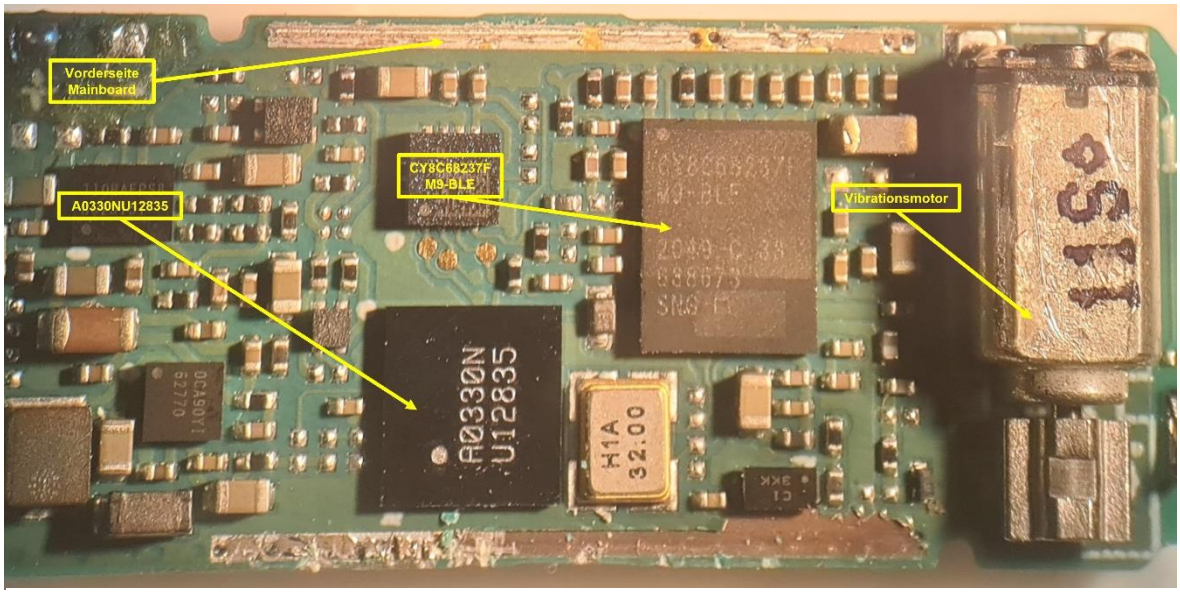


Abbildung 21: Vorderseite des Mainboard vom *Fitbit Inspire 2* (Eigene bearbeitete Aufnahme, Juli 2022)

Erste Vergleichsrecherchen zu den Aufschriften der Chips (detaillierter im Teilkapitel 3.6) ergaben nur beim Chip „CY8C68237FM9-BLE“ einen Treffer, dass es sich um ein SoC der Firma *Cypress Semiconductor* handeln muss.

Die Suche nach den Chips war nun abgeschlossen und im letzten Schritt wurde nun versucht, die beiden Chips vom Mainboard abzulöten. Die Vorgehensweise inklusive der verwendeten Hardware ist hier identisch zur bereits beschriebenen und wird daher nur grob angerissen. Nach dem Auftragen des Lötflussmittel und der Erhitzung dieses auf ca. 300°C konnten unter Verwendung einer Pinzette nach etwa einer halben Minute die Chips vom Mainboard abgenommen werden. Zum Schutz vor äußeren Einwirkungen wurden auch hier die Chips unverzüglich in ein Schutzgehäuse gelegt. Das Chip-Off-Verfahren war nun abgeschlossen.

Zusammengefasst kann gesagt werden, dass das Chip-Off-Verfahren auch beim *Fitbit Inspire 2* nicht zerstörungsfrei durchführbar ist.

3.6 Mikrochips und Adapter

Das folgende Teilkapitel gibt anknüpfend zu den bereits beschriebenen Materialien und Methoden der IT-Forensischen Datensicherung einen Überblick über die im Teilkapitel 3.5.2 detektierten Mikrochips mit dem Ziel Grundlegende Informationen und Funktionsweisen in Bezug auf die Untersuchung zu vermitteln. Dabei wird auch ein Adapter vorgestellt, welcher für die Interpretation eines vorhandenen Speicherchips benötigt wird.

3.6.1 Mikrochip - DA14697

Der *DA14697* gehört zur Familie der *DA1469x Multi-Core-SoC´s* des Unternehmens *Dialog Semiconductor*, die den neuesten *ARM Cortex M33TN*-Anwendungsprozessor mit fortschrittlicher Energieverwaltungsfunktion, kryptografischer Sicherheits-Engine sowie einer softwarekonfigurierbaren Protokoll-Engine mit Funksensor nach *Bluetooth® 5.1* Standard etc. umfassen. Anwendungsbereiche sind unter anderem die Verwendung in Fitnesstrackern, Sportuhren, Smartwatches, Spielzeugen, sprachgesteuerten Fernbedienungen etc. Der benötigte Code wird durch den *ARM Cortex M33TN*-Anwendungsprozessor entweder aus dem eingebetteten Speicher (RAM) oder aus einem externen QSPI-Flash-Speicher (*Quad Serial Peripheral Interface*), der mit einer On-the-Fly-Entschlüsselungsfunktion ohne zusätzliche Wartezeiten ausgestattet ist, ausgeführt. Ein dafür vorhandener Quad-SPI-Flash-Controller (QSPI) unterstützt die Entschlüsselung der vom Flash-Speicher abgerufenen Daten im „Auto-Modus“. Die On-the-fly-Entschlüsselung basiert dabei auf dem CTR-Modus (Counter Mode) des AES-Verschlüsselungsalgorithmus (Advanced Encryption Standard) mit einer Schlüsselgröße von 256-Bit. Der Flash-Inhalt sollte somit bereits mit demselben Algorithmus verschlüsselt sein. Ein zusätzlich vorhandener optimierter und programmierbarer Sensorknotenkontroller ermöglicht die Datenerfassung und den Betrieb der Sensorknoten ohne Eingriff des Anwendungsprozessor, was sich positiv auf den

Stromverbrauch auswirkt. Der *DA14697* unterstützt zudem eine Vielzahl von Standard- und fortschrittlichen Peripheriegeräten, die die Interaktion mit anderen Systemkomponenten und die Entwicklung von fortschrittlichen Benutzeroberflächen und funktionsreichen Anwendungen ermöglicht [65]. Eine Betrachtung des SoC mit Blick auf das Teilkapitel 3.7 erwies sich aufgrund der eingebauten kryptografischen Sicherheits-Engine zur weiteren Betrachtung als **ungeeignet**.

3.6.2 Mikrochip - W25Q256JWPIM

Der *W25Q256JWPIM* ist ein serieller Flash-Speicherchip des Unternehmens *Winbond Electronics Corporation*, der Speicherlösungen für Systeme mit begrenzten Pins, Platz und Leistung bietet. Es ist ein flexibler, leistungsstarker Flash-Baustein, der sich neben Code-Shadowing auf RAM-Speichern ideal für die Ausführung von Code sowie zum Speichern, Text und Daten eignet [66]. Besonders die letzte Eigenschaft könnte im Rahmen der Untersuchung nützlich sein, weswegen der Flash-Speicherchip nun genauer betrachtet werden soll.

Der serielle Flash-Speicherchip besitzt eine Sektorengröße von 4 KB sowie Dual/Quad Ein- und Ausgangsschnittstellen, die die Übertragungsrate verdoppeln/vervierfachen können [67]. Des Weiteren verfügt der Flash-Speicher über eine Bitdichte von 256M-Bit pro Längen-/Flächeneinheit und arbeitet mit einer Versorgungsspannung von 1,7 bis 1,95 Volt. Der Gehäusetyp ist *WSON8 (Plastic Small-outline No-lead Package)* mit einer Chipgröße von 6x5-mm und einer Anzahl von acht Pads, welcher besonders mit Blick auf den passenden Adapter beachtet werden muss. Zu beachten ist zudem, dass die Teilekennzeichnung auf dem Chip selbst kein Unternehmens-Präfix und Angaben zum Temperaturspektrum (W und I) enthält, folglich also *25Q256JWPM* als Bezeichnung auf dem Chip graviert ist [66].

Die Abbildung 22 gibt einen Überblick über die Position, Konfiguration und Funktion der acht einzelnen Pads. Abgebildet ist eine Originalaufnahme des Chips (links, Ansicht von unten) im Vergleich zu einer Skizze aus dem Datenblatt (rechts, Ansicht von oben). Auffällig ist hier eine fehlende Ecke im Rechteck der Kühlfläche (links) sowie ein grauer Punkt in der Zeichnung (rechts), der ebenfalls in der Aufnahme nachgestellt wurde.

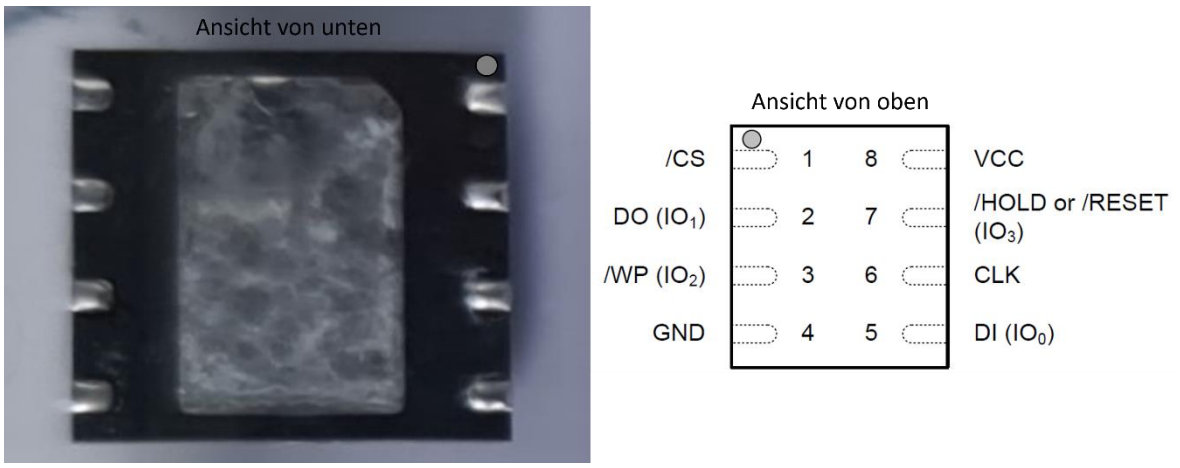


Abbildung 22: *Winbond W25Q256JWPIM* - Pad-Konfiguration [Bearbeitete und zusammengeschnittene Abbildung, bestehend aus: eigene bearbeitete Aufnahme, Juni 2022 (links); Bearbeitete Abbildung aus [66, S. 6] (rechts)]

Eine zusätzliche Tabelle (Tabelle 1) soll die Bedeutung des grauen Punktes und der Abkürzungen der Pads erklären.

Der sogenannte /CS-Pin (*Chip*-Select) aktiviert und deaktiviert den Betrieb des Gerätes und ist aufgrund dieser Aufgabe mit einem grauen Punkt in der Zeichnung sowie mit anderen Kennzeichnungen wie fehlenden Pad-Ecken gekennzeichnet [66].

Die zwei seriellen Dateneingänge- und Ausgänge (DI, DO = *Data-Input, Data-Output*) sowie die vier Daten Ein- und Ausgänge (IO0, IO1, IO2, IO3 = *Input/Output*) stellen den Betrieb der Standard/Dual/Quad-Schnittstellen und deren Befehle sicher [66].

Um das Beschreiben des Statusregisters zu verhindern, wird der Schreibschutz-Pin (/WP = *Write-Protect*) verwendet [66].

Mittels des /HOLD-Pins kann das Gerät angehalten werden [66].

Der CLK-Pin (*Serial-Clock-Input*) kümmert sich in seiner Aufgabe um das Timing für die seriellen Eingangs- und Ausgangsoperationen [66].

Ferner ist der GND-Pin (*Ground*) für die Erdung zuständig [66].

Als letzter Pin kann der /RESET-Pin für das Zurücksetzen aller laufenden Operationen verwendet werden [66].

Tabelle 1: Pad-Beschreibung - *Winbond W25Q256JWPIM* (Eigene Darstellung basierend auf [66, S. 6], Juni 2022)

Pad-Nr.	Pad-Name	E/A	Funktion
1	/CS	E	Chip-Select Eingang (Grauer Punkt)
2	DO (IO1)	E/A	Datenausgabe (Daten Ein- und Ausgabe 1) [1]
3	/WP (IO2)	E/A	Schreibgeschützte Eingabe (Daten Ein- und Ausgabe 2) [2]
4	GND	-	Erdung/Masse
5	DI (IO0)	E/A	Dateneingabe (Daten Ein- und Ausgabe 0) [1]
6	CLK	E	Serieller Takteingang
7	/HOLD oder /RESET (IO3)	E/A	Eingabe für das Halten oder Zurücksetzen aller Operationen (Daten Ein- und Ausgabe 3) [2]
8	VCC	-	Stromanschluss

[1] Die Daten Ein- und Ausgabe 0 und 1 werden für Standard und Dual- Befehle der SPI-Schnittstelle verwendet.

[2] Die Daten Ein- und Ausgabe 0 bis 3 werden für Quad-Befehle der SPI-Schnittstelle verwendet.

Mit Blick auf das Teilkapitel 3.7 könnte sich die Auswertung des *W25Q256JWPIM* aufgrund der fehlenden On-the-Fly-Entschlüsselungsfunktion des *DA14697* als problematisch darstellen, da der Inhalt des Flash-Speicherchips höchstwahrscheinlich AES-verschlüsselt ist. Unter Zuhilfenahme eines speziellen Adapters soll, aufgrund der hohen Wahrscheinlichkeit ermittlungsrelevante Daten zu finden, trotzdem **in Betracht gezogen werden**, Daten aus dem Flash-Speicher zu extrahieren.

3.6.3 Adapter - DIL8/QFN8-1 ZIF-CS SFlash-1a

Der *DIL8/QFN8-1 ZIF-CS SFlash-1a* ist ein Spezial-Adapter der unter anderem für serielle Flash-Speicherchips im 6x5-mm WSON-8-Pad-Gehäuse-Format (WSON8) ausgelegt ist [68]. Beim Einsetzen von Flash-Speicherchips muss man zunächst die Gehäuseform *DIL8* (Dual in-line package 8) des Adapters beachten. Des Weiteren ist der Fuß an der gegenüberliegenden Seite zur Drucksteckmontage, welcher aus 2 Reihen mit je 24 Pins (0,6 x 0,6-mm) und einem Reihen-Abstand von 600mil (1,524cm) besteht, wichtig. Der Sockeltyp des Adapters ist *ZIF QFN8* mit einer mechanischen Lebensdauer von 5000 Zyklen [68]. Die Abbildung 23 veranschaulicht die für den Sockeltyp des Adapters geeignete Chipgröße.

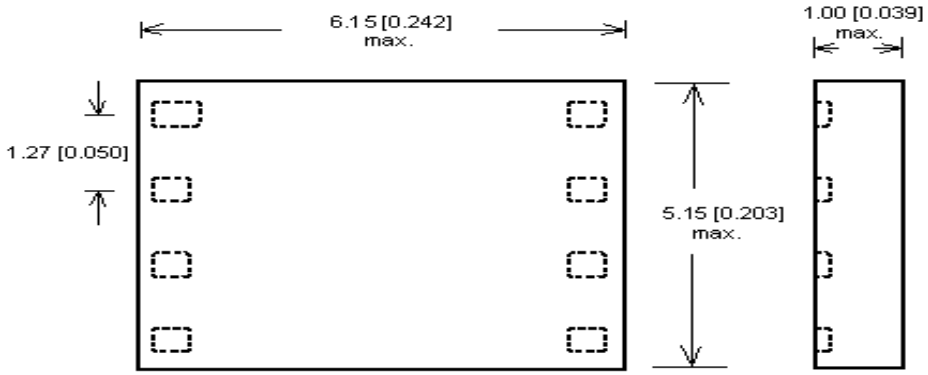


Abbildung 23: Geeignete Chipgröße für Spezial-Adapter (Sockeltyp *ZIF QFN8*) [68]

3.6.4 Mikrochip - CY8C68237FM9-BLET

Der *CY8C68237FM9-BLET* ist ein SoC des Unternehmens *Cypress Semiconductor Corporation* (heute *Infineon Technologies AG*) [69]. Als einziger Mikrochip ist dieser ein kundenspezifisch hergestellter Microkontroller, über den keine öffentlich abrufbaren Informationen in Form von beispielsweise Datenblättern existieren [70]. Nach einer Anfrage beim Hersteller nahm man Kontakt im Entwicklerforum auf. Als Antwort auf ein erstellten Forumseintrag wurde mitgeteilt: „Dieses Teil ist kein marktgängiges Teil und daher können wir nicht viele Details angeben.“ [70] Aufgrund dieser Gegebenheit erwies sich eine weitere Betrachtung des Microkontrollers mit Blick auf das Teilkapitel 3.7 als **ungeeignet**.

3.6.5 Mikrochip - A0330NU12835

Nach umfassenden Recherchen konnten keine weiterführenden Informationen zum Mikrochip *A0330NU12835* gefunden werden. Eine weitere Betrachtung erwies mit Blick auf das Teilkapitel 3.7 als **ungeeignet**.

3.7 Extraktion ermittlungsrelevanter Daten

Nachdem im Teilkapitel 3.5 ein ausführlicher Einblick in die IT-Forensische Sicherung der durch die Fitnesstracker/Fitness-Smartwatches erzeugten Daten gegeben wurde, soll im nachfolgenden Teilkapitel abgewogen werden, welche Daten aus den Sicherungen

ermittlungsrelevant sind. Die Methoden der Datenextraktionen sind vielseitig und bedürfen für jeden einzelnen Hersteller unterschiedliche Herangehensweisen. Allen Herstellern ist gemein, dass sie ihre Daten in Ordnern, benannt nach dem Herstellernamen ablegen, wie das Teilkapitel 3.5 bereits aufzeigte. Wie eine verwandte Forschungsarbeit [6] bereits untersuchte, sind in allen Fitnessapplikationsdaten jeweils Unterordner vorhanden, die diese in drei Kategorien aufteilen. Die Tabelle 2 veranschaulicht die festgestellten Unterordner mit den jeweils darin befindlichen Daten.

Tabelle 2: Unterkategorien der Fitnessapplikationsdaten (Eigene Darstellung basierend auf [6, S. 16], Juli 2022)

Ordnername	Enthaltene Daten
databases	*SQLite*-Datenbanken und Datenbank-Journal-Dateien der Fitnessapplikation
files	Sonstige Dateien, die die Entwickler der Fitnessapplikationen festlegen
shared_prefs	XML-Dateien (Extensible Markup Language), die die Einstellungen der Fitnessapplikation speichern

Der erste Unterordner mit dem Namen „databases“ enthält die Datenbanken der Fitnessapplikationen im *SQLite*-Format. *SQLite* eignet sich als Datenbankformat dahingehend, da Applikationen strukturierte Daten gut und effizient in Datenbanken schreiben können, die über ein effizientes Speichermanagement verfügen. Jede Datenbank ist dabei als einzelne Datei im Ordner abgespeichert. Aus forensischer Sicht speichern die Datenbanken, die Hauptdatenquelle der Fitnessapplikationen, eine Menge an auswertbaren und ermittlungsrelevanten Informationen. Der zweite Unterordner „files“ enthält sämtliche Dateien, die durch die Entwickler der Fitnessapplikationen festgelegt wurden. Demnach ist nicht definiert, was für Daten die jeweiligen Hersteller ablegen und ob diese einer näheren Betrachtung unterzogen werden müssen. Der dritte und letzte relevante Unterordner „shared_prefs“ bietet den Applikationen die Möglichkeit einfache Daten, wie z.B. Einstellungen zu speichern. Die Datenstruktur XML (Extensible Markup Language) speichert Daten als Schlüssel-Wert-Paare ab und wird aufgrund der schnellen Speichermethode von vielen Applikationen genutzt. Dieser Fakt macht die XML-Dateien aus forensischer Sicht ebenfalls interessant [6].

Im Rahmen der Untersuchung musste nun entschieden werden, welcher Ordner mit höchster Wahrscheinlichkeit ermittlungsrelevante Daten enthält. Hierbei kamen erneut die Erkenntnisse aus der Bachelorarbeit von Jacoby [6] sowie eigene Sichtungen der Unterordner mit den enthaltenen Dateien zur Hilfe. Zusammengefasst lässt sich festhalten, dass eine Betrachtung aller Ordner und deren Daten im Rahmen der Untersuchung zu komplex wäre.

Aus forensischer Sicht ist die Betrachtung eines einzelnen Ordners zielführender, weswegen aufgrund der Menge an möglichen ermittlungsrelevanten Daten der **„databases“**-Ordner ausgewählt wurde. Das Teilkapitel 3.7.1 gibt über jeden Hersteller einen Überblick, welche Datenbanken relevante Informationen enthalten und demnach für eine Extraktion in Betracht kämen.

3.7.1 Datenbanken und Tabellen

Mit dem Wissen über den Speicherort der Datenbanken wird in diesem Teilkapitel ein kurzer Überblick über die jeweils herstellerspezifischen Datenbanken mit den dazugehörigen Tabellen gegeben, die aus forensischer Sicht einer Datenextraktion unterzogen werden müssen. Wie auch im vorherigen Teilkapitel, basieren die Ergebnisse dieses Teilkapitels auf den Forschungsergebnissen von Jacoby [6] sowie eigenen Sichtungen der Datenbanken und deren Tabellen. Bei der Suche nach relevanten Datenbanken halfen zwei Indikatoren, sich in der teils großen Menge an Datenbanken im Ordner „databases“ der jeweiligen Hersteller zurecht zu finden.

Als ersten Indikator beachtete man die Datenbankgröße, bei der einerseits auf die Größe der Datenbank (in KB) und andererseits auf das Verhalten der Größe geschaut wurde. Es wurde somit überprüft, ob die Datenbank immer größer wird und demnach neue Einträge hineingeschrieben werden. Wächst die Datenbank stetig, ist dies ein Indiz dafür, dass das der Fitnesstracker oder die Fitness-Smartwatch die Datenbank wahrscheinlich dafür nutzt, Daten abzuspeichern.

Ein zweiter wichtiger Indikator waren die Zeitstempel der *SQLite*-Datenbankdateien. Mithilfe dieser Zeitangaben konnte man nachverfolgen, wann die Datei zuletzt beschrieben wurde. Nach einer Synchronisierung (vgl. Teilkapitel 4.1) und dem anschließenden Vergleich mit den Zeitstempeln aus den Datenbanken, konnte somit feingranular nachgewiesen werden, dass der Fitnesstracker oder die Fitness-Smartwatch die Datenbank nach einer Synchronisierung beschrieben haben.

Die Suche nach ermittlungsrelevanten Daten ist jedoch noch nicht mit der Entscheidung der Datenbank abgeschlossen. Jede Datenbank enthält je nach Hersteller verschiedenste Tabellen, die wiederrum Daten in unterschiedlichen Formaten abspeichern. Erst nach einer Betrachtung dieser konnte entschieden werden, ob die beobachtete Tabelle einer weiteren forensischen Untersuchung unterzogen werden soll. Die Tabelle 3 gibt einen kurzen Überblick über die für die Untersuchung ausgewählten Datenbanken und Tabellen, die in den nächsten Teilkapiteln eine relevante Rolle spielen werden. Nach der Betrachtung jeder Datenbank mit den dazugehörigen Tabellen in Bezug auf die vorgestellten Indikatoren, konnte nach probeweise durchgeführten Synchronisierungen für jeden Hersteller eine interessante Datenbank und Tabelle detektiert werden. Die Suche umfasste insgesamt 153 Datenbanken und Tabellen. Für das *Xiaomi Mi Smart Band 6* gibt dahingehend die Tabelle „DATE_DATA“ aus der Datenbank „origin_db_66af05c3c40b8b31c787efad-1e0dd3f2“, für

das *Fitbit Inspire 2* die Tabelle „HEART_RATE_DAILY_SUMMARY“ aus der Datenbank „heart_rate_db“ und für die *Garmin Forerunner 55* die Tabelle „user_daily_summary“ aus der Datenbank „cache-database“ über die Ergebnisse der Suche Auskunft.

Tabelle 3: Übersicht der relevanten Datenbanken und Tabellen (Eigene Darstellung, Juli 2022)

Hersteller	Anz. DB	!DB!	Anz. Tab.	!Tab.!
Xiaomi	7	**origin_db_66af05c3c40b8b31c787efad1e0dd3f2**	63	**DATE_DATA**
Fitbit	46	**heart_rate_db**	3	**HEART_RATE_DAILY_SUMMARY**
Garmin	13	**cache-database**	21	**user_daily_summary**

- Anz. DB = Anzahl der Datenbanken
- !DB! = Ausgewählte relevante Datenbank
- Anz. Tab. = Anzahl der Tabelle/n
- !Tab.! = Ausgewählte relevante Tabelle

3.7.2 Schritt- und Herzfrequenzdaten

Im Rahmen der Bachelorarbeit geht es hauptsächlich um ermittlungsrelevante Daten. Welche Daten jedoch ermittlungsrelevant sind und welche nicht, wird durch die Umstände des aus forensischer Sicht jeweils zu bearbeitenden Falls bestimmt. Aufgrund aktuell bestehender forensischer Relevanz (vgl. Kapitel 1) sowie des begrenzten zeitliches Rahmens wurden für die Untersuchung, die Schritt- und Herzfrequenzdaten als ermittlungsrelevant festgelegt. Das Teilkapitel 2.2.2 gab dahingehend bereits einen Einblick. Im Folgenden werden die Extraktionsmöglichkeiten der Schritt- und Herzfrequenzdaten für jeden Hersteller einzeln betrachtet.

3.7.2.1 Xiaomi

Die Tabelle „DATE_DATA“ in der ausgewählten Datenbank des ersten Herstellers Xiaomi ist eine der Informationsreichsten und enthält unter anderem die im oberen Teilkapitel definierten ermittlungsrelevanten Daten. Sie beinhaltet 14 Spalten mit den Namen:

„TYPE, SOURCE, DATE, SUMMARY, USER_SUMMARY, INDEXS, DATA, DATA_HR, SUMMARY_HR, SYNC, SYNC_QQHEALTH, TIME_ZONE, DEVICE_ID, STAGE_STEPS_SUMMARY".

Zur Eingrenzung in Bezug auf den Untersuchungsrahmen stellt die Abbildung 24 die relevanten Spalten der Tabelle „DATE_DATA" dar. Die erste Spalte enthält dabei den Datumsvermerk der Eintragung in Klartext. Bei den Spalten zwei und drei fällt auf, dass diese nicht sofort abgelesen werden können. Bei genauem Betrachten der Datenbankzellen der Spalten zwei und drei mittels der Software *DB Browser for SQLite* fand man heraus, dass die Daten in der „DATA_HR"-Spalte als ein großes Binärdatenobjekt (*Binary Large Object* - BLOB) in 1440 Bytes abgelegt werden. In der „STAGE_STEPS_SUMMARY"-Spalte hingegen werden die Daten in 144 JSON-Objekten abgespeichert. Die Abbildung 24 veranschaulicht die Datenbankzellen mit Ihren Inhalten.

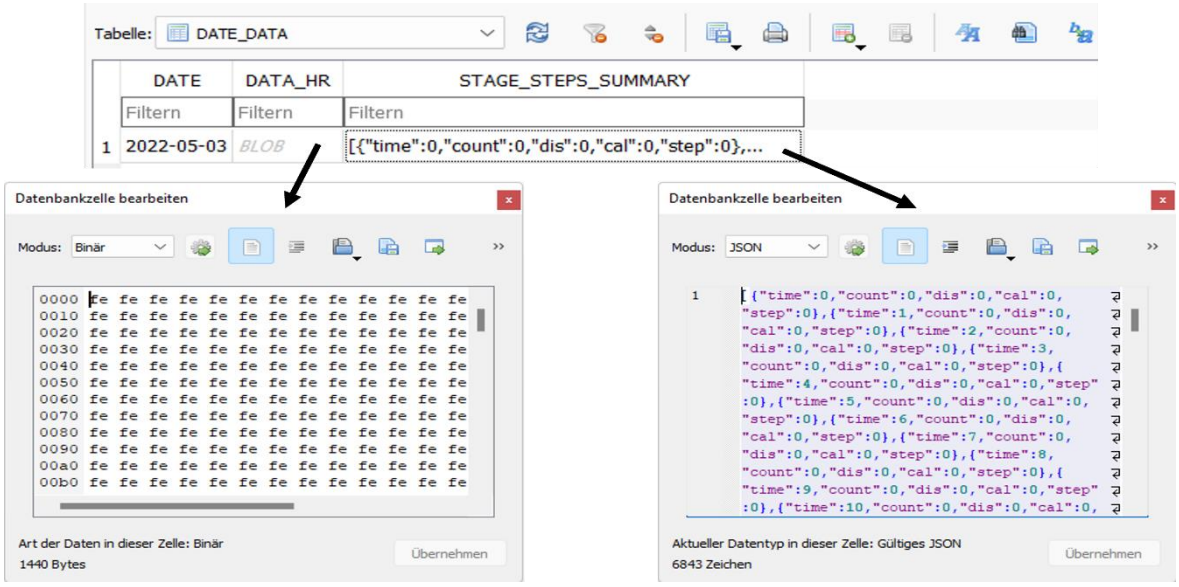


Abbildung 24: Ermittlungsrelevante Daten aus der Tabelle „DATE_DATA" (Zusammengeschnittene und bearbeitete Screenshots, Juli 2022)

Bei der Betrachtung der Datenbankzelle aus der „DATA_HR"-Spalte (Abbildung 24, links) sind zunächst die 1440 Bytes auffällig. Ausgehend von der „DATE"-Spalte stellt jede Zeile einen Tag dar. Gliedert man nun einen Tag in Minuten auf, so erhält man 1440 Minuten pro Tag (24 x 60 = 1440). Aus diesem Zusammenhang lassen sich folgende Hypothesen formulieren:

- **H1**: Die 1440 Byte stellen die Minuten des Tages dar.
- **H2**: Die Byte-Werte sind Herzfrequenzdaten.

Ausgehend von der Hypothese **H1** stünde jedes Byte für eine Minute, beginnend mit dem ersten Byte um 0 Uhr und dem letzten um 23:59 Uhr. Ein Byte wiederum selbst, könnte nach **H2** also die gesuchte Herzfrequenz in Hexadezimaler Schreibweise beinhalten. Um die Hypothesen zu beweisen, müssen Argumente zur Verifizierung dieser gefunden werden.

Um die Bytes und deren Zeitstempel zu untersuchen sowie zu extrahieren, wurde ein eigenes *Python*-Skript mittels *PyCharm* geschrieben, welches die Herzfrequenzdaten für einen ausgewählten Tag in eine übersichtliche dezimale Schreibweise umwandelt. Neben der Umwandlung erzeugt das Skript eine CSV-Datei, in welcher die Herzfrequenzdaten für jede Minute zeilenweise betrachtet werden können. Zur Übersichtlichkeit über den Verlauf der Herzfrequenz erzeugt das Skript auch ein Diagramm der Frequenz. Das Skript mit entsprechender Kommentierung kann in der Anlage, Teil 3 betrachtet werden.

Für eine erste Verifizierung wurde im Skript der 18. Mai 2022 eingelesen (vgl. Teilkapitel 4.2.1.1) und das erzeugte Diagramm der Herzfrequenz mit dem in der Fitnessapplikation erzeugten Diagramm verglichen. Beide Diagramme stimmten in Bezug auf ihre Amplituden überein, weshalb dieses Argument für eine **Verifizierung** der Hypothese **H1** und **H2** spricht.

Betrachtet man die Abbildung 25, so kann man deutlich erkennen, dass sich die Struktur der Binärdaten ab dem Offset 0x297 verändert. Auf Bytes heruntergebrochen sind zum Zeitpunkt der Änderung somit 661 Byte, in Bezug auf H1 also 661 Minuten, vergangen. Geht man nun davon aus, dass ab 0 Uhr 661 Minuten vergangen sind, müsste der Fitnesstracker am 03. Mai 2022 bis 11:01 Uhr nicht in Benutzung gewesen sein. Tatsächlich bestätigte sich mittels externer Aufzeichnungen, dass der Fitnesstracker bis 11:01 Uhr nicht getragen wurde, was ein weiteres Argument zur **Verifizierung** von **H1** und **H2** darstellt.

Betrachtet man nun die Abbildung 25, so erkannt man, dass am zehnten Byte eine Hexadezimale 31 (mit einer 1 markiert) abgelesen werden kann. Eine Hexadezimale 31 ist umgerechnet eine Dezimale 49, eine durchaus realistische Herzfrequenz. Auf der rechten Seite können jeweils die mit einer Uhrzeit versehenen Skriptausgaben betrachtet werden. Für die nächsten neun Minuten überschreibt sich der gemessene Wert in der jeweiligen Datenbankzelle, bis erneut gemessen wird (Position 2). Dies wird so lange fortgesetzt, bis der Fitnesstracker abgelegt wird. Verändert sich kein Byte mehr (Fitnesstracker wurde abgelegt) so wird das letzte geänderte Byte mit den restlichen überschrieben, bis das 1400te-Byte erreicht ist. Die Abbildung 25 stellt ein weiteres Argument zur **Verifizierung** von **H1** und **H2** dar, da die Standardeinstellung in der Fitnessapplikation (10-minütige Herzfrequenzmessung) in den Speicherverhaltensweisen der Binärdaten wiederzuerkennen ist.

Um ein letztes Argument zur **Verifizierung** von **H1** und **H2** zu finden, wurde ab dem 04. Mai 2022 (Start der Untersuchung, vgl. Teilkapitel 4.1.1) in der Fitnessapplikation *Zepp Life* eingestellt, dass jede Minute die Herzfrequenz gemessen werden soll. Bei Betrachtung der Skript-Ausgaben ab dem 04. Mai 2022 stellte man fest, dass sich nun jede Minute, also bei jedem Byte, die Herzfrequenz änderte. Im Gegensatz zum 03. Mai 2022 wurde also nicht mehr 10 Minuten lang derselbe Wert überschrieben, sondern folglich jede Minute mit der aktuellen Herzfrequenz ergänzt.

Zusammengefasst konnten die Hypothesen **H1** und **H2** durch die genannten Argumente verifiziert werden.

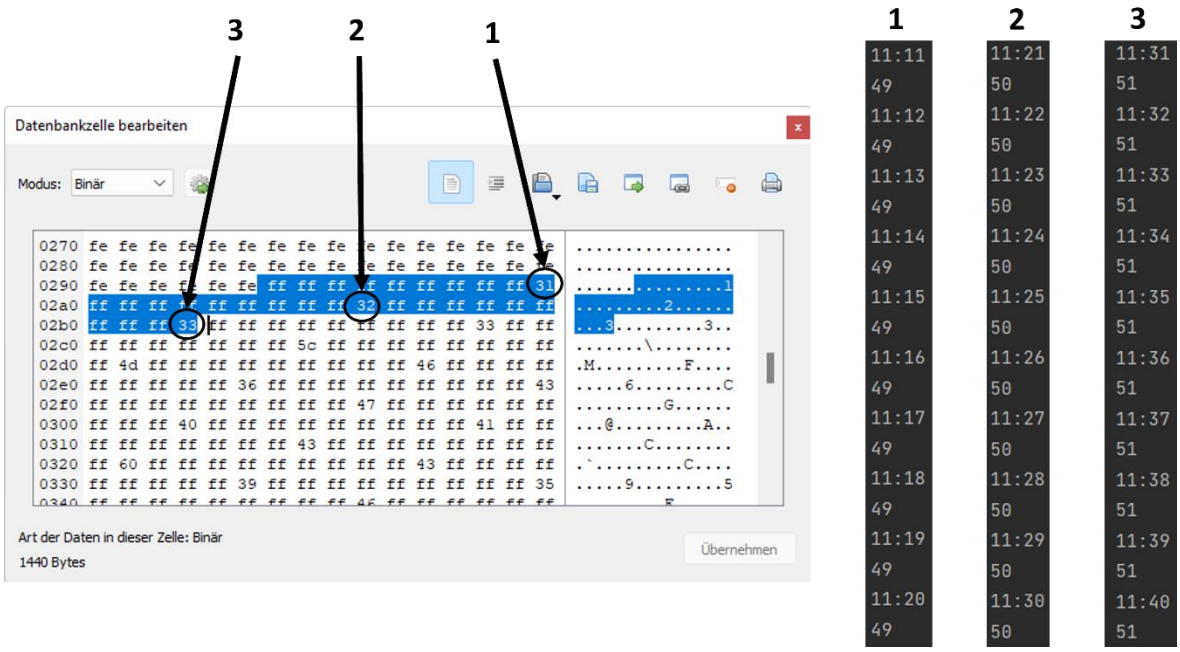


Abbildung 25: Extraktion der Herzfrequenzdaten aus der Datenbankzelle der „DATA_HR“-Spalte in der Tabelle „DATE_DATA“ (Zusammengeschnittene und bearbeitete Screenshots, Juli 2022)

Betrachtet man nun die Datenbankzelle der „STAGE_STEPS_SUMMARY“-Spalte (Abbildung 24, rechts), so fällt auf, dass die Daten in dieser Zelle im Datentyp JSON abgelegt sind. Innerhalb der Datenbankzelle fallen mehrere geschweifte Klammern auf, die jeweils sich wiederholende Namen-Wertepaare beinhalten. Im Datentyp JSON repräsentiert eine offene geschweifte Klammer den Beginn und eine geschlossene geschweifte Klammer das Ende eines neuen Objektes. Innerhalb dieses Objektes gibt es mehrere Namen-Wertepaare, die zusätzliche Daten oder Eigenschaften zu einem Objekt repräsentieren. Die Namen (vgl. Abbildung 24) sind dabei als String dargestellt. Darauffolgend wird ein Doppelpunkt als Zuweisungsoperator gesetzt und es folgt der Wert [71].

In der Abbildung 24 sind die JSON-Objekte, bestehend aus fünf Namen-Wertepaaren: „time, count, dis, cal, step“, deutlich erkennbar. Auffällig ist hierbei, dass der Wert bei „time“ zu Beginn der Datenbankzelle bei 0 beginnt und bis zum Ende auf 143 inkrementiert wird. Mit dem Wissen aus der Datenbankzelle der „DATA_HR“-Spalte könnten die 144 JSON-Objekte jeweils 10 Minuten eines Tages ab 0 Uhr (1440 = 1 Minute) entsprechen. Das Namen-Wertepaar „count“ hingegen ist selbst auf 0 gesetzt, wenn keine Änderungen der drei darauffolgenden Namen-Wertepaare eingetragen sind (Fitnesstracker abgelegt). Sobald Werte eingetragen werden (Fitnesstracker am Handgelenk), wird „count“ auf 1 inkrementiert. Blickt man auf die Namen der letzten drei Paare so ist es naheliegend, dass es sich bei „dis“ um die „distance“ (engl. = *distance;* dt. = Distanz), bei „cal“ um „calories“ (engl. = *calories;* dt. = Kalorien) und bei „step“ um „steps“ (engl. = *steps;* dt. = Schritte) handelt. Aus diesem Zusammenhang lässt sich zwar schlussfolgern, dass die Werte die gesuchten Schrittdaten beinhalten, jedoch nicht ob jedes JSON-Objekt für 10 Minuten eines Tages

stehen. Es wird daher eine dritte Hypothese aufgestellt, die folglich versucht wird zu verifizieren:

- **H3**: Jedes JSON-Objekt steht für 10 Minuten eines Tages.

Um die JSON-Objekte und deren Zeitstempel zu untersuchen sowie zu extrahieren, wird erneut auf das Skript aus der Anlage Teil 3 zurückgegriffen, um die Daten in eine übersichtliche Form umzuwandeln. Wie bereits bei den Herzfrequenzdaten erzeugt das selbst geschriebene Skript auch bei den Schrittdaten eine CSV-Datei und ein Diagramm, um die Daten am jeweiligen Tag übersichtlich darzustellen und entsprechend zu extrahieren.

In Abbildung 26 wird ersichtlich, dass sich das Namen-Wertepaar „count“ ab einer „time“ von 66 das erste Mal auf 1 setzt. Die darauffolgenden Werte müssten sich nun ebenfalls ändern, was sich bestätigte. Bei einer „time“ von 66 legte man 35 Schritte/25 Meter zurück und verbrauchte auf Basis der in der Fitnessapplikation angegeben Daten 1 kcal. Wenn sich „time“ von 0 an bis 143 inkrementiert und jeder „time“-Wert für 10 Minuten steht, so sind beim Wert 66 bereits 660 Minuten umgegangen, was bedeutet, dass der Fitnesstracker zwischen 11 Uhr und 11:10 Uhr angelegt wurde. Dies bestätigte sich bereits bei den Herzfrequenzdaten was für eine **Verifizierung** von **H3** spricht.

Die Abbildung 26 veranschaulicht zudem die Datenumwandlung der ersten 60 Minuten. Die gelben ovalen Kreise markieren die jeweils zu den gelben Pfeilen gehörige Uhrzeit beginnend mit 11 Uhr („time“:66) wohingegen die schwarzen ovale die zu extrahierende Schrittzahl in Verbindung mit den schwarzen Pfeilen darstellen. Im Gegensatz zu den Herzfrequenzdaten, sind die Schrittdaten in dezimaler Zahlenschreibweise abgelegt und bedürfen hier keiner zusätzlichen Umrechnung.

Abbildung 26: Extraktion der Schrittdaten aus der Datenbankzelle der „STAGE_STEPS_SUMMARY“-Spalte in der Tabelle „DATE_DATA“ (Zusammengeschnittene und bearbeitete Screenshots, Juli 2022)

Die festgestellten Verhaltensweisen sowie der Zeitpunkt der Datenaufzeichnung lassen eine **Verifizierung** der Hypothese **H3** ebenfalls zu.

3.7.2.2 Garmin

Der zweite Hersteller *Garmin* unterscheidet sich in Bezug auf die Datenbanktabellen vollständig vom bereits vorgestellten Hersteller *Xiaomi*. Bei der Extraktion der Schritt- und Herzfrequenzdaten wird auf die Tabelle „user_daily_summary“ verwiesen (vgl. Abbildung 27). Die Tabelle ist eine der größten in der Datenbank „cache-database“ und enthält eine Reihe an interessanten Informationen. Zum Überblick wird in der Tabelle „user_daily_summary“ eine tägliche Zusammenfassung der durch den Nutzer durchgeführten Tätigkeiten gegeben. Zur Übersicht werden nun alle Spalten einmal aufgezählt und anschließend die relevanten anschaulich dargestellt. Die Spalten der Tabelle lauten:

> „calendarDate, lastUpdated, displayName, totalKilocalories, activeKilocalories, bmrKilocalories, wellnessKilocalories, wellnessActiveKilocalories, burnedKilocalories, consumedKilocalories, remainingKilocalories, netCalorieGoal, netRemainingKilocalories, totalSteps, dailyStepGoal, totalDistanceMeters, wellnessDistanceMeters, highlyActiveSeconds, activeSeconds, sedentarySeconds, sleepingSeconds, moderateIntensityMinutes, vigorousIntensityMinutes, intensityMinutesGoal, floorsAscendedInMeters, floorsDescendedInMeters, floorsAscended, floorsDescended, userFloorsAscendedGoal, minHeartRate, maxHeartRate, restingHeartRate, lastSevenDaysAvgRestingHeartRate, averageStressLevel, maxStressLevel, stressDuration, restStressDuration, activityStressDuration, uncategorizedStressDuration, totalStressDuration, lowStressDuration, mediumStressDuration, highStressDuration, stressPercentage, restStressPercentage, activityStressPercentage, uncategorizedStressPercentage, lowStressPercentage, mediumStressPercentage, highStressPercentage, stressQualifier, measureableAwakeDuration, measureableAsleepDuration, lastSyncTimestampGMT, bodyBatteryChargedValue, bodyBatteryDrainedValue, bodyBatteryHighestValue, bodyBatteryLowestValue, bodyBatteryMostRecentValue, hydrationValueInML, hydrationGoalInML, averageSpo2, latestSpo2, avgMonitoringEnvironmentAltitude, avgWakingRespirationValue, highestRespirationValue, lowestRespirationValue, latestRespirationValue, latestRespirationTimeGMT”.

Insgesamt besteht die Tabelle somit aus 68 Spalten, die jeweils die unterschiedlichsten Informationen beinhalten. Da im Rahmen der Untersuchung auf die Herz- und Schrittdaten geblendet wird, werden die Spalten auf diese Informationen mit entsprechenden Zeitvermerk eingegrenzt und in Abbildung 27 dargestellt. Insgesamt sind mit Blick auf die Eingrenzung acht Spalten interessant. Zur Extraktion wird die Datenbank in die Software *DB Browser for SQLite* eingelesen und die entsprechend relevante Tabelle mit ihren Spalten herausgefiltert.

Wie in der Abbildung 27 dargestellt, stellen die ersten beiden Spalten einen Datums- und Unix-Zeitvermerk der letzten Aktualisierung dar (1651739797700 Sekunden seit dem 01. Januar 1970 = 05. Mai 2022; 10:36:37 GMT+0200). Aus forensischer Sicht ist dieser wichtig, wenn die dazugehörigen Herzfrequenz- und Schrittdaten in einen Zusammenhang gebracht werden sollen. Die Spalten drei und vier geben die gelaufenen Schritte sowie die insgesamt zurückgelegte Strecke in Metern am jeweiligen Tag an. Die Spalten fünf bis acht stellen eine ausführliche Auskunft über die Herzrate am ausgewählten Tag dar. So kann die minimale-, maximale-, Ruhe- sowie die Durchschnittsherzrate abgelesen werden.

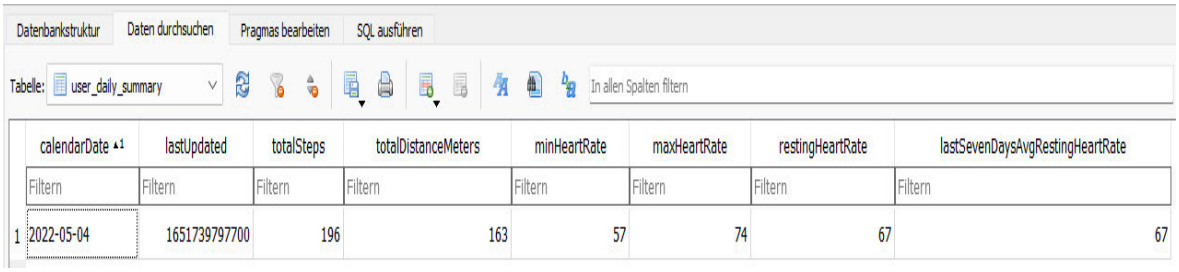


Abbildung 27: Ermittlungsrelevante Daten aus der Tabelle „user_daily_summary“ (Screenshot, Juli 2022)

Zur Extraktion wird nun mittels *DB Browser for SQLite* ein Export im CSV-Dateiformat (*Comma separated values*) durchgeführt. Im Gegensatz zu Teilkapitel 3.7.2.1 müssen die Daten bis auf die Unix-Zeitumrechnung nicht umformatiert werden, bevor diese extrahiert werden können. Alternativ steht eine manuelle Extraktion der Herzfrequenz- und Schrittdaten über die grafische Oberfläche der Fitnessapplikation zur Auswahl.

3.7.2.3 Fitbit

Der dritte und letzte Hersteller *Fitbit* stellt eine Besonderheit zu den anderen Herstellern dar. Als einzige Untersuchung wird hierbei nur eine Tabelle mit Herzfrequenzdaten betrachtet, da keine Schrittdaten detektiert werden konnten. Die ausgewählte Tabelle „HEART_RATE_DAILY_SUMMARY“ besteht aus vier Spalten:

„_id, DATE_TIME, AVERAGE_HEART_RATE, RESTING_HEART_RATE“.

Im Rahmen der Untersuchung wird die Tabelle auch hier wieder eingegrenzt und in Abbildung 28 dargestellt. In der ersten Spalte kann im Unix-Zeitformat der aktuelle Zeitstempel der jeweiligen Herzdaten abgelesen werden (1651312800000 Sekunden seit dem 01. Januar 1970 = 30. April 2022; 12:00:00 GMT+0200). Die Spalten zwei und drei geben die Durchschnitts- sowie die Ruheherzfrequenz am jeweiligen Tag des Unix-Zeitstempels an.

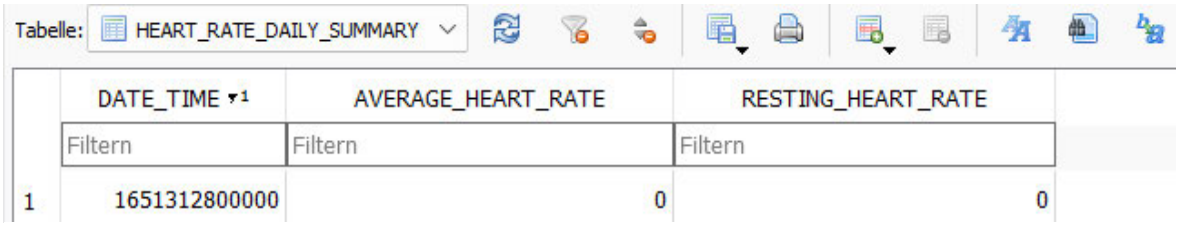


Abbildung 28: Ermittlungsrelevante Daten aus Tabelle „HEART_RATE_DAILY_SUMMARY“ (Screenshot, Juli 2022)

Die Extraktion funktioniert nach dem gleichen Prinzip wie beim Hersteller *Garmin* indem mittels *DB Browser for SQLite* ein Export im CSV-Dateiformat wird. Außer dem Unix-Zeitformat muss auch in dieser Tabelle nichts umformatiert werden, bevor die Daten extrahiert werden können. Alternativ steht auch hier eine manuelle Extraktion der Herzfrequenz- und Schrittdaten über die grafische Oberfläche der Fitnessapplikation zur Auswahl.

3.7.3 Extraktion aus Flash-Speicher

Dieses Teilkapitel gibt einen Einblick in die Datenextraktion aus einem Flash-Speicher-Chip. Wie aus dem Teilkapitel 3.6 hervorgeht, wird im Rahmen der Untersuchung eine Datenextraktion des Flash-Speicherchips *W25Q256JWPIM* in Betracht gezogen. Bevor die eigentliche Datensichtung- und Extraktion stattfinden kann, gibt es jedoch sowohl von Seiten der Hard- als auch Software einige Vorbereitungen zu treffen.

Zur Interpretation der im Flash-Speicherchip enthaltenen Daten wird der im Teilkapitel 3.2 beschriebene *BeeProg2* verwendet. Zunächst muss dabei der Gehäusetyp *WSON8* des *W25Q256JWPIM* beachtet werden. Für den *BeeProg2* existieren eine Reihe von Adaptern, die es ermöglichen, diverse Chips zu programmieren. Für die Untersuchung wurde im ersten Schritt der Spezial-Adapter *DIL8/QFN8-1 ZIF-CS SFlash-1a* zur Kompatibilität mit dem *BeeProg2* verwendet. Die Abbildung 29 veranschaulicht den eingesetzten Flash-Speicherchip *W25Q256JWPIM* im Spezial-Adapter. Dieser wird unter Beachtung des /CS-Pins sowie der gegebenen Markierung (markiert als Punkt mit einer 1, vgl. Teilkapitel 3.6) entsprechend eingesetzt.

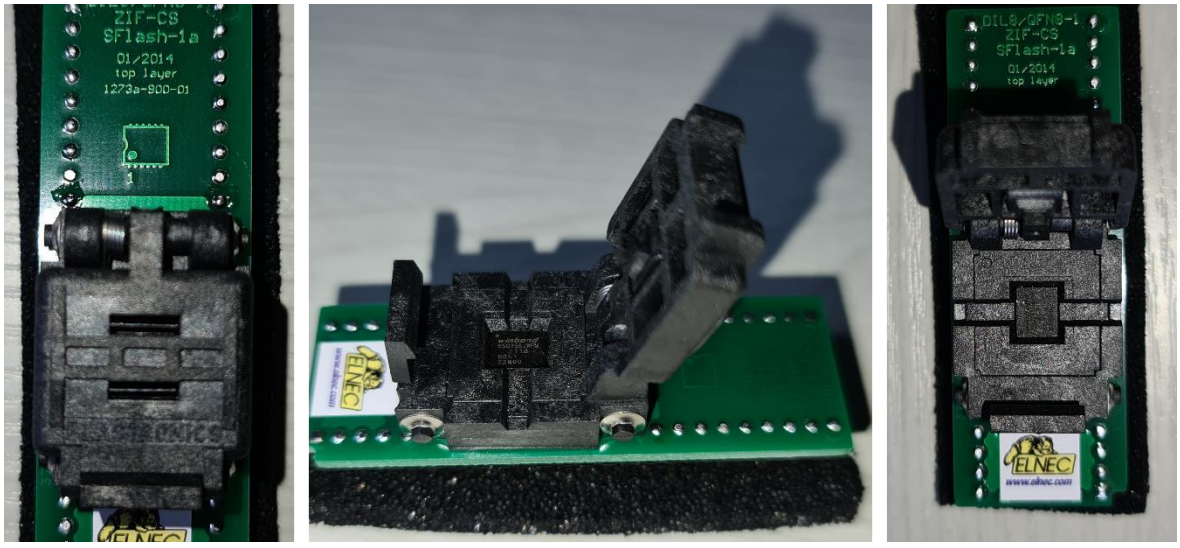


Abbildung 29: Flash-Speicherchip *W25Q256JWPIM* im Spezial-Adapter *DIL8/QFN8-1 ZIF-CS SFlash-1a* (Eigene zusammengeschnittene Aufnahmen, Juli 2022)

Im zweiten Schritt der Extraktion wird der Adapter nun im *BeeProg2* verankert. Dieser muss dafür auf das 48-Pin-Gehäuse des *BeeProg2* gesteckt und anschließend festgeklemmt werden. Die Abbildung 30 zeigt den Adapter im *BeeProg2*. Bei der Verankerung des Adapters gibt es eine Reihe von Schritten zu beachten. Zuerst wird der Staubschutz entfernt, der

über dem Gehäuse liegt und dieses vor äußeren Einflüssen schützt. Der Aluminium-Hebel am unteren rechten Ende des Gehäuses ist für die Verankerung der Stecker verantwortlich. Ist dieser nach unten gedrückt, so sind die Pin-Eingänge geschlossen. Für die Installation des Adapters wird der Hebel folglich nach oben gedrückt, der Adapter eingesetzt und anschließend wieder nach unten gedrückt. Auch beim Einsetzen gibt es eine Besonderheit zu beachten. Der obere linke Pin der 48-Adapter-Pins ist als einziger quadratisch mit einem Punkt in der Mitte angelötet. Dieser Pin muss auch im *BeeProg2* oben links verankert werden.

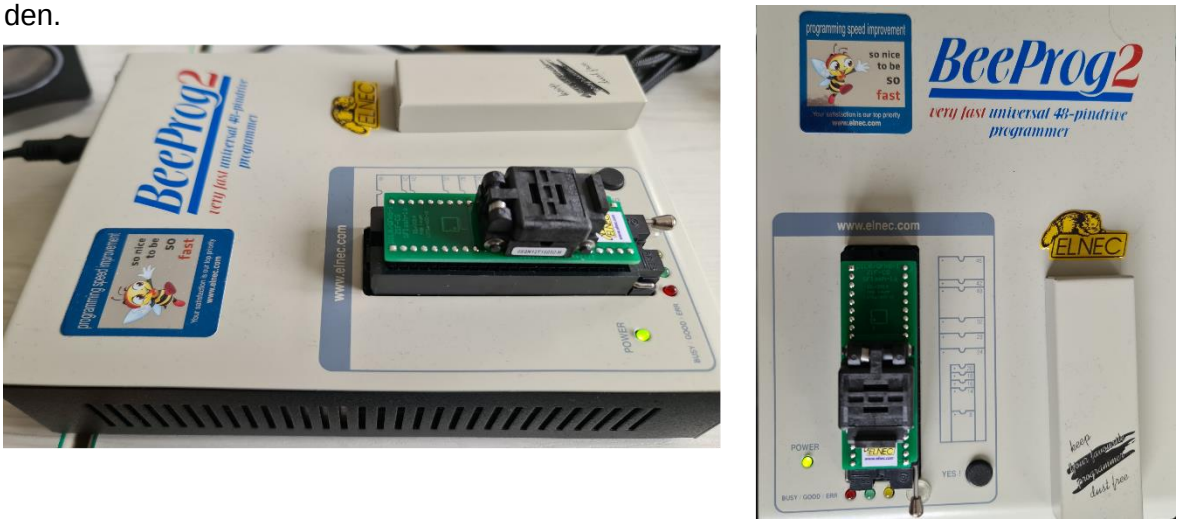


Abbildung 30: Spezial-Adapter *DIL8/QFN8-1 ZIF-CS SFlash-1a* im *BeeProg2* (Eigene zusammengeschnittene Aufnahmen, Juli 2022)

Im dritten und letzten Schritt der Extraktion wird der im Adapter eingesetzte Chip nun eingelesen und versucht, die Daten zu extrahieren. Der *BeeProg2* muss dafür an den Strom angeschlossen und über eine USB-Verbindung mit dem Untersuchungsgerät (*HP*-Laptop) verbunden werden. Sind alle Anschlüsse getätigt, so wird der *BeeProg2* eingeschaltet und das Steuerprogramm *PG4UW* gestartet. Das Steuerprogramm durchsucht selbstständig die USB-Schnittstellen des *HP*-Laptops und detektiert angeschlossene *Elnec*-Produkte automatisch. Nachdem alles ordnungsgemäß detektiert wurde, muss folglich das Bauteil in der Software ausgewählt werden. *PG4UW* verfügt über eine integrierte Datenbank die diverse Hersteller mit den jeweiligen Chips beinhaltet. Die Bauteil-Familie wurde folglich ausgewählt und der Lesevorgang gestartet.

Die Abbildung 31 veranschaulicht den Lesevorgang. Das Steuerprogramm stellt ein Informationsfenster zur Verfügung, welches den aktuellen Status des Lesevorgangs, die Position im Bauteil sowie im Puffer darstellt. Der Puffer erfüllt eine wichtige Aufgabe, da in diesem der gelesene Inhalt geschrieben und zwischengespeichert wird. Am Programmiergerät können zudem, wie in der Infoanzeige dargestellt, drei Farben an drei LEDs (Light Emitting Diode) eingesehen werden, die über den jeweiligen Status des Gerätes Auskunft geben. Letztlich wird noch die Bauteil-Familie farblich hervorgehoben. Ist der Chip in den Puffer eingelesen wurden, so wird der Puffer zum Schluss mit dem Chip-Inhalt verglichen/verifiziert, um mögliche Lesefehler auszuschließen.

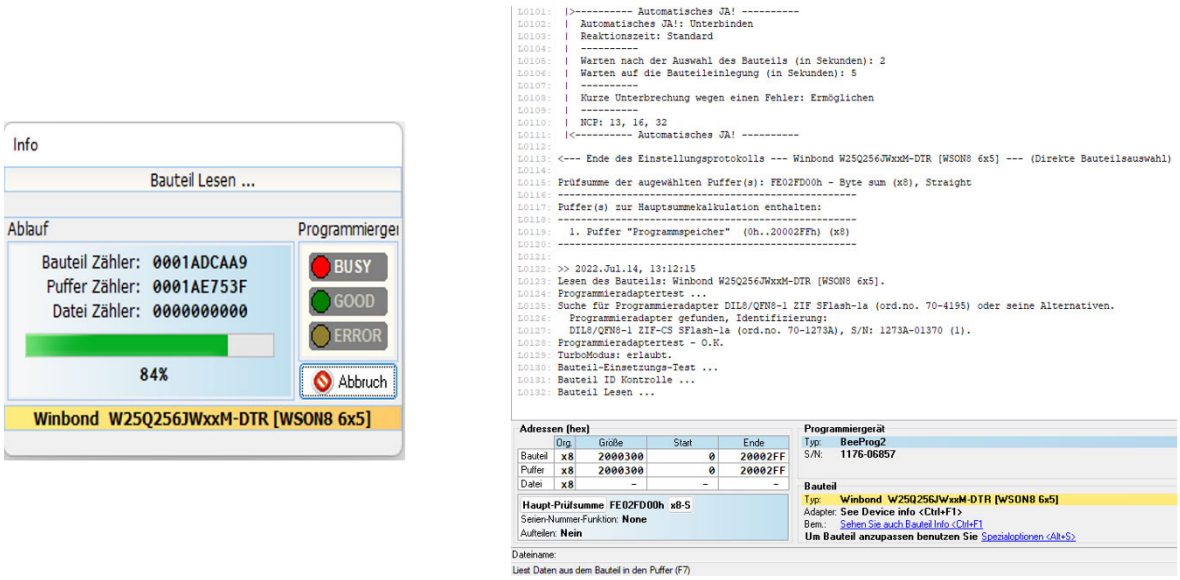


Abbildung 31: Lesevorgang *PG4UW* (Zusammengeschnittene Screenshots, Juli 2022)

Zur finalen Extraktion wird der Puffer nun als Binärdatei/Binärabbild auf dem Untersuchungsgerät abgespeichert und manuell mittels eines Editors sowie weiterer hilfreicher Tools interpretiert. Weiterführend sei auf das Teilkapitel 4.3 verwiesen, welches einen Einblick in die gewonnenen Ergebnisse aus der Binärdatei gibt. Die Extraktion der im Flash-Speicherchip enthaltenen Daten ist somit abgeschlossen.

4 Ergebnisse

Gegenstand dieses Kapitels sind die Ergebnisse, die man mit Blick auf die in der Untersuchung gesetzten Ziele (vgl. Teilkapitel 1.2) erreichen konnte. Dabei werden die Grundlagen, Materialen und Methoden aus den vorrangegangenen Teilkapiteln in einen Gesamtzusammenhang gebracht. Im ersten Teilkapitel wird auf das Synchronisations- und Speicherverhalten der Fitnesstracker/Fitness-Smartwatch geblendet. Das zweite Teilkapitel geht dann auf die Ergebnisse der Zugangsmöglichkeiten ein, um darauffolgend zu erörtern, welche Zugangsmöglichkeiten unter der bearbeiteten Problemstellung für den Ermittler bestehen. Zum Schluss werden die Ergebnisse der Datenextraktion aus Teilkapitel 3.7.3 reflektiert, welche komplexere Alternativen, zu den im Teilkapitel 4.2 beschriebenen Möglichkeiten darstellen.

4.1 Synchronisations- und Speicherverhalten

Im Teil 1 der Zielsetzung (vgl. Teilkapitel 1.2) stand im Vordergrund des Interesse zu untersuchen, ob der/die ausgewählte Fitnesstracker/Fitness-Smartwatch selbst Daten speichern kann. Hierfür musste zunächst ein einheitliches Untersuchungsdesign erstellt werden. Im Rahmen der Untersuchungen einigte man sich daher auf einen Synchronisationsabstand von einem, vier und sieben Tag/en, in welchem für jedes Gerät die in Teilkapitel 3.5.1 beschriebenen Methoden zur Datensicherung und die in Teilkapitel 3.7.2 verwendeten Methoden zur Datenextraktion angewandt wurden. Während der Synchronisierungszeiträume fanden die ausgewählte/n Fitnesstracker/Fitness-Smartwatch als alleinstehende Systeme Anwendung und wurden bis zum Synchronisierungszeitpunkt nicht mit dem Simulationsgerät verbunden. So konnten unter gleichen Bedingungen die Synchronisierungs- und Speicherverhaltensauffälligkeiten jedes Herstellers verglichen werden.

4.1.1 Xiaomi Mi Smart Band 6

Als erstes Gerät wurde das *Xiaomi Mi Smart Band 6* unter den definierten Bedingungen auf das Synchronisations- und Speicherverhalten hin untersucht. Zum Zeitpunkt der Untersuchung war auf dem Band die Firmware-Version 1.0.6.16 und auf dem Simulationsgerät die Applikationsversion 6.0.2 installiert. Zur Verifizierung benutzte man zwei verschiedene Methoden. Zum einem griff man auf das Vorwissen (vgl. Teilkapitel 3.7.2.1) zurück, um zu untersuchen, ob sich die Datenbankzeilen um die jeweiligen Tagesabstände ergänzen, der Fitnesstracker die Daten also gespeichert hatte, zum anderen betrachtete man die ergänzten Daten in der Fitnessapplikation *Zepp Life*.

Die Ergebnisse der ersten Untersuchung sind anschaulich in der Abbildung 32 zusammengefasst. Der Start der Untersuchung war der 4. Mai 2022 (Tag 0). Ab diesem Tag wurde nach den jeweiligen Synchronisationsabständen, also einem, vier und sieben Tagen in der Datenbank auf dem Simulationsgerät nachgeschaut, ob sich die jeweiligen Zeilen der Tage zwischen den Synchronisierungen ergänzt haben. Die Abbildung 32 zeigt, dass das *Xiaomi Mi Smart Band 6* auch nach sieben Tagen alle Daten speicherte und bei der Synchronisierung an Tag 12 die jeweiligen Zeilen ab dem 9. Mai 2022 ergänzt wurden.

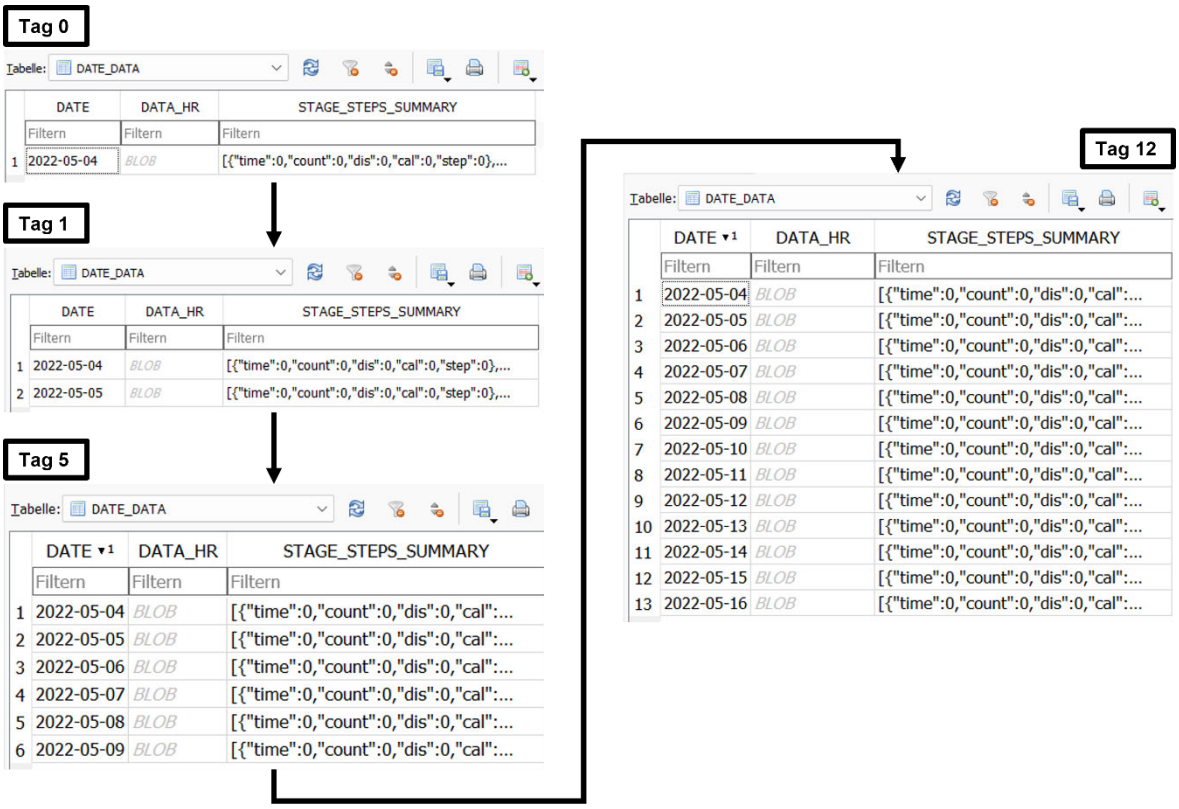


Abbildung 32: Synchronisations- und Speicherverhalten *Xiaomi Mi Smart Band 6* (Zusammengeschnittene und bearbeitete Screenshots, Juli 2022)

In der Fitnessapplikation wurden die Daten ebenfalls entsprechend aufbereitet. Es bestand hier die Möglichkeit, Zeiträume grafisch aufgearbeitet in Form von Diagrammen auszugeben.

Im Vergleich zur Forschungsarbeit von Jacoby [6], welche das *Xiaomi Mi Band 3* untersuchte, wurde in Bezug auf die aktuellen Ergebnisse eine deutliche Änderung in der Herzfrequenzmessung festgestellt. Während Jacoby [6] in Bezug auf die Herzfrequenz nur die Tabelle „HEART_RATE“ betrachtete und zum Ergebnis kam, dass der Fitnesstracker nur auf manuellem Befehl eine Herzfrequenz misst und nicht dauerhaft, wurde in dieser Forschungsarbeit gezeigt, dass das *Xiaomi Mi Smart Band 6* im Vergleich zu seinen Vorgängern eine dauerhafte Pulsmessung unterstützt (vgl. Teilkapitel 3.7.2.1).

Zusammengefasst ist das *Xiaomi Mi Smart Band 6* in der Lage, bis zu sieben Tage alleinstehend Daten aufzuzeichnen und diese selbst zu speichern.

4.1.2 Garmin Forerunner 55

Beim zweiten Untersuchungsgerät handelt es sich um die Fitness-Smartwatch *Garmin Forerunner 55*. Zum Zeitpunkt der Untersuchung war auf der Fitness-Smartwatch die Softwareversion 5.07 [DFU-5beea5] und auf dem Simulationsgerät die Applikationsversion 4.54.1 installiert. Die Methoden zur Untersuchung des Synchronisations- und Speicherverhaltens der Fitness-Smartwatch blieben dabei unverändert (vgl. Teilkapitel 4.1.1). In Bezug auf die Tabelle „user_daily_summary“ wurde entsprechend den Synchronisationsabständen auf ergänzende Zeilen und Änderungen in der Fitnessapplikation geachtet.

Die Abbildung 33 gibt einen Überblick über die Ergebnisse der Untersuchung. Parallel zum *Xiaomi Mi Smart Band 6* begann die Untersuchung am 4. Mai 2022. Im selben Synchronisationsabstand von einem, vier und sieben Tagen untersuchte man, ob die Fitness-Smartwatch alleinstehend Vitaldaten aufzeichnet, speichert und bei einer Synchronisierung teilen kann. Wie die Abbildung 33 deutlich zeigt, ist auch die *Garmin Forerunner 55* in der Lage, Vitaldaten eigenständig bis zu sieben Tage zu speichern. Entsprechend ab dem 9. Mai 2022 wurden die Zeilen der letzten sieben Tage seit letzter Synchronisierung ergänzt.

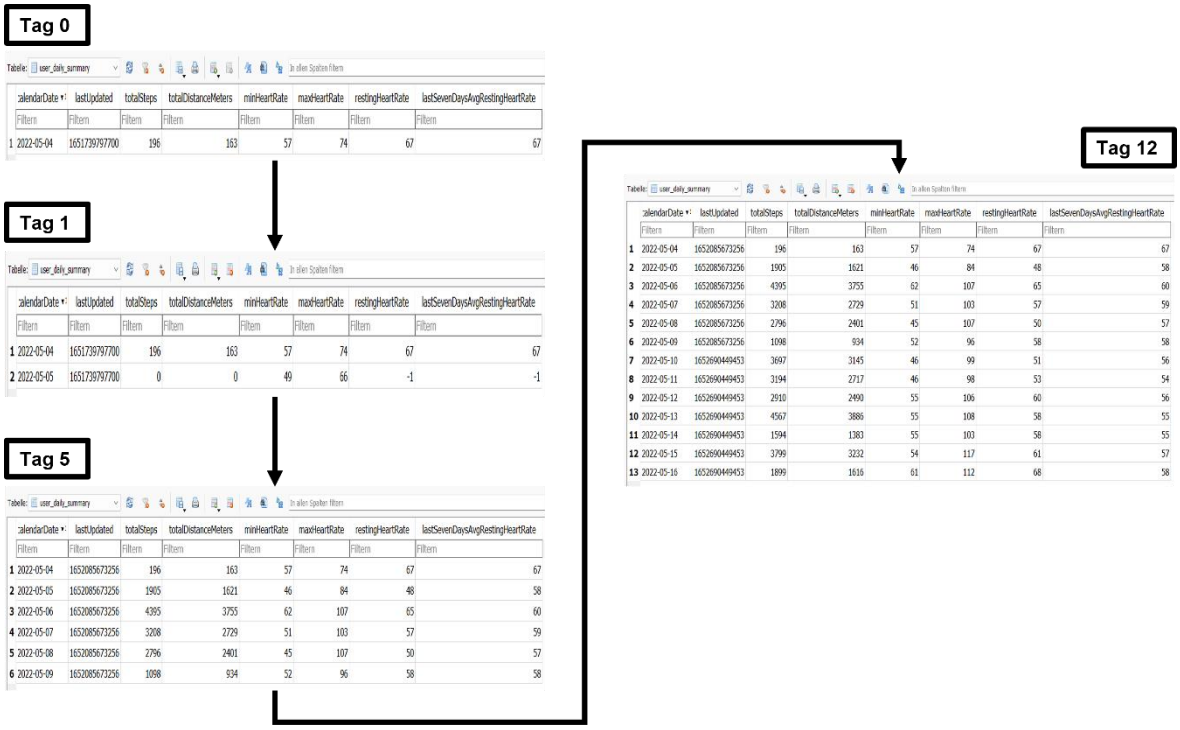


Abbildung 33: Synchronisations- und Speicherverhalten *Garmin Forerunner 55* (Zusammengeschnittene und bearbeitete Screenshots, Juli 2022)

Im Vergleich zu den Ergebnissen von Jacoby [6] sind bei der Tabelle „user_daily_summary“ die Spalten:

> „measureableAwakeDuration, measureableAsleepDuration, lastSyncTimestampGMT, bodyBatteryChargedValue, bodyBatteryDrainedValue, bodyBatteryHighestValue, bodyBatteryLowestValue, bodyBatteryMostRecentValue, hydrationValueInML, hydrationGoalInML, averageSpo2, latestSpo2,

avgMonitoringEnvironmentAltitude, avgWakingRespirationValue, highestRespirationValue, lowestRespirationValue, latestRespirationValue, latestRespirationTimeGMT",

neu hinzugekommen.

Wie im Teilkapitel 4.1.1 dargestellt, wurden in der Fitnessapplikation *Garmin Connect*™ die Daten entsprechend aufbereitet zur Verfügung gestellt. Es bestand auch hier die Möglichkeit, Zeiträume grafisch aufgearbeitet in Form von Diagrammen auszugeben.

Zusammengefasst ist die *Garmin Forerunner 55* in der Lage, bis zu sieben Tage alleinstehend Daten aufzuzeichnen und diese selbst zu speichern.

4.1.3 Fitbit Inspire 2

Das dritte, unter den definierten Bedingungen untersuchte Gerät, war der Fitnesstracker *Fitbit Inspire 2*. Zum Zeitpunkt der Untersuchung war auf dem Fitnesstracker die Firmware-Version 53.20001.124.28 (FIT OS, Aktivierung 02. Juni 2021) und auf der Fitnessapplikation die Version 3.58 (20263692) installiert. Die Ergebnisse unterscheiden sich deutlich zu den bereits vorgestellten. Wie auch in Teilkapitel 4.1.1 und 4.1.2 wurde der Fitnesstracker auf die drei festgelegten Synchronisationsabstände untersucht. Der Unterschied war hier, dass aus zeitlichen Gegebenheiten, mit Blick auf das Teilkapitel 4.2, zunächst ein, dann sieben und zur Vollständigkeit noch einmal vier Tage untersucht wurden.

In der Abbildung 34 können die Ergebnisse der Untersuchung eingesehen werden. Es fällt auf, dass in der untersuchten Tabelle sowohl nach einem als auch nach sieben Tagen Synchronisierung keine neuen Daten ergänzt wurden. Dies hat sich einerseits im „databases"-Ordner der *Fitbit*-Fitnessapplikation bemerkbar gemacht, da sich die 46 Datenbankdateien von ihrer Größe nicht verändert haben, andererseits ist auch keine neue Zeile bei der Synchronisierung in der Struktur der untersuchten Tabelle ergänzt worden. Die Tabelle beinhaltet 31 teils leere Zeilen die vom Unix-Zeitstempel her Zeilen vom 30. April 2022 bis zum 30. Mai 2022 (1651312800000 bis 1653904800000, 31 Tage) beinhalten.

Die Untersuchung selbst startete mit der Ein-Tag-Synchronisierung am 30. Mai 2022. Am 31. Mai 2022 folgte dann die Sieben-Tage-Synchronisierung bis zum 07. Juni 2022. Aus zeitlichen Gründen wurde mit Blick auf das Teilkapitel 4.2 bis zum 09. Juni 2022 eine zwei-Tage-Synchronisierung durchgeführt, weshalb ab dem 09. Juni 2022 dann bis zum 13. Juni 2022 die letzte Vier-Tage-Synchronisierung untersucht wurde. Blickt man nun auf die Tabellenstruktur am 14 Untersuchungstag, so ergänzten sich hier ab der 32-Zeile alle bisher gemessenen Werte der Ruheherzfrequenz ab dem 31. Mai 2022 bis zum letzten Tag dem

13. Juni 2022 (1653991200000 bis 1655114400000, 14 Tage). Auf mögliche Ursachen wird im Teilkapitel 5.3 geblendet.

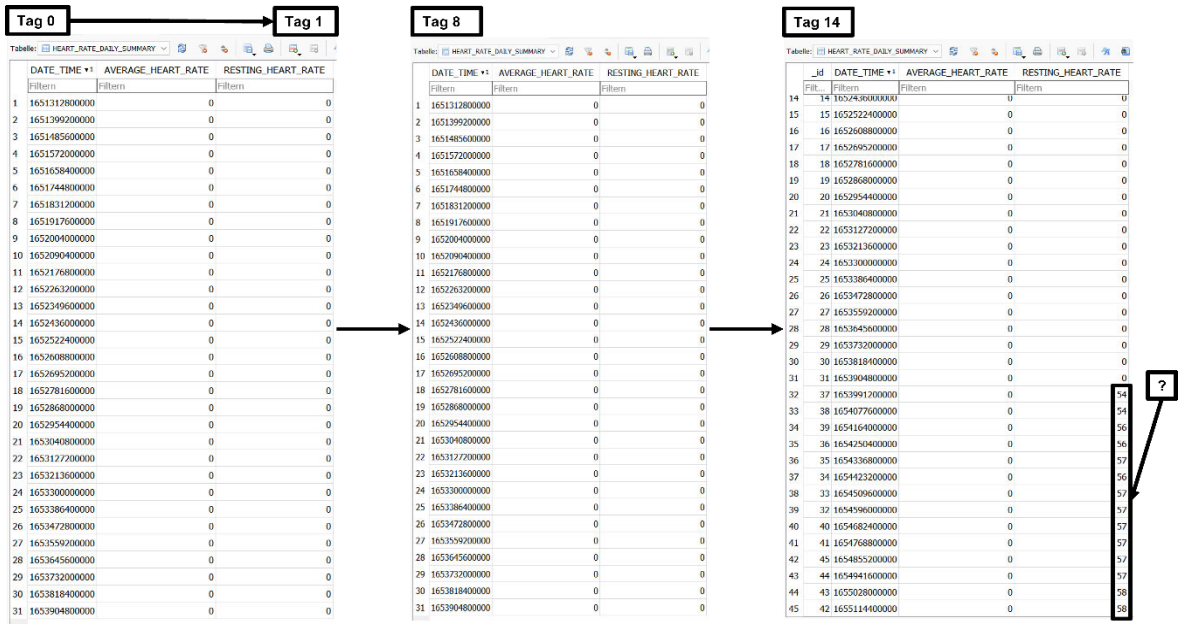


Abbildung 34: Synchronisations- und Speicherverhalten *Fitbit Inspire 2* (Zusammengeschnittene und bearbeitete Screenshots, Juli 2022)

Im Gegensatz zur Datenbank „HEART_RATE_DAILY_SUMMARY“ synchronisierten sich die Daten nach den jeweiligen Abständen mit der Fitnessapplikation von *Fitbit*. Nach den jeweiligen Zeiträumen konnte in der Applikation nachvollzogen werden, dass der Fitnesstracker die Daten selbstständig aufgenommen und gespeichert haben muss. Grafisch aufgearbeitet, wurden die jeweilige Herzfrequenz pro Tag und die gelaufenen Schritte in der Applikation dargestellt. Wie auch in den Teilkapiteln 4.1.1 und 4.1.2 aufgeführt, bestätigte die Applikation das Synchronisationsverhalten beim *Fitbit Inspire 2* auf alle drei Untersuchungszeiträume. Zudem konnten die nicht gefundenen Schrittdaten in der Datenbank durch die Applikation eingesehen werden.

Man fand zudem heraus, dass die *fitbit*-Fitnessapplikation als einzige untersuchte Applikation nur mit einer aktiven Internetverbindung in der Lage ist, Vitaldaten mit dem Fitnesstracker zu synchronisieren. Besteht keine Verbindung zum Internet, so ist die Applikationsoberfläche leer und man kann keine Synchronisierungen durchführen. Sobald eine Verbindung aufgebaut wurde, kann man sehen, wie sich die grafische Oberfläche mit den aktuellen Vitaldaten füllt und die Synchronisierung mit dem *Fitbit Inspire 2* unter der Bedingung, dass eine *Bluetooth*-Verbindung besteht, beginnt.

Zusammengefasst stellten sich die Ergebnisse aus der Untersuchung der *Fitbit Inspire 2* in ihren Zwischenständen als deutlich unterschiedlich im Gegensatz zu den vorherigen dar. Durch den Abgleich mit der Fitnessapplikation konnte jedoch auch hier am Ende nachgewiesen werden, dass der Fitnesstracker in der Lage ist, bis zu sieben Tage alleinstehend Daten aufzuzeichnen und diese selbst zu speichern.

4.2 Zugangsmöglichkeiten

Im Teilkapitel 4.1 konnte zunächst festgehalten werden, dass der/die ausgewählte Fitnesstracker/Fitness-Smartwatch selbst Daten speichern kann. Auf Grundlage dieser Ergebnisse beschäftigt sich dieses Teilkapitel ebenfalls mit dem ersten Teil der Zielsetzung (vgl. Teilkapitel 1.2) der Untersuchung, unter welcher Konstellation die auf Fitnesstrackern/Fitness-Smartwatches abgelegten Daten forensisch gesichert werden können. Um dies zu beantworten, wurde auch hier ein einheitliches Untersuchungsdesign verwendet. Da der Rahmen der Untersuchung definiert, über keine Zugriffsmöglichkeit zum ursprünglich gekoppelten Smartphone zu verfügen, wurde hierfür ein zweites baugleiches Simulationsgerät (*Raspberry Pi Model 4 B)* hinzugezogen. Dieses soll das Gerät, welches noch nie mit den Fitnesstrackern/Fitness-Smartwatches gekoppelt war, simulieren. Zudem wird unter dem Zugang durch bekannte und neue Nutzerdaten unterschieden. Hierfür wurden neben den bestehenden Fitnessapplikations-Accounts, neue Accounts auf dem zweiten Simulationsgerät (mit neuem *Google*-Konto) erstellt. Unter den bereits beschriebenen Methoden zur Datensicherung sowie Datenextraktion und einem festgelegten Synchronisationsabstand von zwei Tagen (zwischen bestehenden und neuem Account) konnten die Zugangsmöglichkeiten sowie die vorgefundenen Daten auf dem neuem Simulationsgerät untersucht werden. Im Folgenden werden die Ergebnisse für jeden Hersteller vorgestellt.

4.2.1 Zugang durch bekannte Nutzerdaten

Dieses Teilkapitel präsentiert die Ergebnisse, die bei einer Synchronisierung mit einem neuen Simulationsgerät und bekannten Nutzerdaten erzielt werden konnten. Nachdem die Untersuchungsergebnisse aus Teilkapitel 4.1 vorgestellt wurden, trennte man den/die Fitnesstracker/Fitness-Smartwatch vom ursprünglichen Simulationsgerät erzeugte alleinstehend zwei Tage Vitaldaten und versuchte, diese anschließend mit einem neuen Simulationsgerät und den bisher bekannten Nutzerdaten zu synchronisieren. Die Ergebnisse sind vielfältig sowie Herstellerspezifisch und werden im Folgenden präsentiert.

4.2.1.1 Xiaomi Mi Smart Band 6

Als erstes Gerät wurde der Fitnesstracker *Xiaomi Mi Smart Band 6* untersucht. Die Firmware-Version des Bandes sowie die Applikationsversion des Simulationsgerätes glichen hierbei zum Zeitpunkt der Untersuchung den Versionen aus dem Teilkapitel 4.1.1. Die Untersuchung begann am 16. Mai 2022. Der Fitnesstracker wurde dahingehend bis zum 18. Mai 2022 als alleinstehendes System verwendet, bevor er für die Untersuchung synchronisiert wurde.

Im ersten Schritt installierte man die Fitnessapplikation *Zepp Life* auf dem neuem Simulationsgerät und machte bereits hier erste Erkenntnisse. Nach der Installation zeigte sich, dass im Ordner der Fitnessapplikationsdaten (vgl. Teilkapitel 3.5) unter anderem noch kein „databases“-Ordner angelegt wurde.

Im nächsten Schritt wurde sich mit dem bereits bestehenden Account angemeldet. Man stellte fest, dass nach einer Anmeldung in der Applikation der Fitnesstracker nicht neu mit dem Account verknüpft werden musste, sondern bereits nach der Anmeldung auf einem neuen Gerät mit dem Account gekoppelt war. Das neue Simulationsgerät mit eingeschaltetem *Bluetooth* detektierte somit das *Xiaomi Mi Smart Band 6* und synchronisierte es nach der Anmeldung direkt mit der Fitnessapplikation. In der Fitnessapplikation selbst konnte man alle Daten die seit Beginn der Untersuchung, also dem 3. Mai 2022, erzeugt wurden einsehen. Auch die Ordnerstruktur änderte sich nach der Anmeldung. So tauchte der „databases“ Ordner wieder auf und bei einer anschließenden Analyse der Datenbank erhielt man weitere Erkenntnisse.

Die Abbildung 35 veranschaulicht die vorgefundene Tabelle (links) nach der Anmeldung und stellt als Vergleich die Schrittdaten in der Fitnessapp (rechts) dar, die bis zum 3. Mai 2022 feingranular zurückverfolgt werden können. Es fällt auf, dass auch in der Tabelle die Zeilen zurück bis zum 3. Mai 2022 ergänzt wurden. Dabei wurden alle Herzfrequenzdaten, die seit Beginn erzeugt wurden, in die Spalte „DATA_HR“ auf dem neuen Simulationsgerät ergänzt. Bei der Spalte „STAGE_STEPS_SUMMARY“ hingegen wurden nur die Schrittdaten seit der letzten Synchronisierung, also dem 16. Mai 2022 ergänzt. Die Fitnessapplikation zeigt jedoch, dass alle Schrittdaten dort bis zum 3. Mai 2022 grafisch eingesehen werden können.

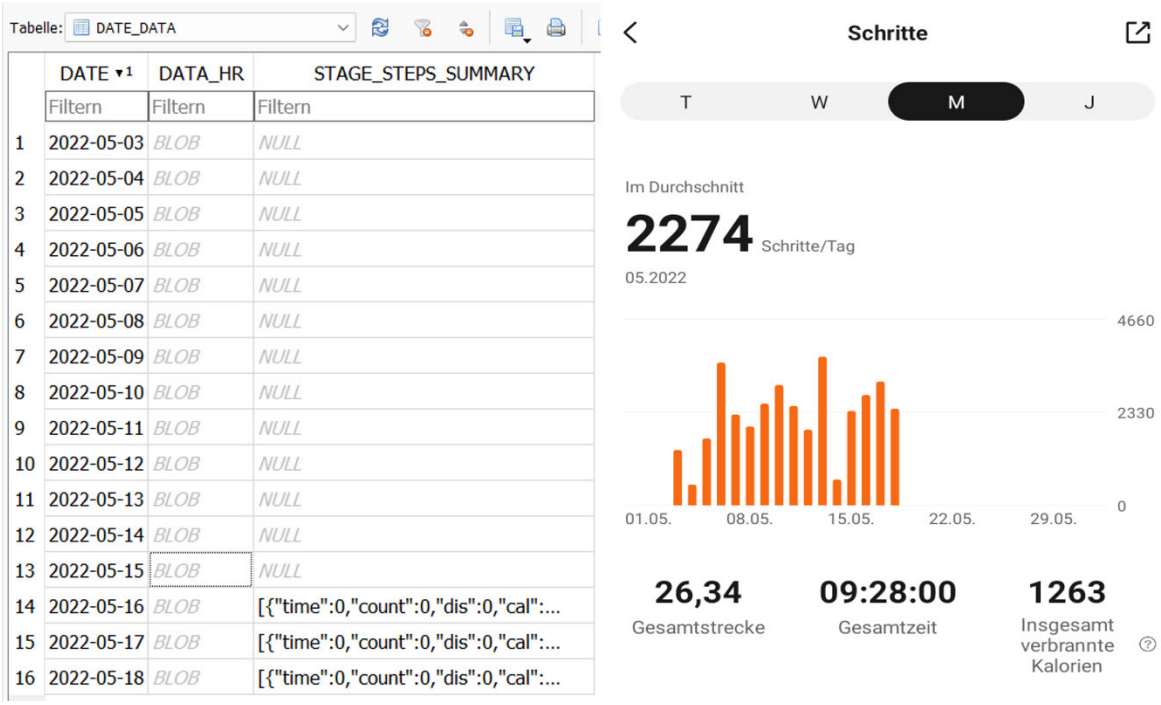


Abbildung 35: Ergebnisse - Zugang durch bekannte Nutzerdaten *Xiaomi Mi Smart Band 6* (Zusammengeschnittene Screenshots, Juli 2022)

Zusammengefasst können bei einem Zugang durch bekannte Nutzerdaten auf einem neuen Simulationsgerät, alle mit dem verknüpften Account erzeugten ermittlungsrelevanten Daten des *Xiaomi Mi Smart Band 6* eingesehen werden. Sowohl die Tabelle

als auch die Fitnessapplikation geben einen feingranularen Einblick in die erzeugten Vitaldaten, wobei in der Fitnessapplikation im Gegensatz zur Tabelle alle seit der Verknüpfung des Accounts erzeugten Schrittdaten eingesehen werden können.

4.2.1.2 Garmin Forerunner 55

Als zweites Gerät wurde die Fitness-Smartwatch *Garmin Forerunner 55* untersucht. Zum Zeitpunkt der Untersuchung war auf der Fitness-Smartwatch die Softwareversion 4.11 [DFU-5beea5] und auf dem Simulationsgerät die Applikationsversion 4.54.1 installiert. Die Untersuchung startete auch hier parallel zum *Xiaomi Mi Smart Band 6* am 16. Mai 2022 und endete am 18. Mai 2022 in der Synchronisierung mit dem neuen Simulationsgerät.

Als erster Bearbeitungsschritt wurde die *Garmin Connect*™-Fitnessapplikation installiert. Es zeigte sich auch hier, dass in den Fitnessapplikationsdaten kein „databases"-Ordner erzeugt wurde.

Nach einer erfolgreichen Anmeldung betrachtete man im zweiten Bearbeitungsschritt zunächst die Fitnessapplikation. In dieser synchronisierten sich nach der Anmeldung alle Vitaldaten, die seit dem 4. Mai 2022 (Beginn der Untersuchung) bis zum Zeitpunkt der letzten Synchronisierung (16. Mai 2022) erzeugt wurden. Ein Blick in die Ordnerstruktur der Fitnessapplikationsdaten zeigte, dass eine Anmeldung den „databases"-Ordner erstellte. Die gesuchte „cache-database" ist jedoch nicht vorhanden gewesen. Im Gegensatz zum *Xiaomi Mi Smart Band 6* war die *Garmin Forerunner 55* nicht mit dem Account verknüpft und musste daher im nächsten Schritt neu gekoppelt werden.

Für eine neue Verknüpfung setzte man die Fitness-Smartwatch zunächst in den Kopplungsmodus. Die Fitnessapplikation erkannte auf dem neuem Simulationsgerät bei eingeschaltetem *Bluetooth* die Fitness-Smartwatch und man konnte diese mittels eines Kopplungscodes nun verknüpfen. Nach der erfolgreichen Verknüpfung begann die Fitnessapplikation die Daten aus der Fitness-Smartwatch zu synchronisieren.

Die Abbildung 36 veranschaulicht die Ergebnisse aus der Synchronisierung mit der Fitnessapplikation. Im „databases"-Ordner erschien die „cache-database" mit der Tabelle „user_daily_summary" (oben) und konnte als erstes eingesehen werden. In dieser stellte man fest, dass die Zeilen ab dem Untersuchungstag (18. Mai 2022) bis sieben Tage zurück (12. Mai 2022) in die Tabelle geschrieben wurden. In allen Spalten, auf die man sich eingrenzte, konnten die jeweiligen Werte eingesehen werden. In der darunter abgebildeten Übersicht der Herzfrequenzdaten ist zudem deutlich zu erkennen, dass nun ab dem 04. Mai 2022 bis zum 18. Mai 2022 die fehlenden Herzfrequenzdaten durch eine Synchronisierung mit der *Garmin Forerunner 55* ergänzt wurden.

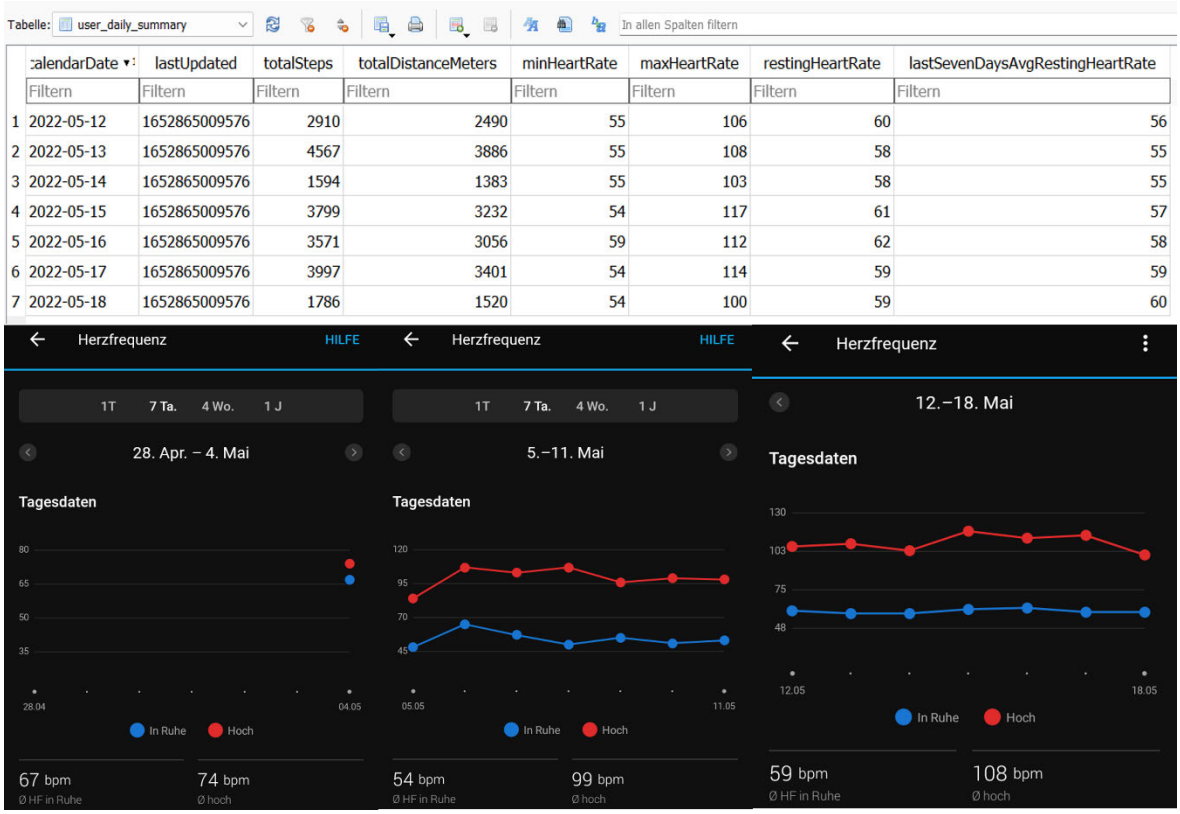


Abbildung 36: Ergebnisse - Zugang durch bekannte Nutzerdaten *Garmin Forerunner 55* (Zusammengeschnittene Screenshots, Juli 2022)

Zusammengefasst können bei einem Zugang durch bekannte Nutzerdaten auf einem neuen Simulationsgerät alle mit dem verknüpften Account erzeugten ermittlungsrelevanten Daten der *Garmin Forerunner 55* eingesehen werden. In der Tabelle selbst können im Gegensatz zur Fitnessapplikation nur die erzeugten Daten der letzten sieben Tage eingesehen werden.

4.2.1.3 Fitbit Inspire 2

Als letztes Gerät wurde der Fitnesstracker *Fitbit Inspire 2* untersucht. Zum Zeitpunkt der Untersuchung war auf dem Fitnesstracker die Firmware-Version 53.20001.124.28 (FIT OS, Aktivierung 2. Juni 2021) und auf der Fitnessapplikation die Version 3.59.1 (20263715) installiert. Die Untersuchung startete am 7. Juni 2022 und wurde am 9. Juni 2022 durch eine Synchronisierung mit dem neuen Simulationsgerät beendet.

Zu Beginn installierte man die *fitbit*-Fitnessapplikation. Mit Blick auf die Fitnessapplikationsdaten fand man auch hier zunächst eine leere Ordnerstruktur mit fehlendem „databases“-Ordner vor.

Im Folgenden galt es die bestehenden Accountdaten zur Anmeldung auf dem neuen Simulationsgerät zu verwenden, um neue Erkenntnisse zu gewinnen. Nach einer Anmeldung in der Fitnessapplikation zeigte sich, dass der Fitnesstracker nicht erneut mit dem Gerät gekoppelt werden muss, da er mit dem bestehenden Account verknüpft war. Die

Fitnessapplikation startete somit automatisch nach Anmeldung und eingeschaltetem *Bluetooth* auf dem Simulationsgerät die Synchronisierung mit dem Fitnesstracker. In der Fitnessapplikation selbst synchronisierten sich alle Vitaldaten, die seit Beginn der Untersuchung mit dem Account und dem Fitnesstracker erzeugt wurden (31. Mai 2022). Auch der „database“-Ordner wurde angezeigt und erbrachte bei der Untersuchung der „heart_rate_db“ neue Erkenntnisse.

Die Abbildung 37 veranschaulicht die Ergebnisse nach einer Synchronisierung mit dem *Fitbit Inspire 2*. In der Tabelle (links) ist deutlich zu erkennen, dass ab dem 31. Mai 2022 (165399120000) bis zum aktuellen Synchronisierungszeitpunkt (9. Juni 2022 – 1654768800000) die Ruheherzfrequenz in die jeweiligen Zeilen der Tage geschrieben wurde. Auch ein Blick in die Fitnessapplikation (rechts) zeigt, dass die Herzfrequenz durch die Anmeldung und anschließende Synchronisierung von Beginn an bis zum 9. Juni 2022 grafisch eingesehen werden kann.

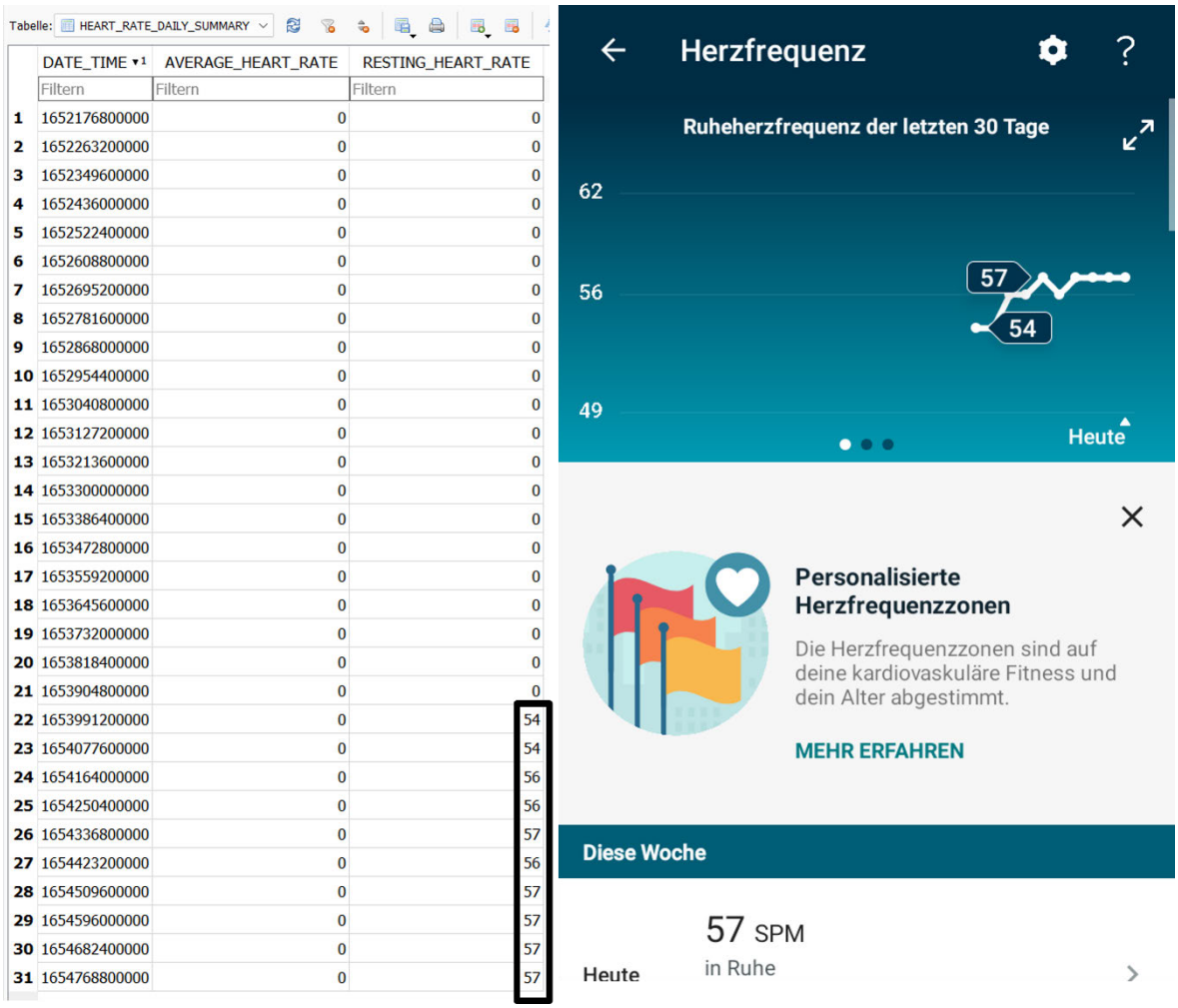


Tabelle: HEART_RATE_DAILY_SUMMARY

	DATE_TIME	AVERAGE_HEART_RATE	RESTING_HEART_RATE
	Filtern	Filtern	Filtern
1	1652176800000	0	0
2	1652263200000	0	0
3	1652349600000	0	0
4	1652436000000	0	0
5	1652522400000	0	0
6	1652608800000	0	0
7	1652695200000	0	0
8	1652781600000	0	0
9	1652868000000	0	0
10	1652954400000	0	0
11	1653040800000	0	0
12	1653127200000	0	0
13	1653213600000	0	0
14	1653300000000	0	0
15	1653386400000	0	0
16	1653472800000	0	0
17	1653559200000	0	0
18	1653645600000	0	0
19	1653732000000	0	0
20	1653818400000	0	0
21	1653904800000	0	0
22	1653991200000	0	54
23	1654077600000	0	54
24	1654164000000	0	56
25	1654250400000	0	56
26	1654336800000	0	57
27	1654423200000	0	56
28	1654509600000	0	57
29	1654596000000	0	57
30	1654682400000	0	57
31	1654768800000	0	57

Abbildung 37: Ergebnisse - Zugang durch bekannte Nutzerdaten *Fitbit Inspire 2* (Zusammengeschnittene und bearbeitete Screenshots, Juli 2022)

Zusammengefasst können bei einem Zugang durch bekannte Nutzerdaten auf einem neuen Simulationsgerät alle mit dem verknüpften Account erzeugten

ermittlungsrelevanten Daten der *Fitbit Inspire 2* eingesehen werden. Die Fitnessapplikation gibt hier einen feingranularen und grafischen Einblick in die erzeugten Vitaldaten. Die Tabelle hingegen gibt Auskunft über die Ruheherzfrequenz, die seit Beginn der Nutzung aufgezeichnet wurde.

4.2.2 Zugang durch neue Nutzerdaten

Gegenstand dieses Teilkapitels ist die Vorstellung der Ergebnisse, die bei einer Synchronisierung mit einem neuen Simulationsgerät und neu erstellten Nutzerdaten erzielt werden können. Die Untersuchungsmethodik ist hierbei dieselbe wie im Teilkapitel 4.2.1. Damit die Untersuchung unter gleichen Bedingungen wie im vorherigen Teilkapitel durchgeführt werden kann, wurden alle Fitnessapplikationen mit den jeweils dazugehörigen Fitnessapplikationsdaten zu Beginn vom neuen Simulationsgerät entfernt. Die Ergebnisse sind auch hier vielfältig sowie Herstellerspezifisch und werden im Folgenden präsentiert.

4.2.2.1 Xiaomi Mi Smart Band 6

Als erstes Gerät wurde der Fitnesstracker *Xiaomi Mi Smart Band 6* untersucht. Die Firmware-Version des Bandes sowie die Applikationsversion des Simulationsgerätes glichen hierbei zum Zeitpunkt der Untersuchung den Versionen aus dem Teilkapitel 4.2.1.1. Die Untersuchung startete am 18. Mai 2022 und lief unter den definierten Bedingungen bis zum 20. Mai 2022.

Im ersten Schritt wurde auch hier die dazugehörige Fitnessapplikation *Zepp Life* installiert. Die nach der Installation vorgefundene Ordnerstruktur glich dabei der Struktur aus dem Teilkapitel 4.2.1.1, in welcher kein „databases“-Ordner vorhanden war. Im Unterschied zur vorherigen Untersuchungsmethodik wird im folgenden Teilkapitel ein neuer *Zepp Life*-Account mit den *Google*-Konto-Daten des neuen Simulationsgerätes erzeugt.

Nach der Erstellung des Accounts meldete man sich im zweiten Schritt in der Fitnessapplikation an und betrachtete die definierte Datenbank sowie die Oberfläche aus der Fitnessapplikation. Die Fitnessapplikationsdaten-Ordnerstruktur erschien nach der Anmeldung und wurde als erstes begutachtet.

Die Abbildung 38 veranschaulicht die Ergebnisse nach einer Anmeldung, die mit einem neuem Account erzielt werden konnten. Sowohl die Tabelle „DATE_DATA“ (links oben) als auch die Benutzeroberfläche der Fitnessapplikation (links unten) beinhalteten keinerlei ermittlungsrelevante Daten. Da die Ausführungen im Teilkapitel 4.2.1.1 gezeigt haben, dass der ursprüngliche Account mit dem Fitnesstracker verknüpft ist, wurde im Folgenden versucht, das *Xiaomi Mi Smart Band 6* mit dem neuen Account zu verknüpfen.

Beim Versuch den Fitnesstracker im dritten Schritt neu zu koppeln, stellte man fest, dass dieser zunächst vom alten Simulationsgerät entkoppelt oder auf Werkseinstellungen zurückgesetzt werden musste. Da das Untersuchungsdesign jedoch definiert, kein altes

Simulationsgerät zur Verfügung zu haben, blieb nur noch die Variante den Fitnesstracker auf seine Werkseinstellungen zurückzusetzen. Auch diese Variante wurde ausgeschlossen, da ein Zurücksetzen sämtliche ermittlungsrelevante Daten löschen würde.

Die Abbildung 38 veranschaulicht die gezeigte Fehlermeldung (rechts), die nicht umgangen werden kann. An dieser Stelle sei auf das Teilkapitel 4.3 verwiesen, in welchem eine Alternative Untersuchungsmethodik des Fitnesstrackers betrachtet wird.

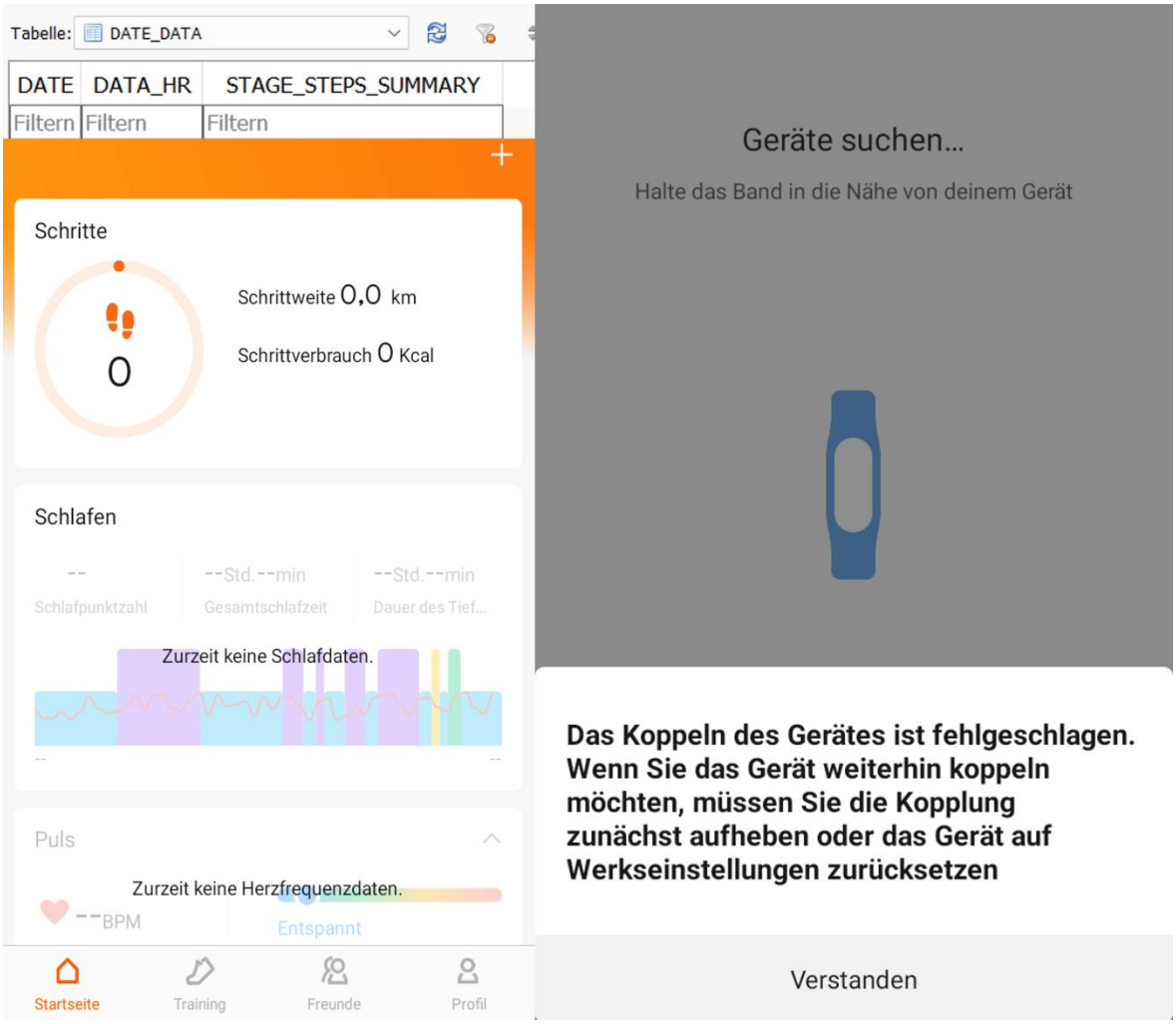


Abbildung 38: Ergebnisse - Zugang durch neue Nutzerdaten *Xiaomi Mi Smart Band 6* (Zusammengeschnittene und bearbeitete Screenshots, Juli 2022)

Zusammengefasst können bei einem Zugang durch neue Nutzerdaten auf einem neuen Simulationsgerät, keine ermittlungsrelevanten Daten des *Xiaomi Mi Smart Band 6* eingesehen werden. Eine Untersuchung der Tabelle und Fitnessapplikation blieb ohne Erfolg.

4.2.2.2 Garmin Forerunner 55

Als zweites Gerät wurde die Fitness-Smartwatch *Garmin Forerunner 55* untersucht. Zum Zeitpunkt der Untersuchung war auf der Fitness-Smartwatch die Softwareversion 5.07 [DFU-5beea5] und auf dem Simulationsgerät die Applikationsversion 4.54.1 installiert. Die

Untersuchung startete auch hier parallel zum *Xiaomi Mi Smart Band 6* am 18. Mai 2022 und endete am 20. Mai 2022 in der Anmeldung und Synchronisierung mit dem neuen Simulationsgerät.

Im ersten Schritt wurde zunächst auch hier die *Garmin Connect*™-Fitnessapplikation installiert. Die Fitnessapplikationsdaten und deren Ordnerstruktur waren ebenfalls noch leer und enthielten kein „databases“-Ordner. Nach der Installation erzeugte man auf dem neuen Simulationsgerät einen neuen *Garmin Connect*™-Account mit den Daten des *Google*-Kontos.

Nachdem der Account erstellt wurde, meldete man sich im zweiten Schritt in der Applikation an und fand zunächst sowohl in der nun erschienenen Datenbank als auch in der Fitnessapplikation keine ermittlungsrelevanten Daten vor. Im Unterschied zum vorherigen Teilkapitel detektierte jedoch die Fitnessapplikation unmittelbar nach der Anmeldung die in der Nähe am Handgelenk getragene *Garmin Forerunner 55* und stellte dem Nutzer die Möglichkeit einer Synchronisierung zur Auswahl. Diese Möglichkeit nahm man wahr und synchronisierte die Uhr unmittelbar nach der Anmeldung mit dem neuen Account.

Die nun sichtbaren Daten waren forensisch wertvoll und sind in der Abbildung 39 dargestellt. Nachdem die Fitness-Smartwatch fertig synchronisiert wurde, begutachtete man zunächst die „cache-database“. In der Tabelle „user_daily_summary“ (oben) fand man nun Einträge vor, die die letzten drei Tage an detektierten Vitaldaten beinhalteten. Das bedeutet, dass die *Garmin Forerunner 55* sämtliche Daten seit Beginn der Untersuchung (18. Mai 2022) aufgezeichnet, gespeichert und in die Datenbank der Fitnessapplikation geschrieben hat, obwohl man ein vollständig neu erzeugten Account verwendete. Ein Blick in die Übersicht der Herzfrequenz- und Schrittdaten in der Fitnessapplikation (unten) bestätigten die Ergebnisse aus der Tabelle. Sämtliche ermittlungsrelevante Daten sind seit dem 18. Mai 2022 grafisch aufbereitet und können begutachtet werden.

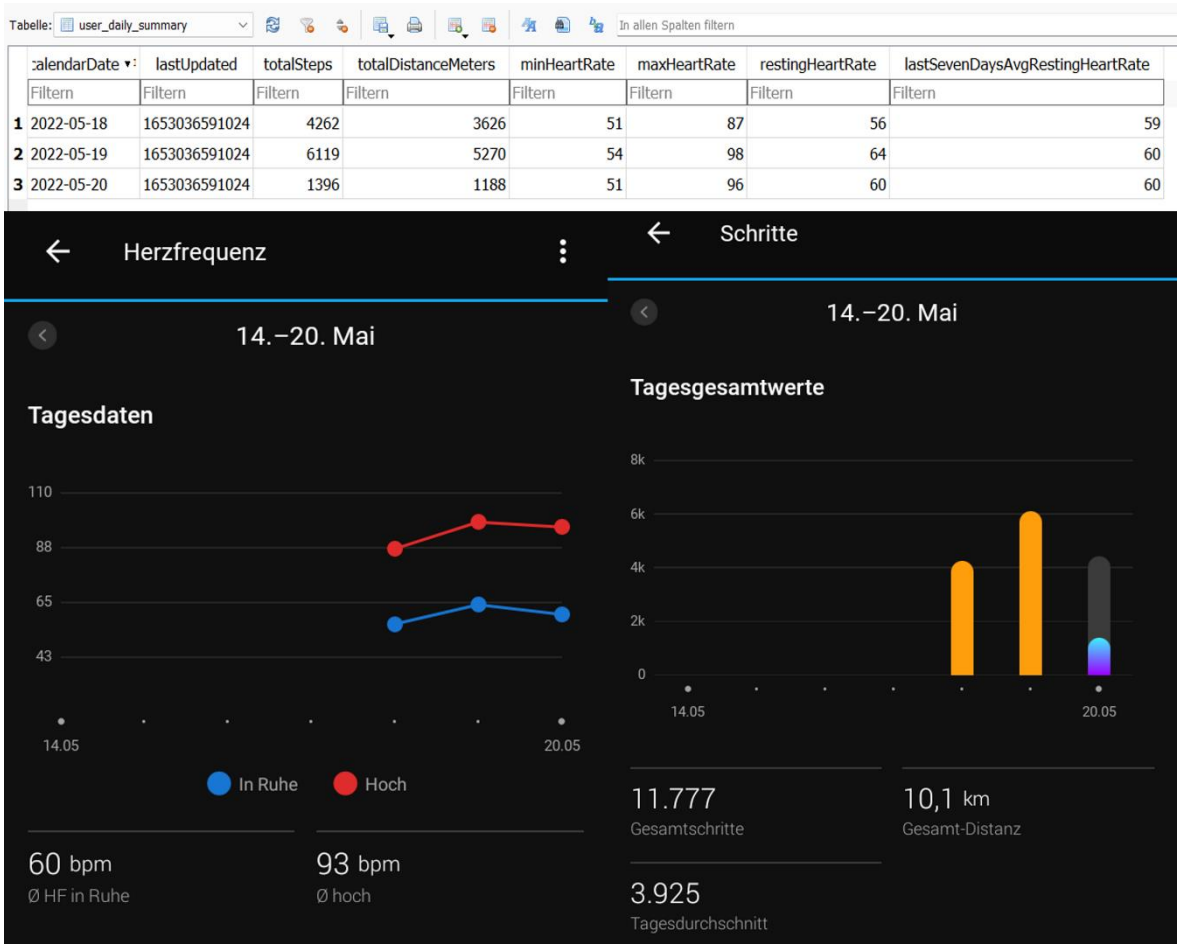


Abbildung 39: Ergebnisse - Zugang durch neue Nutzerdaten *Garmin Forerunner 55* (Zusammengeschnittene und bearbeitete Screenshots, Juli 2022)

Zusammengefasst können bei einem Zugang durch neue Nutzerdaten auf einem neuen Simulationsgerät ermittlungsrelevante Daten der *Garmin Forerunner 55* eingesehen werden, die seit dem Zeitpunkt der letzten Synchronisierung mit einem anderem Gerät erzeugt wurden. Sowohl die Tabelle als auch die Fitnessapplikation geben einen feingranularen und grafischen Einblick in die erzeugten Vitaldaten.

4.2.2.3 Fitbit Inspire 2

Als letztes Gerät wurde der Fitnesstracker *Fitbit Inspire 2* untersucht. Die Firmware-Version des Bandes sowie die Applikationsversion des Simulationsgerätes glichen hierbei zum Zeitpunkt der Untersuchung den Versionen aus dem Teilkapitel 4.2.1.3. Die Untersuchung startete am 13. Juni 2022 und wurde am 15. Juni 2022 durch eine Synchronisierung mit neuen Nutzerdaten auf dem neuen Simulationsgerät beendet.

Zu Beginn wurde die *fitbit*-Fitnessapplikation installiert. Nach der Installation erstellte man mittels der *Google*-Kontodaten einen neuen *fitbit*-Account, um sich im Folgenden mit neuen Nutzerdaten anzumelden.

Kurz nach der Anmeldung machte man bereits eine Reihe an neuen Erkenntnissen. Mit Blick auf die Fitnessapplikationsdaten waren auch hier bis zur Anmeldung leere Ordnerstrukturen zu verzeichnen. Nach der Anmeldung erschienen die Datenbanken, die wie erwartet, keine Informationen beinhalteten. Die Oberfläche der Fitnessapplikation zeigte bis auf den bisherigen Kalorienverbrauch, der auf Basis der im Account angegeben Gewichtswerte und der aktuellen Uhrzeit berechnet wurde, keine weitere ermittlungsrelevanten Daten. Wie im Teilkapitel 4.2.1.3 dargestellt, war der Fitnesstracker mit dem alten Account verknüpft, weswegen man auch hier versuchte, den *Fitbit Inspire 2* mit dem neu erstellten Account zu koppeln.

Im Gegensatz zum *Xiaomi Mi Smart Band 6* ließ sich dieser problemlos mit der App verknüpfen. Nach der Verknüpfung begann die Fitnessapplikation die Daten auf dem Fitnesstracker zu synchronisieren.

Die Ergebnisse der Synchronisierung sind in der Abbildung 40 dargestellt. Nach erfolgter Synchronisierung widmete man sich zunächst der „heart_rate_db“ und der zu untersuchenden Tabelle „HEART_RATE_SUMMARY“ (mittig). Entgegen der Erwartung aus den Voruntersuchungen war die Tabelle leer und beinhaltete keine Durchschnitts- und Ruheherzfrequenzdaten. Auch ein Blick in die Fitnessapplikation (rechts) zeigte, dass keine Herzfrequenzdaten synchronisiert wurden. Im Gegensatz zur Herzfrequenz wurden jedoch die Schrittdaten, die seit dem 13. Juni 2022 aufgezeichnet wurden, synchronisiert. Das bedeutet, dass sämtliche Schrittdaten seit Beginn der Untersuchung (13. Juni 2022) aufgezeichnet, gespeichert und in der Fitnessapplikation *fitbit* dargestellt sind (links), obwohl auch hier ein vollständig neu erzeugter Account verwendet wurde.

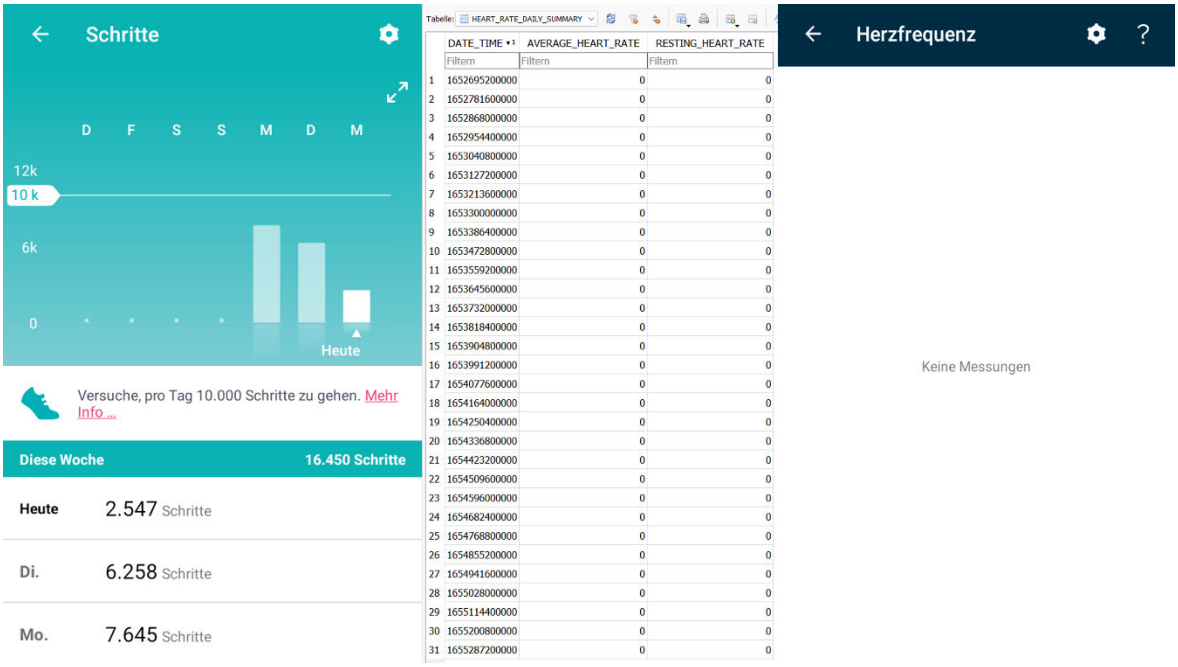


Abbildung 40: Ergebnisse - Zugang durch neue Nutzerdaten *Fitbit Inspire 2* (Zusammengeschnittene und bearbeitete Screenshots, Juli 2022)

Zusammengefasst können bei einem Zugang durch neue Nutzerdaten auf einem neuen Simulationsgerät ermittlungsrelevante Schrittdaten der *Fitbit Inspire 2* eingesehen werden, die seit dem Zeitpunkt der letzten Synchronisierung erzeugt wurden. Die Fitnessapplikation gab einen feingranularen und grafischen Einblick in die erzeugten Schrittdaten. Eine Untersuchung der Tabelle blieb ohne Erfolg.

4.3 Chip-Off-Analyse und Datenextraktion

Der Gegenstand dieses Teilkapitels ist die Darstellung der Ergebnisse aus der Datenextraktion (vgl. Teilkapitel 3.7.3) die auf Grundlage des zweiten Teils der Zielsetzung (vgl. Teilkapitel 1.2) durchgeführt wurde. Hierfür ist die extrahierte Binärdatei mittels mehrerer Tools bearbeitet und interpretiert wurden. Die Ergebnisse erwiesen sich mit Blick auf das Teilkapitel 3.6.2 als forensisch wertvoll.

Um sich einen Überblick über die extrahierte Binärdatei zu verschaffen, wurde diese mit dem Tool *VISUAL NAND RECONSTRUCTOR* zunächst visuell analysiert. Die Erkennung und Analyse von Binärmustern in Flash-Speicherchips ist hierbei der wichtigste Schritt bei der Extrahierung und Wiederherstellung von Chip-Off-Daten. Das Tool ermöglicht eine Analyse im Bitmap-Modus, da es die klassische Hex-Editor-Ansicht nicht erlaubt, binäre Muster zu verfolgen [72].

Die Abbildung 41 veranschaulicht die Binärdatei im *VISUAL NAND RECONSTRUCTOR.* Damit die Muster im Bitmap-Modus korrekt angezeigt werden, war es zunächst notwendig, die typischen Pagegrößen für Speicherchips auszutesten und einzustellen, bis eine Struktur wie in Abbildung 41 dargestellt, erkennbar war. Dabei griff man auf typische Pagegrößen für Speicherchips zurück und probierte diese im *VISUAL NAND RECONSTRUCTOR* durch. Beginnend mit einer Pagegröße von 2112 Bytes (2KB) stellte man bereits bei einer Größe von 4224 Bytes (4KB) eine Struktur fest und setzte die visuelle Untersuchung der Binärdatei fort [73].

Ein Blick in den dekodierten Text in der Abbildung 41 (rechts) zeigt, dass die Daten der ersten Bytes unverschlüsselt im Klartext vorliegen. Zusätzlich zum dekodierten Text sind durch eine Pagegröße von 4224 Byte verschiedenste Strukturen im grafischen Dump erkennbar. Unverschlüsselte Daten haben recht hohe Dichten und weisen im *VISUAL NAND RECONSTRUCTOR* horizontale Muster auf, die wie Streifen, Würfel etc. aussehen. Diese Datenbereiche sind im Tool grau (vgl. Abbildung 41) hervorgehoben. Verschlüsselte Daten hingegen weisen keine typischen Datenmuster auf, sondern sehen aus wie Rauschen (Entropie des weißen Rauschen) [72]. Durch das niedrige Rauschen an den jeweiligen Stellen mit horizontalen Mustern lässt sich bereits visuell darauf erkennen, dass diese Strukturen nicht verschlüsselt und somit der gesamte Flash-Speicherchip nicht voll verschlüsselt ist. Eine Vollverschlüsselung würde sich somit über ein großes weißes Rauschen über den

gesamten Binärcode zeigen. Da dies aber nicht der Fall ist, wird die Binärdatei an den jeweiligen Stellen mit Mustern, im Folgenden weiterer Untersuchungen unterzogen.

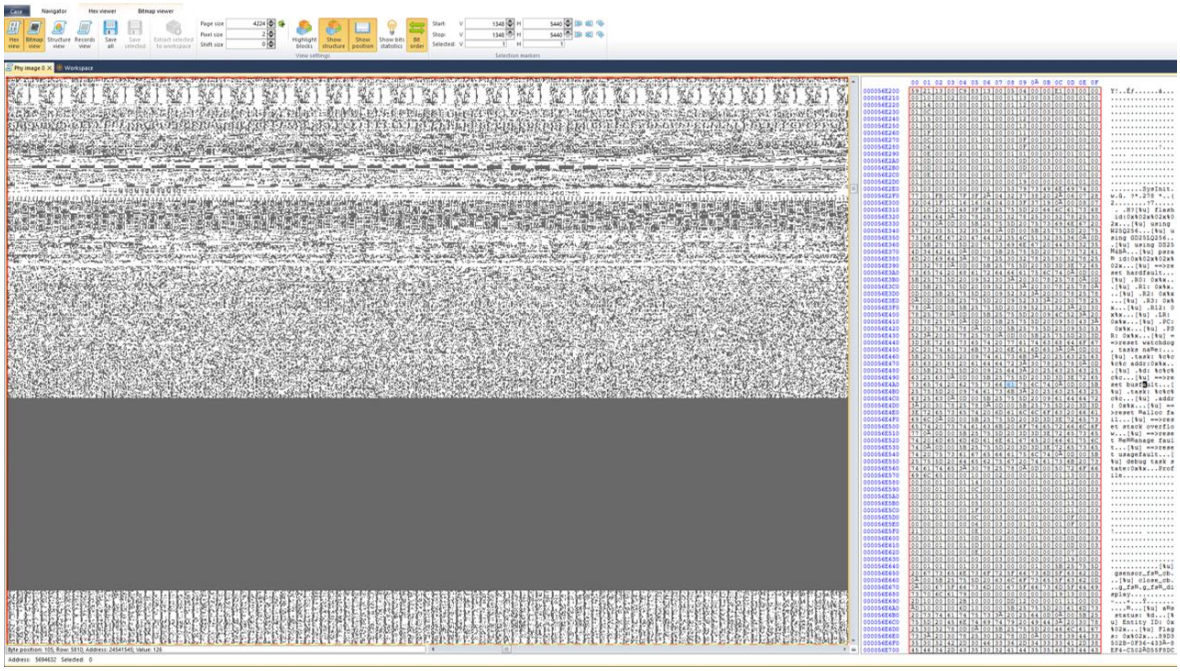


Abbildung 41: Visualisierung der extrahierten Binärdatei aus der Chip-Off-Analyse mittels *VISUAL NAND RECONSTRUCTOR* (Screenshot, Juli 2022)

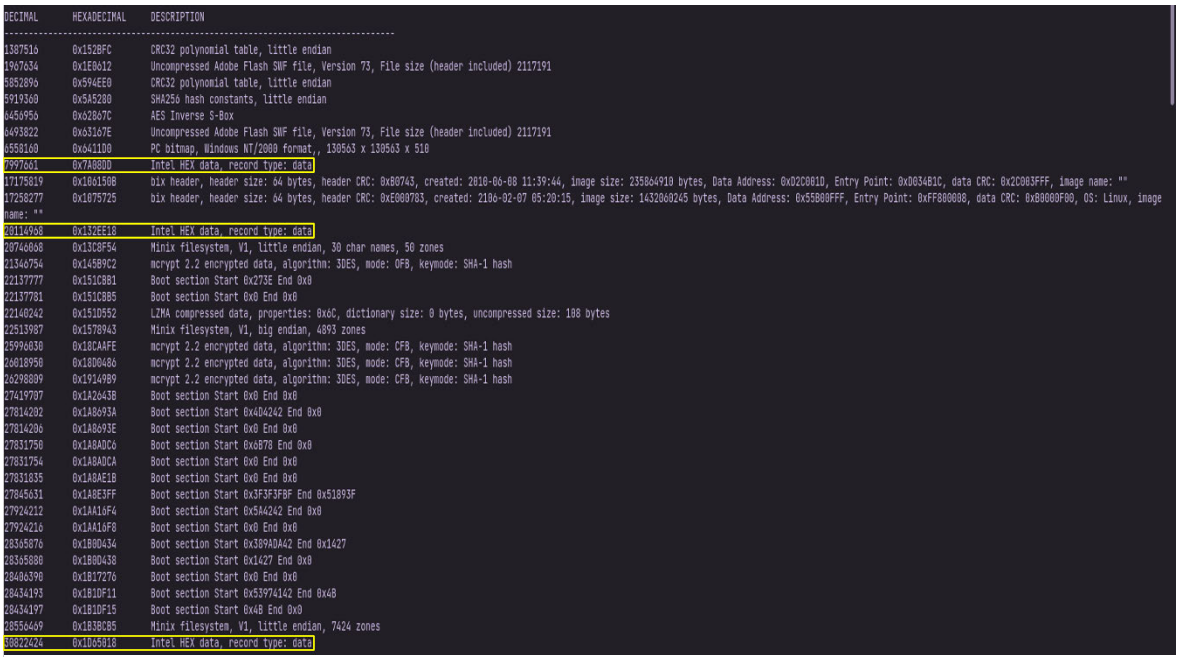
Aus den Ergebnissen der visuellen Vorbetrachtung ließ sich zunächst festhalten, dass es aus forensischer Sicht sinnvoll wäre, die Binärdatei, vor allem die unverschlüsselten Bereiche, weiter zu analysieren. Hilfreich bei der weiteren Untersuchung war das Tool *binwalk*. Das Tool wurde dabei unter Verwendung eines *Linux*-Betriebssystems über die Kommandozeile gestartet. Es bietet viele Analysemöglichkeiten von großen unüberschaubaren Binärdateien. Im Rahmen der Untersuchung verwendete man die Signatur- sowie Entropieanalysefunktionen des Tools. Um eine Signaturanalyse unter *binwalk* durchzuführen, muss der Befehl:

```
# binwalk -B „Binärdatei“
```

ausgeführt werden. Der Parameter „-B“ sorgt dafür, dass das Tool alle Offsets der Binärdatei auf bekannte Dateisignaturen prüft und das Ergebnis anschließend geordnet auf der Kommandozeile ausgibt.

Die Abbildung 42 veranschaulicht die Ergebnisse aus der Signaturanalyse. Neben einem *Minix filesystem*, vielen verschlüsselten Bereichen, Bootsektoren etc. detektierte die Signaturanalyse auch Bereiche in denen *Intel HEX*-Daten abgelegt sind. Da man im Rahmen der Untersuchung auf der Suche nach Daten war und diese auf den ersten Blick nicht verschlüsselt zu sein schienen, wurden die Offsets der Signaturen notiert, um einer weiteren Untersuchung später unterzogen zu werden. Dabei war es wichtig, sich sowohl die

dezimalen- als auch die hexadezimalen-Offsetpositionen zu notieren, um in beiden Zahlensystemen nachvollziehen zu können, wo die Bereiche der Signaturen lagen.



```
DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
1387516       0x152BFC        CRC32 polynomial table, little endian
1967634       0x1E0612        Uncompressed Adobe Flash SWF file, Version 73, File size (header included) 2117191
5852896       0x594EE0        CRC32 polynomial table, little endian
5919360       0x5A5280        SHA256 hash constants, little endian
6456956       0x62867C        AES Inverse S-Box
6493822       0x63167E        Uncompressed Adobe Flash SWF file, Version 73, File size (header included) 2117191
6558160       0x641100        PC bitmap, Windows NT/2000 format,, 130563 x 130563 x 510
7997601       0x7A0B0D        Intel HEX data, record type: data
17175819      0x106150B       bix header, header size: 64 bytes, header CRC: 0x80743, created: 2010-06-08 11:39:44, image size: 235864910 bytes, Data Address: 0xD2C001D, Entry Point: 0x0034B1C, data CRC: 0x2C083FFF, image name: ""
17258277      0x1075725       bix header, header size: 64 bytes, header CRC: 0xE080783, created: 2106-02-07 05:20:15, image size: 1432060245 bytes, Data Address: 0x55B80FFF, Entry Point: 0xFF880088, data CRC: 0x80069F00, OS: Linux, image
name: ""
20114968      0x132EE18       Intel HEX data, record type: data
20744068      0x13C0F54       Minix filesystem, V1, little endian, 30 char names, 50 zones
21346754      0x145B9C2       mcrypt 2.2 encrypted data, algorithm: 3DES, mode: OFB, keymode: SHA-1 hash
22137777      0x151CBB1       Boot section Start 0x273E End 0x0
22137781      0x151CBB5       Boot section Start 0x0 End 0x0
22140242      0x151D552       LZMA compressed data, properties: 0x6C, dictionary size: 0 bytes, uncompressed size: 108 bytes
22513987      0x1578943       Minix filesystem, V1, big endian, 4893 zones
25996630      0x18CAAFE       mcrypt 2.2 encrypted data, algorithm: 3DES, mode: CFB, keymode: SHA-1 hash
26018950      0x18D0486       mcrypt 2.2 encrypted data, algorithm: 3DES, mode: CFB, keymode: SHA-1 hash
26298809      0x1914B9        mcrypt 2.2 encrypted data, algorithm: 3DES, mode: CFB, keymode: SHA-1 hash
27419707      0x1A2643B       Boot section Start 0x0 End 0x0
27814202      0x1A8693A       Boot section Start 0x4D4242 End 0x0
27814206      0x1A8693E       Boot section Start 0x0 End 0x0
27831750      0x1A8ADC6       Boot section Start 0x6B78 End 0x0
27831754      0x1A8ADCA       Boot section Start 0x0 End 0x0
27831835      0x1A8AE1B       Boot section Start 0x0 End 0x0
27845631      0x1A8E3FF       Boot section Start 0x3F3F3FBF End 0x51893F
27924212      0x1AA16F4       Boot section Start 0x544242 End 0x0
27924216      0x1AA16F8       Boot section Start 0x0 End 0x0
28365876      0x1B0D434       Boot section Start 0x389ADA42 End 0x1427
28365880      0x1B0D438       Boot section Start 0x1427 End 0x0
28486390      0x1B17276       Boot section Start 0x0 End 0x0
28434193      0x1B1DF11       Boot section Start 0x53974142 End 0x4B
28434197      0x1B1DF15       Boot section Start 0x4B End 0x0
28556469      0x1B3BCB5       Minix filesystem, V1, little endian, 7424 zones
30822424      0x1D65018       Intel HEX data, record type: data
```

Abbildung 42: Ergebnisse aus der Signatursuche mittels *binwalk* (Screenshot, Juli 2022)

Neben einer Signaturanalyse wurde mittels *binwalk* ebenso eine Entropieanalyse durchgeführt, um zum einen die visuell festgestellten Auffälligkeiten zu verifizieren und zum anderen Bereiche aus der Signaturanalyse mit einer Entropie zu verknüpfen. Um eine Entropieanalyse unter *binwalk* durchzuführen, muss der Befehl:

```
# binwalk -E „Binärdatei“
```

ausgeführt werden. Der Parameter „-E“ sorgt dafür, dass das Tool für die gesamte Binärdatei an allen Offsets eine Entropie kalkuliert und anschließend grafisch übersichtlich als Liniendiagramm darstellt.

Die Abbildung 43 zeigt das Liniendiagramm. Deutlich zu sehen sind die Bereiche mit einer hohen Entropie, die anhand der Y-Achse abgemessen werden. Umso näher ein Offset (X-Achse) der 1,0 auf der Y-Achse kommt, umso höher ist die Entropie. Dies bedeutet, dass diese Bereiche ein hohes Rauschen aufweisen, höchstwahrscheinlich verschlüsselt sind und von einer weiteren Betrachtung ausgeschlossen werden. Es sind jedoch auch Bereiche zu erkennen, in denen die Entropie über eine große Offsetlänge konstant null ist. Hier erhoffte man sich, unverschlüsselte Rohdaten zu finden. Die Offsets sind hierbei in der Dezimalschreibweise dargestellt und wurden zur Übersichtlichkeit an den jeweiligen Startbereichen mit niedriger Entropie ausgerechnet: $0{,}25 * 10^7 = \mathbf{2500000}$; $0{,}75 * 10^7 = \mathbf{7500000}$; $0{,}8 * 10^7 = \mathbf{8000000}$; $1{,}95 * 10^7 = \mathbf{19500000}$; $2{,}95 * 10^7 = \mathbf{29500000}$; $3{,}3 * 10^7 = \mathbf{33000000}$. Betrachtet man die dezimalen Offsetbereiche, an denen die Entropie 0 ist, so fällt auf, dass die durch die Signaturanalyse markierten *Intel HEX*-Bereiche (vgl. Abbildung 42) zu drei im Liniendiagramm abgebildeten Offsetbereichen passen. Dies bestätigte, dass

die *Intel HEX*-Daten eine niedrige Entropie sowie ein niedriges Rauschen aufweisen und folglich nicht verschlüsselt sind.

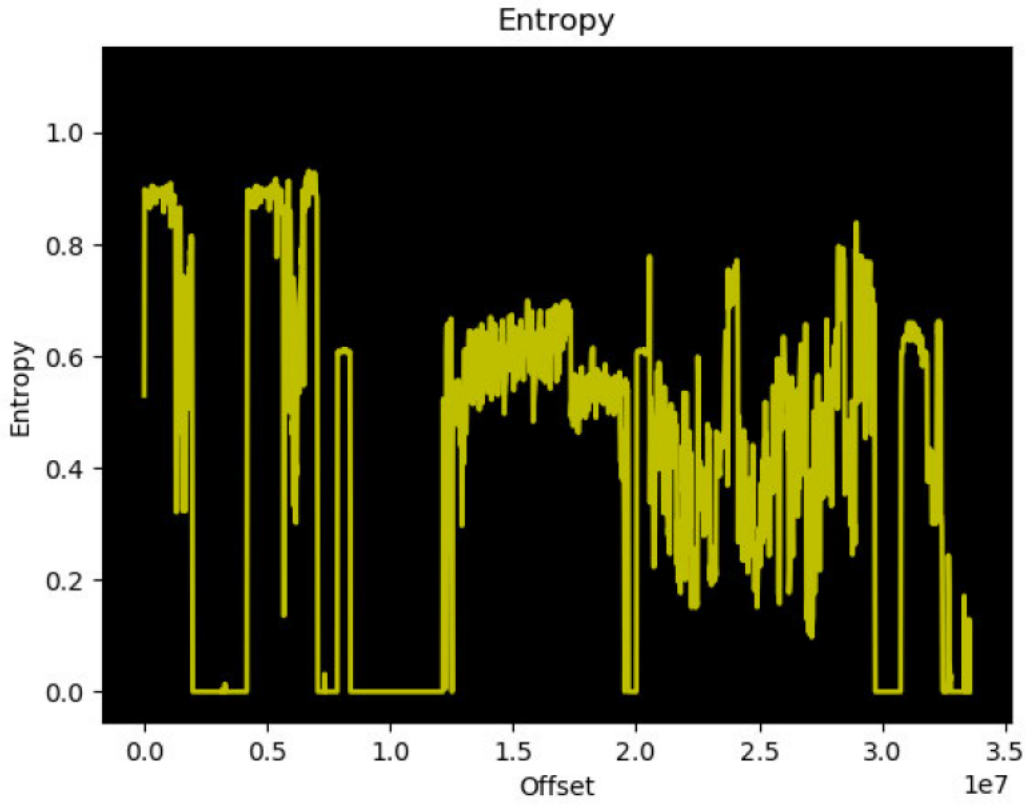


Abbildung 43: Liniendiagramm - Entropie der extrahierten Binärdatei aus der Chip-Off-Analyse (Eigene Darstellung erzeugt mittels *binwalk*, Juli 2022)

Durch die Ergebnisse, die man mittels der beiden vorgestellten Tools erzielte, sah man von einer Betrachtung weiterer Signaturbereiche ab und fokussierte sich auf die *Intel HEX*-Daten mit dem Ziel, ermittlungsrelevante Daten extrahieren zu können.

Mit dem Wissen über die Signaturbereiche nahm man sich den Hex-Editor *HxD* zur Hilfe, um die jeweiligen Bereiche zu extrahieren. Im Hex-Editor fügte man die Binärdatei ein, sprang zu den Signaturoffsets, suchte sich die Start- und Endoffset heraus und extrahierte die jeweiligen *Intel HEX*-Datenblöcke in eine Textdatei. Die drei Bereiche fügte man anschließend zusammen, wodurch eine rund zwei Megabyte große und 51261 Zeilen lange Textdatei entstand. Man grenzte somit die rund 32 Megabyte große Binärdatei auf eine rund zwei Megabyte große Textdatei ein. Die genauere Untersuchung der *Intel-HEX*-Daten erbrachte viele Ergebnisse, auf die im Folgenden nun genauer eingegangen wird.

Beim Betrachten der extrahierten Daten zeigte sich, dass es sich um Rohdaten des Fitnesstrackers handelte, die unverschlüsselt, zeilenweise in den jeweiligen Bereichen auf dem Flash-Speicherchip abgelegt wurden. Zudem erkannte man eine Struktur in den Rohdaten, die unter anderen durch das Wort *time* (dt. = Zeit) mit einem dazugehörigen Zeitstempel versehen war. Mit dem Zeitstempel verfolgte man die Rohdatenstrukturen bis zum

6. Juni 2022 um 17:57:58 Uhr zurück. Ab diesem Datum beginnen die Strukturen und werden von dort an minütlich neu erzeugt.

Die Abbildung 44 gibt einen Einblick in die Rohdatenstruktur vom 7. Juni 2022 von 08:05:58 Uhr bis 08:06:58 Uhr. Die Einträge beginnen dabei immer mit einem „ALG_SPT“ und enden mit einem „[HP]“-Eintrag. Die Bedeutung dieser Einträge konnte nicht ermittelt werden. Neben dem „[TIME]“-Eintrag gab der „[BAT]“-Eintrag ebenfalls den Zeitstempel an und ist in der Abbildung 44 dahingehend mit einem gelben Rechteck umrandet. Des Weiteren fielen Einträge mit dem Namen „wear_n“ und „wear“ auf, denen eine 0 zugeordnet wurde.

Abbildung 44: Rohdatenstruktur - *Intel HEX*-Daten (Zusammengeschnittene und bearbeitete Screenshots, Juli 2022)

Das Schlagwort *wear* (dt. = tragen) brachte die Untersuchungsidee hervor, den Zeitpunkt herauszufinden, ab wann der Fitnesstracker am 07. Juni 2022 im Rahmen der Untersuchung getragen wurde, um vor der Chip-Off-Analyse Daten zu erzeugen. Externe Aufzeichnungen belegten, dass der Fitnesstracker am 07. Juni 2022 um 08:07 Uhr angelegt wurde. Beim Untersuchen der Rohdatenstruktur um 08:07 Uhr bestätigte sich die Untersuchungsidee und man gewann weitere Erkenntnisse.

Die Abbildung 45 veranschaulicht die Rohdatenstruktur vom 07. Juni 2022 um 08:07:58 Uhr. Als erste Auffälligkeit lässt sich festhalten, dass diese Rohdatenstruktur wesentlich komplexer und länger ausfiel, als die Strukturen bis zum 06. Juni 2022 um 17:57:58 Uhr rückwärts betrachtet. Analysiert man nun erneut die Einträge „wear_n“ und „wear“, so zeigt sich, dass diesen nun eine 1 zugeordnet wurde. Das bedeutet, wenn der Fitnesstracker abgelegt ist, der Eintrag auf 0 und wenn er angelegt ist, auf 1 gesetzt wird. Anhand dieses Eintrages ist es also möglich abzulesen, wann der Fitnesstracker getragen wurde und wann nicht. Über dem bekannten „[TIME]“ und „[BAT]“-Eintrag ist zudem ein neuer „[hr ver]“-Eintrag hinzugekommen. Betrachtet man die Abkürzungen, so ist es naheliegend, dass diese

für die Herzrate und Version stehen könnten, da im Eintrag „v.3.9.4“ steht, was üblicherweise eine Schreibweise für Versionsnummern darstellt.

Als deutlichste Änderung im Gegensatz zur Rohdatenstruktur vor 08:07:58 Uhr sind jedoch die Einträge unterhalb von „[BAT]“ und „[hr ver]“ hervorzuheben, aus welchen sich eine vierte Hypothese formulieren lässt:

- **H4**: Es handelt sich bei den gefundenen Werten um Herzfrequenzdaten.

Der erste Eintrag unterhalb von „[hr ver]“ nennt sich „[PPG]“. Die Abkürzung PPG, bekannt aus Teilkapitel 2.2.2, steht für Photoplethysmographie und ist die Bezeichnung für das Verfahren ist, mit welchem der optische Sensor die Herzfrequenz ermittelt. Dies ist ein erstes Argument zur **Verifizierung** von **H4**.

Die 13 folgenden Einträge mit dem Namen „hr“ sind ein weiteres Indiz dafür, dass es sich um Einträge in Bezug auf die Herzrate handeln muss und **H4** somit **verifiziert** werden kann. In 12 Zeilen liegen dabei „invalid hr“-Werte vor, was darauf schließen lässt, dass dies ungültig gemessene Herzraten sind, ausgehend vom englischen Wort *invalid* (dt. = ungültig). Eine von 13 Zeilen enthält einen gültigen Eintrag, erkennbar an „hr:71“, also eine realistische Herzfrequenz von 71 Schlägen pro Minute.

Als letzte Auffälligkeit ist der „[hr_avg]“-Eintrag unter dem „[HP]“-Eintrag hervorzuheben. Wird der Fitnesstracker getragen, so endet die Rohdatenstruktur mit einem „[hr_avg]“ statt mit einem „[HP]“-Eintrag. Der Name „hr_avg“ könnte hierbei für die englischen Wörter *heartrate average* (dt. = Durchschnittsherzrate) stehen, was die im Rahmen der Untersuchung gesuchte Herzfrequenz wäre. Der zugewiesene Wert (71) lässt darauf schließen, dass der Durchschnitt aus dem einzig gültig gemessenen Wert berechnet wurde. Zur Verifizierung stellte man bei Probesichtungen zwischen 08:07:58 und 11:03:58 Uhr fest, dass die als gültig gemessenen Werte immer im Durchschnitt den jeweiligen „hr_avg“-Wert ergaben. Diese beiden Argumente stehen ebenfalls für eine **Verifizierung** von **H4**.

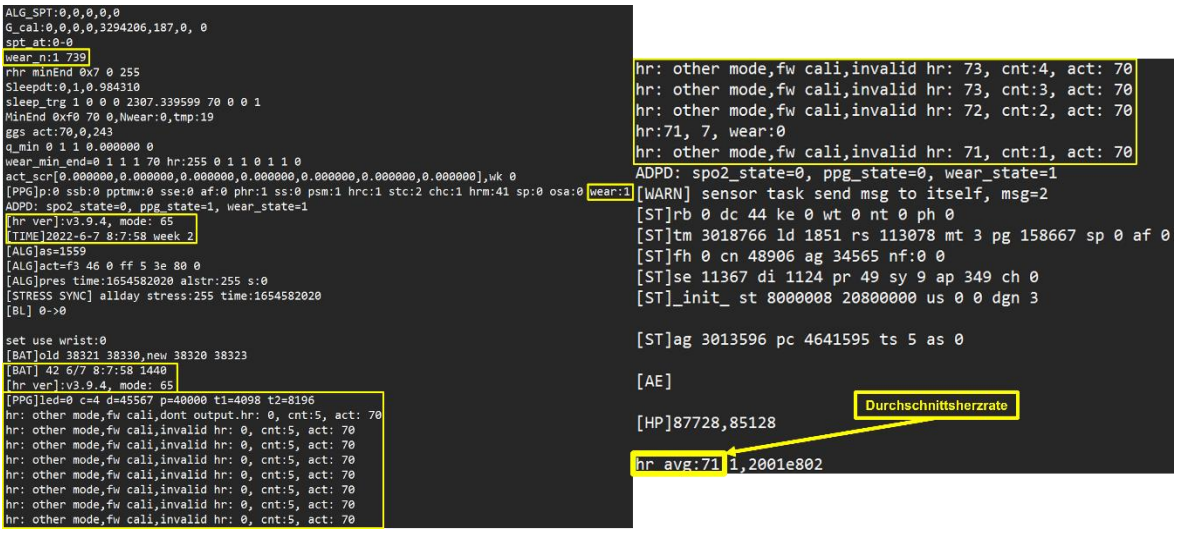


Abbildung 45: Rohdatenstruktur bei angelegtem Fitnesstracker - *Intel HEX*-Daten (Zusammengeschnittene und bearbeitete Screenshots, Juli 2022)

Mit der naheliegen Verifizierung wurde als zusätzlicher Schritt eine Volltextsuche über die *Intel-HEX*-Daten ab dem 7. Juni 2022 08:07:58 Uhr mit dem Stichwort „hr_avg“ durchgeführt. Die Volltextsuche ergab insgesamt 176 Treffer, die alle jeweils das Stichwort in Verbindung mit der dahinter liegenden Herzrate beinhalteten. Da die Rohdatenstruktur jede Minute erzeugt wurde, ist es naheliegend, dass insgesamt 176 Minuten lang Herzfrequenzen aufgezeichnet wurden. Addiert man 08:07:58 Uhr um 176 Minuten auf, so erhält man die Uhrzeit 11:03:58 Uhr. Tatsächlich stellte sich sowohl anhand von externen Aufzeichnungen als auch mit Blick auf die Rohdaten heraus, dass die letzte Herzrate um 11:03:58 Uhr gemessen wurde, da der Fitnesstracker zur Chip-Off-Analyse abgenommen wurde und von fort an keine Herzfrequenz detektieren werden konnte. Dieses Argument steht deutlich für eine weitere **Verifizierung** von **H4**.

Zusammenfassend kann die Hypothese **H4** durch die genannten Argumente **verifiziert** werden.

Am 7. Juni 2022 zwischen 11:03:58 und 11:36:58 Uhr sowie 08:07:58 und 11:03:58 Uhr wurden weitere interessante Daten detektiert. Die Abbildung 46 veranschaulicht diese zum Teil.

Man stellte zunächst fest, dass die Rohdatenstruktur, gemessen an den Zeitstempeln, am 07. Juni 2022 um 11:36:58 Uhr endete. Diese Uhrzeit gibt den Zeitpunkt der Chip-Off-Analyse an, an dem der Akkumulator vom Mainboard abgelötet wurde (vgl. Teilkapitel 3.5.2.1) und keinen Strom mehr für dieses lieferte.

Neben dem Zeitpunkt des Ablötens vom Akkumulator um 11:36:58 Uhr konnte in den Rohdaten ebenfalls der Zeitpunkt der Mainboard-Extraktion aus dem Fitnesstracker-Gehäuse und den dazugehörigen Verkabelungen (vgl. Teilkapitel 3.5.2.1) abgelesen werden. Der erste Ausschnitt (markiert mit einer 1) veranschaulicht die um 11:26:58 Uhr in Zeilen geschriebenen Fehlermeldungen, die aufgrund der Mainboard-Extraktion und der damit verbundenen Trennung einiger Komponenten einhergeht. Die Fehlermeldungen häufen sich bis zur letzten Meldung um 11:36:58 Uhr.

Ferner stellte man im Zeitraum zwischen 11:03:58 Uhr und 11:36:58 Uhr mögliche Platzhalter für Wetterdaten (markiert mit einer 3) fest. Es zeigten sich Einträge für Temperatur, Wetter, Feuchtigkeit, Wind, UV-Index und nicht klar definierte Einträge in der „[TH]“ Zeile, die von ihrer Struktur her, wie Koordinaten aussehen. Eine genaue Bedeutung der Werte kann aufgrund der fehlenden Eintragungen sowie Vergleichsaufzeichnungen nicht gegeben werden.

In der Zeit von 08:07:58 bis 11:03:58 Uhr zeigten sich zwei weitere interessante Ergebnisse. An vereinzelnden Stellen war es möglich, mittels der Rohdaten nachzuvollziehen, wann der Fitnesstracker mit der Fitnessapplikation kommunizierte. Ein Beispiel ist in der Abbildung 46 mit einer 2 markiert. Zu sehen ist ein sogenannter Diffie-Hellman-Schlüsselaustausch, abgekürzt ECDH (Elliptic-curve Diffie-Hellman). Der ECDH ermöglicht es zwei

Kommunikationspartnern einen gemeinsamen geheimen Schlüssel in Form einer Zahl, über eine unsichere Leitung, zu vereinbaren [74]. Im Beispiel wurde somit über die einsehbaren (unsicheren) *Intel-HEX*-Daten im Flash-Speicherchip ein geheimer Schlüssel für einen unbekannten Zweck vereinbart.

Neben undefinierten Hex-Daten, die empfangen und gesendet wurden, stellte man zusätzlich AES-Schlüssel in den Rohdaten fest. In der Abbildung 46 mit einer 4 markiert, wird ein solcher AES-Schlüssel (gelb umrissen) dargestellt. Abgebildet ist ein 128 Bit (16 Byte) Schlüssel dessen Verwendung nicht definiert werden kann. Es bestätigt jedoch die Erkenntnis aus dem Teilkapitel 3.6.2 das zumindest Teile der Kommunikation, Daten etc. AES verschlüsselt sein müssen.

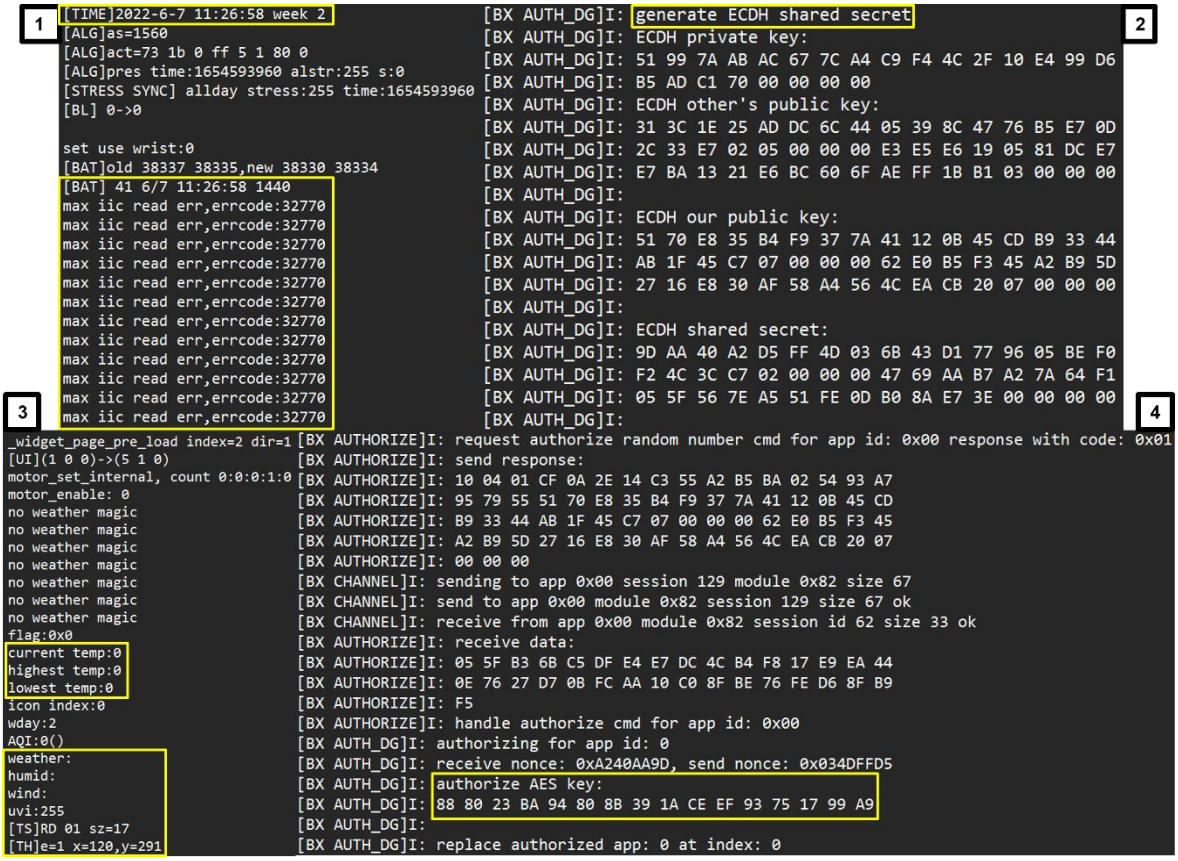


Abbildung 46: Weitere Ergebnisse aus den *Intel HEX*-Daten (Zusammengeschnittene und bearbeitete Screenshots, Juli 2022)

Zusammengefasst können durch eine Chip-Off-Analyse und anschließende Datenextraktion des Flash-Speicherchips *W25Q256JWPIM* aus dem *Xiaomi Mi Smart Band 6* ermittlungsrelevante Herzfrequenzdaten extrahiert werden. Wie lange diese gespeichert sind, ist unbekannt. Die zweiten als ermittlungsrelevant definierten Schrittdaten konnten nicht lokalisiert und extrahiert werden.

5 Diskussion

Das Ziel dieser Bachelorarbeit bestand darin, zu untersuchen, ob und wenn ja, unter welcher Konstellation die auf Fitnesstrackern/Fitness-Smartwatches abgelegten Daten forensisch gesichert werden können, wenn keine Zugriffsmöglichkeit zum ursprünglich gekoppelten Smartphone besteht. Durch den aktuellen Bezug (vgl. Kapitel 1) beschränkte man sich auf Herzfrequenz- und Schrittdaten, die die Fitnesstrackern/Fitness-Smartwatches aufzeichnen und entsprechend ablegen. Die während der Untersuchungen entstandenen Ergebnisse sind teils vielseitig, waren überraschend, aber vor allem forensisch interessant.

5.1 Xiaomi Mi Smart Band 6

Als erster Fitnesstracker wurde das *Xiaomi Mi Smart Band 6* untersucht und mit dem *Fitbit Inspire 2* einer Chip-Off-Analyse unterzogen, die in ihrer anspruchsvollen Durchführungsweise forensisch relevante Ergebnisse erzielte. Im Folgenden sollen die einzelnen Ergebnisse diskutiert werden.

In Bezug auf die erste Untersuchung, der Analyse des Synchronisations- und Speicherverhalten, lässt sich festhalten, dass das *Xiaomi Mi Smart Band 6* bis zu sieben Tage die definierten ermittlungsrelevanten Daten aufzeichnen, speichern und synchronisieren kann. Durch die dabei aufgebaute Verbindungsumgebung stellte man fest, dass die Synchronisierung sowohl in der Tabelle als auch in der Fitnessapplikation feingranular durchgeführt wird.

Aus forensischer Sicht sind diese Ergebnisse von großem Interesse. Bei Ermittlungen, in denen der untersuchte Fitnesstracker involviert ist, kann nun sichergestellt werden, dass dieser mindestens die Herzfrequenz- und Schrittdaten der letzten sieben Tage gespeichert hat, wenn dieser seitdem nicht synchronisiert wurde. Insbesondere sollte aber der Umstand beachtet werden, dass der Fitnesstracker in diesem Zeitraum seit letzter Synchronisierung (sieben Tage) gesichert werden sollte, da das Synchronisations- und Speicherverhalten darüber hinaus nicht untersucht wurde.

Die zweite Untersuchung (Zugangsmöglichkeiten für einen IT-Forensiker) hat gezeigt, dass aus forensischer Sicht nur begrenzte Möglichkeiten bestehen, über diesen Weg ermittlungsrelevante Daten zu sichern. Als oberste Maxime zeigte bereits die Forschungsarbeit von Jacoby [6], dass es für jeden Forensiker unabdingbar ist, einen Root-Zugang zum Mobilgerät aufzubauen. Die vorliegende Bachelorarbeit hat in ihrem Versuchsaufbau und den Untersuchungen gezeigt, dass sich die Einrichtung eines *Raspberry Pi 4 Model B* als *Android*-Gerät und der anschließenden Dateiübertragung über SFTP als nützlich und forensisch wertvoll herausstellen, da über diesen Weg der Ermittler stets mit Root-Rechten auf das

Endgerät zugreifen kann. Mit den notwendigen Root-Rechten konnten die Zugangsmöglichkeiten eines Forensikers in Bezug auf den Fitnesstracker und der dazugehörigen Fitnessapplikation *Zepp Life* untersucht werden. Verwendete man das gleiche Benutzerkonto wie für die Untersuchung des Synchronisations- und Speicherverhaltens, so ergaben sich hier einige forensisch wertvolle Erkenntnisse. Es ist einem Forensiker möglich, sofern er die ursprünglichen Accountdaten besitzt, den Fitnesstracker mit jedem anderen beliebigen *Android*-Gerät, auf welchem die Applikation installiert ist, zu koppeln. Bei der Untersuchung stellte man zudem fest, dass nicht nur die Daten seit der letzten Synchronisierung (im Rahmen der Untersuchung über zwei Tage) übertragen wurden, sondern auch alle mit dem Fitnesstracker erzeugten Daten seit der ersten Nutzung.

Dieses Wissen ist für einen IT-Forensiker von großem Interesse, da mit bekannten Nutzerdaten ermittlungsrelevante Daten bis zu ihrem Ursprung zurück ermittelt werden können. Dabei muss jedoch der Umstand beachtet werden, dass nur die Fitnessapplikation eine feingranulare Verfolgung der Schrittdaten erlaubt. In der Tabelle „DATE_DATA“ wurden diese hingegen nur seit der letzten Synchronisierung ergänzt. Aus forensischer Sicht ist es trotzdem empfehlenswert, auf die feingranularen, grafisch aufgearbeiteten ermittlungsrelevanten Daten zurückzugreifen, die mittels des *Python*-Skript (vgl. Anhang Teil 3) aus den Daten der Tabelle erzeugt werden. Benötigt man die Schrittdaten, die vor der letzten Synchronisierung erzeugt wurden, so kann man auf die Fitnessapplikation zurückgreifen.

Ferner ist zu erwähnen, dass das *Xiaomi Mi Smart Band 6* mit dem gekoppelten Account fest verknüpft ist. Die Untersuchung hat gezeigt, dass die Sicherungsmöglichkeiten, die bei bekannten Nutzerdaten bestehen, keine Anwendung finden, wenn man die Zugangsdaten nicht zur Verfügung hat. Durch den Zugang mittels neuer Nutzerdaten wurde bestätigt, dass der Fitnesstracker Accountgebunden eingerichtet wurde. Das *Xiaomi Mi Smart Band 6* kann somit mit beliebig neuen *Android*-Geräten verknüpft werden, wenn man die bekannten Nutzerdaten besitzt. Sobald neue Nutzerdaten erzeugt werden müssen, ist es nicht mehr möglich den Fitnesstracker mit einem neuem Account sowie *Android*-Gerät zu verknüpfen. Für einen IT-Forensiker ist diese Erkenntnis wichtig, da man über den Zugangsweg nur mit bekannten Nutzerdaten des ursprünglich verwendeten Fitnessapplikationskonto ermittlungsrelevante Daten sichern kann.

Die Möglichkeiten der forensischen Datensicherung sind nach dieser Erkenntnis jedoch nicht aufgebraucht. Durch eine Chip-Off-Analyse, als Alternative ohne bekannte Nutzerdaten, erlangte man viele forensisch gewinnbringende Ergebnisse.

Zunächst muss festgehalten werden, dass diese Datensicherungsalternative beim untersuchten Fitnesstracker nicht zerstörungsfrei durchgeführt werden kann. An dieser Stelle sei auf die Anlage Teil 1 verwiesen, die aufzeigt, welche Komponenten des *Xiaomi Mi Smart Band 6* ausgebaut werden müssen, ehe man ein Chip-Off durchführen sollte. Aus forensischer Sicht muss zudem der Umstand beachtet werden, dass eine Chip-Off-Analyse einer der anspruchsvollsten Datensicherungstechniken ist und bis zum Schritt der Extraktion der ermittlungsrelevanten Daten eine Menge an Fehlern gemacht werden können. Diese

zerstören im schlimmsten Fall nicht nur den Fitnesstracker, sondern auch die Chips und die darauf liegenden Daten.

Die im Rahmen des Bachelorprojektes durchgeführte Chip-Off-Analyse zeigte, dass ein Chip-Off des im *Xiaomi Mi Smart Band 6* befindlichen Flash-Speicherchips möglich ist. Entgegen den Erwartungen, die man durch die Auswertung der Datenblätter des dazugehörigen SoC hatte (vgl. Teilkapitel 3.6.1), stellte man durch die Mithilfe vieler forensisch wertvoller Tools fest, dass der Flash-Speicherchip nicht vollverschlüsselt wurde. Mit dieser Erkenntnis untersuchte man dann die extrahierte Binärdatei. Dabei stellten sich die Bereiche der *Intel HEX*-Daten als forensisch wertvoll heraus. Neben einer Rohdatenstruktur und den jeweiligen Zeitstempeln fanden sich auch Namen-Wertepaare die als die gesuchten ermittlungsrelevanten Herzfrequenzdaten zu interpretieren sind. Stichwörter wie „PPG“, „hr“ und „hr_avg“ sowie weitere Argumente (vgl. Teilkapitel 3.7.2.1) führten zum Entschluss, dass es sich um die Rohdaten der Herzfrequenz handelt.

Aus forensischer Sicht kann zusammenfassend festgehalten werden, dass es ohne Zugangsdaten zum ursprünglichen Fitnessapplikationskonto durch eine Chip-Off-Analyse möglich ist, Rohdaten der Herzfrequenz zu extrahieren. Mögliche ermittlungsrelevante Schrittdaten konnten nicht ermittelt werden.

5.2 Garmin Forerunner 55

Als zweites Gerät wurde die Fitness-Smartwatch *Garmin Forerunner 55* untersucht. Diese wurde als einzige keiner Chip-Off-Analyse unterzogen. Im Folgenden sollen die erzielten Ergebnisse aus den beiden Untersuchungen diskutiert werden.

In Bezug auf die erste Untersuchung, dem Synchronisations- und Speicherverhalten, kann zusammenfassend festgehalten werden, dass die *Garmin Forerunner 55* bis zu sieben Tage die definierten ermittlungsrelevanten Daten aufzeichnen, speichern und synchronisieren kann. Durch die dabei aufgebaute Verbindungsumgebung fand man heraus, dass die Fitness-Smartwatch die Synchronisierung sowohl in der Datenbank als auch in der Fitnessapplikation feingranular durchführt.

Aus forensischer Sicht können diese Ergebnisse von großer Relevanz sein. Bei Ermittlungen, in denen die untersuchte Fitness-Smartwatch involviert ist, kann nun sichergestellt werden, dass diese mindestens die Herzfrequenz- und Schrittdaten der letzten sieben Tage gespeichert hat, wenn diese seitdem nicht synchronisiert wurde. Insbesondere muss man hier den Umstand beachten, dass die Fitness-Smartwatch binnen der sieben Tage seit letzter Synchronisierung gesichert werden sollte, da das Synchronisations- und Speicherverhalten darüber hinaus nicht untersucht wurde.

Die zweite Untersuchung (Zugangsmöglichkeiten für einen IT-Forensiker) brachte die Erkenntnis, dass es aus forensischer Sicht sinnvoll ist, bei der *Garmin Forerunner 55* das im Rahmen der Untersuchung angewandte Verfahren zu verwenden, um ermittlungsrelevante

Daten zu extrahieren. Auch hier ist es für jeden ermittelnden Forensiker unabdingbar sicherzustellen, mit Root-Rechten auf die Endgeräte zuzugreifen, um die Zugangsmöglichkeiten zu untersuchen. Aus forensischer Sicht ergaben sich bei der Untersuchung mit bekannten Zugangsdaten Erkenntnisse, die sich von denen aus der Untersuchung des *Xiaomi Mi Smart Band 6* unterschieden. So konnten nach einer Anmeldung mit bekannten Nutzerdaten zunächst keine Datenbaken eingesehen werden. Die Fitnessapplikation hingegen stellte alle ermittlungsrelevanten Vitaldaten seit der letzten Synchronisierung feingranular und grafisch dar. Ein weiterer Unterschied ist, dass die Fitness-Smartwatch im Gegensatz zum *Xiaomi* Fitnesstracker nicht an den Account der Fitnessapplikation gebunden war. Diese Information ist für den ermittelnden Forensiker wichtig, da mit einer einfachen Anmeldung mit bekannten Nutzerdaten nur die Daten seit der letzten Synchronisierung eingesehen werden können. Wird die Fitness-Smartwatch jedoch anschließend gekoppelt, so ergänzen sich nicht nur in der Fitnessapplikation die jeweils fehlenden Tage seit der Synchronisierung (In der Untersuchung 2 Tage), auch die „cache-database“ wird erzeugt und enthält in der untersuchten Tabelle „user_daily_summary“ die Vitaldaten der letzten sieben Tage.

Das heißt, dass die Fitness-Smartwatch ohne Zugriffsmöglichkeit auf das ursprünglich gekoppelte Smartphone, wie es die Untersuchung vorgab, sieben Tage intern die ermittlungsrelevanten speichert, um sie nach einer Kopplung in die Tabelle zu schreiben. Aus welchem Grund die Fitness-Smartwatch die letzten sieben Tage speichert und in die Tabelle schreibt, wurde nicht untersucht. Forensisch relevant ist daher die Zeitangabe der letzten sieben Tage, in der sichergestellt werden kann, dass man die ermittlungsrelevanten Daten erhält. Es ist daher nicht möglich über die Tabelle im Falle einer Synchronisierung Daten einzusehen die älter als sieben Tage sind. In diesem Falle muss der IT-Forensiker auf die Daten in der Fitnessapplikation zurückreifen.

Im Gegensatz zum *Xiaomi Mi Smart Band 6* ergaben sich bei der *Garmin Forerunner 55* auch in Bezug auf die Zugangsmöglichkeiten ohne bekannte Nutzerdaten deutlich unterschiedliche Ergebnisse. Nach einer zweitägigen Synchronisationspause untersuchte man die Zugangsmöglichkeiten und die dadurch entstehenden Möglichkeiten, ermittlungsrelevante Daten zu extrahieren. Die Fitness-Smartwatch ließ sich auch hier ohne Komplikationen mit dem neuen Account koppeln. Obwohl ein neues Gerät und ein neuer Account verwendet wurde, synchronisierte die *Garmin Forerunner 55* sowohl in der Fitnessapplikation als auch in der untersuchten Tabelle alle ermittlungsrelevanten Daten seit dem Zeitpunkt der letzten Synchronisierung aufgezeichnet wurden.

Diese Erkenntnis ist für einen IT-Forensiker von großem Interesse, da die Untersuchung zeigte, dass die *Garmin Forerunner 55* mindestens drei Tage ermittlungsrelevante Daten aufzeichnen, speichern und anschließend auf ein neues Gerät mit neuem Account übertragen kann. Dem ermittelnden Forensiker ist es somit möglich, Zeiträume mit den dazugehörigen Daten nachzuvollziehen, die ab der letzten Synchronisierung erzeugt wurden.

5.3 Fitbit Inspire 2

Als letztes Gerät wurde der Fitnesstracker *Fitbit Inspire 2* untersucht. Dieser wurde als zweiter einer Chip-Off-Analyse unterzogen, die in ihrer anspruchsvollen Durchführungsweise deutlich unterschiedliche Ergebnisse im Gegensatz zum *Xiaomi Mi Smart Band 6* erzielte. Im Folgenden sollen die einzelnen Ergebnisse diskutiert werden.

Die erste Untersuchung in Bezug auf das Synchronisations- und Speicherverhalten zeigte, dass der *Fitbit Inspire 2* ebenfalls in der Lage ist, bis zu sieben Tage die definierten ermittlungsrelevanten Daten aufzuzeichnen, zu speichern und zu synchronisieren. Während die beiden bereits diskutierten Geräte eine konstante Synchronisierung, sowohl in der Datenbank als auch Fitnessapplikation aufwiesen, synchronisiert der *Fitbit Inspire 2* allein in der Fitnessapplikation. Die untersuchte Tabelle „HEART_RATE_DAILY_SUMMARY“ wies während der Untersuchung auffällige Verhaltensweisen auf, indem sie entweder nach den definierten Synchronisierungszeiträumen leere Tabellen aufwies oder beim Wechsel der Simulationsgeräte aus unbekannten Gründen die Ruheherzfrequenz seit Beginn der Untersuchung in die Tabellen ergänzte. Um eine Begründung für dieses besondere Verhaltensmuster zu finden, kann im Folgenden nochmals auf das Teilkapitel 2.2.1 verwiesen werden. Betrachtet man den hier untersuchten Fitnesstracker, so sprechen die genannten Verhaltensmuster dafür, dass der Fitnesstracker die aufgezeichneten und gespeicherten Rohdaten nicht selbst verarbeiten kann. Die Daten werden deshalb über ein gekoppeltes Endgerät zu einem entfernten Server gesendet (vgl. Teilkapitel 2.2.1), der die Daten verarbeitet und anschließend in der Fitnessapplikation grafisch und feingranular zur Verfügung stellt.

Ein weiterer Aspekt, der für diese Begründung spricht, wäre, dass die *fitbit*-Fitnessapplikation nur mit einer aktiven Internetverbindung die ermittlungsrelevanten Daten aus dem Fitnesstracker synchronisieren und grafisch in der Applikation darstellen kann. Sobald keine Internetverbindung besteht, ist die grafische Oberfläche der Fitnessapplikation leer und der Fitnesstracker lässt sich nicht synchronisieren. Diese Erkenntnis ist nicht nur für die Begründung relevant, auch aus forensischer Sicht gilt es den besonderen Umstand zu beachten, dass eine Untersuchung der auf dem Fitnesstracker abgelegten Daten nur mit einer aktiven Internetverbindung durchgeführt werden kann.

Die zweite Untersuchung nach den Zugangsmöglichkeiten zeigte, dass es auch bei der *Fitbit Inspire 2* möglich ist, über die in der Untersuchung angewandten Verfahren, ermittlungsrelevante Daten zu extrahieren. Wie auch bei den vorherigen Untersuchungsgeräten ist es auch hier nötig sicherzustellen, mit Root-Rechten auf das Endgerät zuzugreifen, um mögliche Ruheherzfrequenzdaten zu extrahieren.

Im ersten Teil der Untersuchung verwendete man die Nutzerdaten aus der ersten Untersuchung auf einem neuen Gerät, um sich in der Fitnessapplikation anzumelden. Nach einer Anmeldung unter Beachtung einer aktiven Internetverbindung, ergänzten sich in der leeren Oberfläche der Fitnessapplikation alle Daten, die seit Beginn der Untersuchung erzeugt wurde. Wie beim *Xiaomi Mi Smart Band 6* war der hier untersuchte Fitnesstracker mit dem

Account verknüpft und synchronisierte sich unmittelbar nach der Anmeldung. Durch den Zugang mit Root-Rechten konnte dann festgestellt werden, dass sich in der Datenbank die vermutete Ruheherzfrequenzrate ergänzte, die seit Beginn der Untersuchung aufgezeichnet wurde. Auch die Daten, die seit der letzten Synchronisierung aufgezeichnet, gespeichert und erzeugt wurden, ergänzten sich zu den bereits geladenen in der Fitnessapplikation.

Aus forensischer Sicht kann festgehalten werden, dass bei einer Anmeldung mit bekannten Nutzerdaten keine neue Kopplung mit dem Band durchgeführt werden muss und bei aktiver Internetverbindung alle jemals mit den Account erzeugten Daten synchronisiert werden. Warum bei einem Geräte-Wechsel die Datenbank mit der Ruheherzfrequenzrate beschrieben wird, kann nicht begründet werden.

Anders verhielt sich der Fitnesstracker, als er auf die Zugangsmöglichkeiten durch neue Nutzerdaten untersucht wurde. Bei der Anmeldung mit einem neuen Account war es zunächst wichtig sicherzustellen, ob der Fitnesstracker mit dem neuen Account verknüpft werden kann oder wie beim *Xiaomi Mi Smart Band 6* fest mit dem ursprünglichen Account gekoppelt war. Entgegen der Erwartung ergab die Untersuchung, dass sich der *Fitbit Inspire 2* problemlos mit dem neuen Account verknüpfen ließ. Nach dem Verknüpfen synchronisierten sich weder in der Tabelle „HEART_RATE_DAILY_SUMMARY“ noch in der Fitnessapplikation die Herzfrequenzdaten des festgelegten Synchronisierungszeitraums. Die einzigen synchronisierten Daten waren die Schrittdaten, die in dem Zeitraum erzeugt wurden. Diese Besonderheit gilt es zu beachten, wenn ein ermittelnder Forensiker mit neuen Accountdaten den Fitnesstracker untersuchen möchte.

Im Rahmen der dritten Untersuchung, der Chip-Off-Analyse der *Fitbit Inspire 2,* verzichtete man nach einem erfolgreichen Chip-Off auf eine weitere Datenextraktion. Eine der Hauptgründe sind die fehlenden Informationen, die zu den Chips *CY8C68237FM9-BLET* und *A0330NU12835* zur Verfügung stehen. Mit Blick auf die für Datenextraktion benötigten Information wie etwa Pin-Belegung, Chip-Größe, Gehäusetyp etc. wurde von einer weiteren Untersuchung abgesehen.

6 Fazit und Ausblick

Gegenstand dieses Kapitels ist die Zusammenfassung der aus der Diskussion erzielten forensisch relevanten Erkenntnisse in einem abschließendem Fazit. Es werden Erkenntnisse und Nutzen speziell für die IT-Forensik mit Blick auf die Problemfragen (vgl. Teilkapitel 1.1) dargestellt. Ein anschließender Ausblick blendet auf nicht weiter untersuchte Ergebnisse und stellt in Zukunft zu beachtende Gegebenheiten in den Vordergrund.

6.1 Fazit

In der Einleitung (vgl. Teilkapitel 1.1) wurden nachfolgende Forschungsfragen aufgeworfen:

1. Sind auf den Fitnesstrackern/Fitness-Smartwatches selbst ermittlungsrelevante Daten abgelegt?

2. Wenn ja, wie können diese forensisch gesichert werden?

3. Was ergibt ein Vergleich exemplarisch ausgewählter Hersteller?

4. Ist es möglich, eine entsprechende Handlungsempfehlung für zukünftige derartige Fragestellung für den IT-Forensiker zu erarbeiten?

Nachfolgend werden diese oben erwähnten Fragen beantwortet:

Innerhalb der ersten Problemfrage lässt sich konstatieren, dass die zwei untersuchten Fitnesstracker der Firmen *Xiaomi und Fitibit* und die Fitness-Smartwatch der Firma *Garmin* selbständig ermittlungsrelevante Herzfrequenz- und Schrittdaten aufzeichnen sowie speichern können. Mithilfe eines selbst definierten Untersuchungsdesign zeigte sich, dass alle Geräte in der Lage sind, mindestens sieben Tage diese Daten aufzuzeichnen und zu speichern.

Die Beantwortung der zweiten Frage hingegen zeigte, dass eine generelle forensische Datensicherung mit den derzeit verfügbaren technischen Gegebenheiten möglich ist. Über die Untersuchung möglicher Zugangswege (Neuer und alter Nutzerdaten) sowie der Chip-Off-Analyse der zwei Fitnesstracker, ergaben sich neue forensische Sicherungsmöglichkeiten für die IT-Forensik.

In Bezug auf die dritte Problemfrage ergab ein Vergleich der untersuchten Geräte hinsichtlich der Zugangswege und Chip-Off-Analyse, zahlreiche Gemeinsamkeiten und Unterschiede. Durch den Zugang mittels bekannter Nutzerdaten konnte zusammenfassend ermittelt werden, dass ein IT-Forensiker bei allen Geräten ermittlungsrelevante Daten sichern

kann. Wird der Zugang hingegen über neue Nutzerdaten versucht, so zeigte die Untersuchung, dass bei allen Geräten außer dem *Xiaomi Mi Smart Band 6* Möglichkeiten bestehen, forensisch relevante Daten zu sichern. Als Alternative zum Zugangsversuch über neue Nutzerdaten brachte die Chip-Off-Analyse inklusive einer Datenextraktion, die am *Xiaomi Mi Smart Band 6* und dem dazugehörigen Flash-Speicherchip durchgeführt wurde, einen reichen Fundus an forensisch relevanten Ergebnissen. Entgegen der Erwartung war dieser nicht vollverschlüsselt und ermöglichte dadurch Untersuchungen, die im forensischem Sinne relevante Ergebnisse hervorbrachten. Die Untersuchung zeigte auch, dass alle untersuchten Geräte nach wie vor die erzeugten Daten unverschlüsselt in die jeweiligen SQLite-Datenbanken ablegen, wie es bereits durch Jacoby [6] im Jahr 2019 festgestellt wurde. Der Vergleich der untersuchten Geräte ergab abschließend mehr Gemeinsamkeiten als Unterschiede.

Die vierte und letzte Frage galt hingegen den Zukunftsaussichten derartiger praxisrelevanter Fragestellungen sowie einer Handlungsempfehlung zur Beantwortung dieser. Aufgrund der erzielten Ergebnisse war es möglich eine Handlungsempfehlung für die IT-Forensik zu erstellen, die im Anhang Teil 4 einzusehen und ausführlich dargestellt ist. Die Handlungsempfehlung zeigt den bestmöglichen Verfahrensweg für den IT-Forensiker unter den definierten Bedingungen und gibt eine Übersicht über die zu erwartenden ermittlungsrelevanten Daten. Es bleibt zu hoffen, dass die hier erstmals erstellte Handlungsempfehlung perspektivisch auch Nutzen für die polizeiliche Arbeit erbringen wird.

Im forensischen Sinne ist abschließend zu erwähnen, dass die erzielten Erkenntnisse immer als einzelne Indizien (Puzzleteile) in einem großem Ganzen (Puzzle) betrachtet und stets kritisch hinterfragt werden müssen. So zeigte eine eigens durchgeführte Untersuchung mit dem *Fitbit Inspire 2,* dass die durch den Fitnesstracker erfassten Herzfrequenzdaten auch einfach manipuliert werden können. Die Abbildung 47 veranschaulicht den Manipulationsversuch, der verdeutlicht, dass eine Banane einen durchschnittlichen Puls von 75 Herzschlägen pro Minute besitzt. Blickt man auf die Funktionsweise von optischen Sensoren aus Teilkapitel 2.2.2 so ist es nicht verwunderlich, dass die durch den Sensor ausgesendeten Lichtsignale durch das dicke Fruchtfleisch sowie die Schale der Banane selbst reflektiert werden und dadurch eine scheinbare Herzfrequenz detektiert wird.

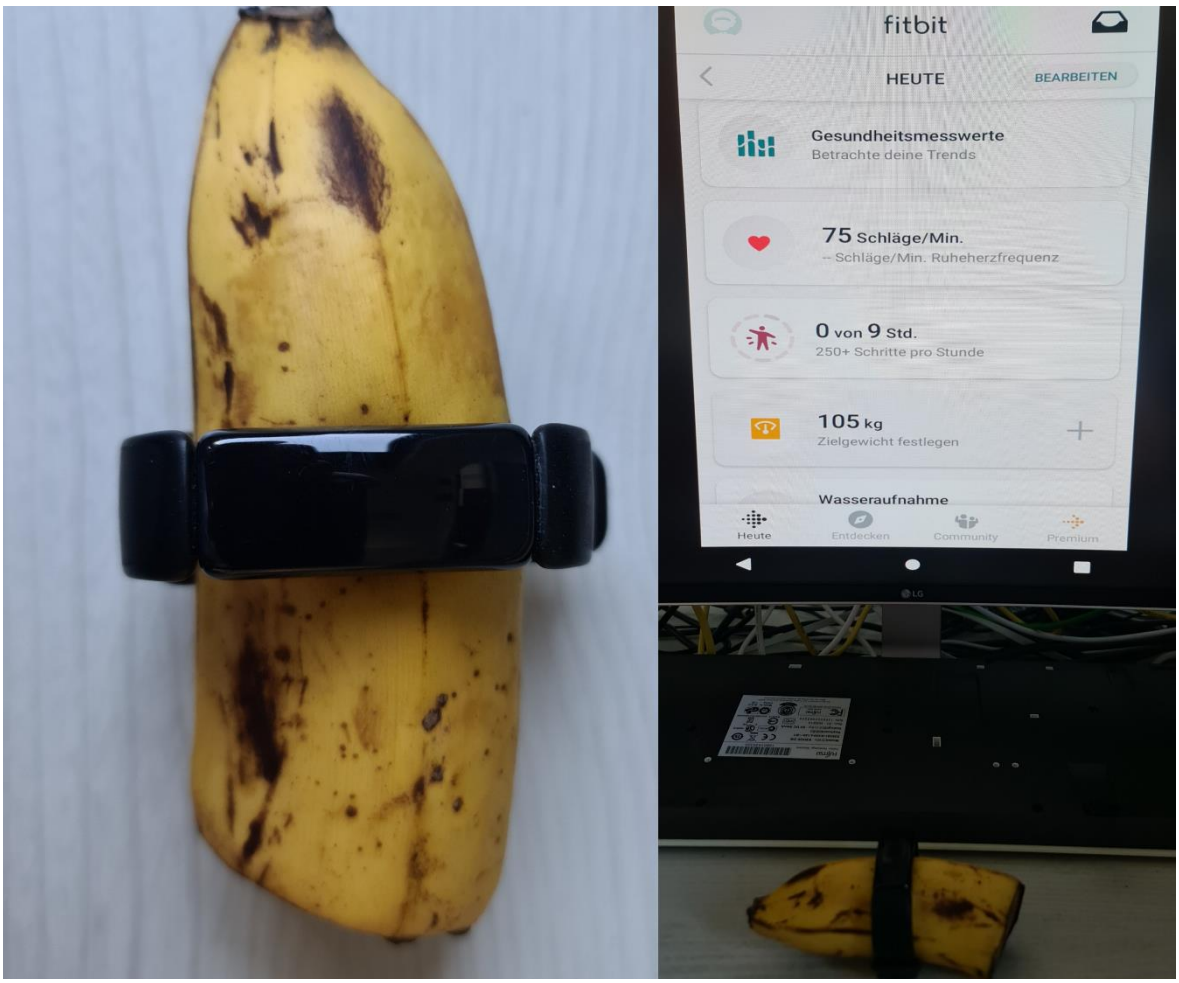


Abbildung 47: Manipulation der gemessenen Herzfrequenz durch den *Fitbit Inspire 2* (Eigene zusammengeschnittene Aufnahmen, Juni 2022)

Der Versuch sollte dabei nicht die „Herzfrequenz von Früchten“ untersuchen, sondern demonstrieren, wie manipulierbar die durch den Fitnesstracker ermittelten Herzfrequenzdaten sein können. Im forensischen Sinne ist es daher immer wichtig, mehrere Indizien in einen Gesamtzusammenhang (Evidenz) zu bringen und niemals ein alleinstehendes Indiz als Beweismittel zu betrachten. Durch manipulierte Herzfrequenzdaten können Beweismittel vor Gericht entkräftet und potenziell beschuldigte Personen entlastet werden. Da es für einen Forensiker jedoch immer um evidenzbasierte Daten in seiner Beweisaufnahme geht, muss jeglicher Manipulationsverdacht verhindert werden.

Zusammenfassend lässt sich festhalten, dass die anfangs aufgestellte Problemstellung gelöst werden konnte. Die Untersuchung zeigte, dass Fitnesstracker und Fitness-Smartwatches als sichergestelltes digitales Beweismittel unbedingt im Rahmen einer forensischen Sonderuntersuchung ausgewertet werden sollten, da diese auch ohne Zugriffsmöglichkeit zum ursprünglich gekoppelten Smartphone ermittlungsrelevante Daten enthalten und somit forensisch relevante Erkenntnisse liefern können.

6.2 Ausblick

In Anbetracht der stetig fortschreitenden Digitalisierung und der damit einhergehenden breiten Verfügbarkeit von Fitnesstrackern und Fitness-Smartwatches lässt sich aus forensischer Sicht festhalten, dass die hier analysierten Geräte langfristig an Bedeutung zunehmen und bspw. bei forensischen Untersuchungen mit beachtet werden müssen. Dabei sollten sich nicht nur die Dienstleister hilfreicher forensischer Software an den Wandel anpassen, auch die IT-Forensiker selbst müssen durch Weiterbildungsmaßnahmen sicherstellen, auf dem neuesten Stand der Forschung und der damit einhergehenden Technik zu bleiben. Ein aktuelles Beispiel ist das Ende Mai 2022 in China vorgestellte neue *Xiaomi Smart Band 7,* welches den Nachfolger des in dieser Bachelorarbeit untersuchten *Xiaomi Mi Smart Band 6* darstellt. Der Fitnesstracker ist seit Juni 2022 auch in Deutschland erhältlich und sollte neben der Namensänderung im Rahmen einer IT-forensischen Untersuchung auf weitere Neuerungen überprüft werden [75]. Der Umstand, dass ein während einer Untersuchung aktuelles Gerät am Ende dieser, durch einen neueren Nachfolger abgelöst wird, verdeutlicht den ständig steigenden Zuwachs an veränderter Technik.

Da sich diese Bachelorarbeit nur mit den in der Zielstellung definierten Untersuchungszielen (vgl. Teilkapitel 1.2) beschäftigt, bleiben für nachfolgende Untersuchungen zahlreiche Forschungsdesiderate. In erster Linie wäre eine Untersuchung in Bezug auf das Speicher- und Synchronisationsverhalten mit länger als sieben Tagen hilfreich. Des Weiteren wäre es lohnend zu untersuchen, was mit den ermittlungsrelevanten Daten passiert, wenn der Akkumulator der Geräte leer und dieser erst im forensischen Labor wieder aufgeladen wird. Auch bei den Ergebnissen in Bezug auf die aus dem Flash-Speicherchip *W25Q256JWPIM* extrahierten Rohdaten bleiben viele Aspekte noch ungeklärt. Neben den Platzhaltern für die Wetterdaten ist eine Begutachtung der Kommunikation mit der App in den Rohdaten mit Sicherheit gewinnbringend. Vor allem die detektierten AES- und ECDH-Schlüssel könnten bei der Entschlüsselungen möglicher Kommunikationsdaten hilfreich sein, um somit die Verhaltensweise des Fitnesstrackers auch in Bezug auf die Kommunikation mit der Fitnessapplikation nachzuvollziehen. Im Rahmen der Untersuchung wurden Geräte namentlich bekannter Hersteller unter einer *Android*-Umgebung getestet. Für nachfolgende Arbeiten wäre somit ebenfalls eine Untersuchung unter *iOS* mit den eventuell dazugehörigen *Apple Watches* interessant und erstrebenswert. Als letzte Forschungsmöglichkeiten ist mit Blick auf die Zugangsmöglichkeiten durch bekannte Nutzerdaten eine Ausgabe der personenbezogenen Daten hilfreich. Nach Art. 15 der DSGVO (Datenschutz-Grundverordnung) müssen die Hersteller, insofern sie personenbezogene Daten erheben, dem Nutzer der Fitnessapplikationen Auskunft über diese geben [76]. Die dadurch zur Verfügung gestellten Datenpakete können aus forensischer Sicht wertvoll sein, da sämtliche mit den Account erzeugten Daten in diesen enthalten sind. Vor der Umsetzung bedarf es hier jedoch einer rechtlichen Klärung, da das eigentliche Nutzerkonto nicht dem Forensiker „gehört“ und es somit nicht „seine“ personenbezogenen Daten sind.

Literatur

[1] E.-W. Luthe, S. V. Müller und I. Schiering, Hg., *Assistive Technologien im Sozial- und Gesundheitssektor,* 1. Aufl. Wiesbaden: Springer Fachmedien Wiesbaden; Imprint: Springer VS, 2022.

[2] Statista, *Themenseite: Wearables.* [Online]. Verfügbar unter: https://de.statista.com/themen/3471/wearables/#topicHeader__wrapper (Zugriff am: 1. Juni 2022).

[3] Statista, *Fitness-Tracker - Absatz weltweit bis 2022* | *Statista* (Zugriff am: 1. Juni 2022).

[4] D. Spiegel, „Stiefvater angeklagt: Fitnesstracker verrät Verdächtigen in einem Mordfall“, *DER SPIEGEL*, 4. Okt. 2018, 2018. [Online]. Verfügbar unter: https://www.spiegel.de/netzwelt/gadgets/fitbit-armband-fitnesstracker-hilft-bei-mordermittlungen-in-den-usa-a-1231463.html. Zugriff am: 1. Juni 2022.

[5] DER STANDARD, „Fitnesstracker überführt Ehemann in Athen als mutmaßlichen Mörder“, *DER STANDARD*, 18. Juni 2021, 2021. [Online]. Verfügbar unter: https://www.derstandard.de/story/2000127527286/fitnesstracker-ueberfuehrt-ehemann-in-athen-als-moerder. Zugriff am: 8. August 2022.

[6] J. Jacoby, „Forensische Untersuchung verbleibender Datenbanken von Fitness-Trackern auf Mobilgeräten“. Bachelorarbeit, Angewandte Computer- und Biowissenschaften, Hochschule Mittweida, Mittweida, 2019.

[7] D. Heinson, *IT-Forensik: Zur Erhebung und Verwertung von Beweisen aus informationstechnischen Systemen*. zugl.: Kassel, Univ., Diss., 2014. Tübingen: Mohr Siebeck, 2015.

[8] K. Marschall, „Rechtsverträgliche Gestaltung IT-forensischer Systeme“. Dissertation, Universität Kassel; Springer Vieweg.

[9] Bundesamt für Sicherheit in der Informationstechnik, „Leitfaden IT-Forensik: Version 1.0.1 (März 2011)“, 2011.

[10] A. Geschonneck, *Computer-Forensik: Computerstraftaten erkennen, ermitteln, aufklären,* 6. Aufl. Heidelberg: dpunkt.verlag, 2014.

[11] D. Pawlaszczyk, „Digitaler Tatort, Sicherung und Verfolgung digitaler Spuren“ in *Forensik in der digitalen Welt: Moderne Methoden der forensischen Fallarbeit in der*

digitalen und digitalisierten realen Welt, D. Labudde und M. Spranger, Hg., Berlin, [Heidelberg]: Springer Spektrum, 2017, S. 113–166.

[12] R. Bodach, *SKRIPT für das Modul Computerforensische Methoden,* 3. Aufl., 2021.

[13] D. Kostadinov, *The mobile forensics process: steps and types - Infosec Resources.* [Online]. Verfügbar unter: https://resources.infosecinstitute.com/topic/mobile-forensics-process-steps-types/ (Zugriff am: 3. Juni 2022).

[14] A. Fukami, S. Ghose, Y. Luo, Y. Cai und O. Mutlu, „Improving the reliability of chip-off forensic analysis of NAND flash memory devices“, *Digital Investigation*, Jg. 20, S1-S11, 2017, doi: 10.1016/j.diin.2017.01.011.

[15] S. Seyrkammer, *Wearable Computing Technology: Potenzielle Einsatzmöglichkeiten in der Industrie*. Hamburg: Diplomica-Verl., 2015. [Online]. Verfügbar unter: http://www.diplomica-verlag.de/

[16] T. Merkel, „Activitytracker“ und Sportuhren als Element der arbeitswissenschaftlichen Analyse: Professur Arbeitswissenschaft, Institut für Produktionstechnik, Westsächsische Hochschule Zwickau, Dr.-Friedrichs-Ring 2a, D-08056 Zwickau“, *Arbeit in komplexen Systemen. Digital, vernetzt, human?!*, A.8.4.

[17] „Fitness-Smartwatch Test & Vergleich: Das sind die beliebtesten Fitness-Smartwatches 2022“, *WELT*, 1. März 2022, 2022. [Online]. Verfügbar unter: https://www.welt.de/vergleich/fitness-smartwatch. Zugriff am: 7. Juni 2022.

[18] R. Mertens, „Fitness-Tracker im Test auf Fitnessarmband.eu“, *fitnessarmband.eu*, 22. Apr. 2017, 2017. [Online]. Verfügbar unter: https://fitnessarmband.eu/so-funktionieren-fitness-armbaender-und-fitness-tracker/. Zugriff am: 8. Juni 2022.

[19] EURONICS, *Activity Tracker/Smartbänder.* [Online]. Verfügbar unter: https://www.euronics.de/telefon-und-navigation/smart-wearables/activity-trackers-martbaender/?p=1 (Zugriff am: 8. Juni 2022).

[20] *rotation_frame.jpg (JPEG-Grafik, 515 × 600 Pixel).* [Online]. Verfügbar unter: https://ase.in.tum.de/lehrstuhl_1/images/projects/sgd-ws13/tutorials/core-motion/rotation_frame.jpg (Zugriff am: 8. Juni 2022).

[21] F. Jung, *Fitness Tracker Test - Wie funktionieren Fitness Tracker und Fitnessarmbänder?* [Online]. Verfügbar unter: https://www.fitness-tracker-test.info/ratgeber/funktionsweise/#bioelektrische_sensoren (Zugriff am: 8. Juni 2022).

[22] F. Jung, *Fitness Tracker Test - Pulsmessung mit optischen Sensoren.* [Online]. Verfügbar unter: https://www.fitness-tracker-test.info/ratgeber/funktionsweise/pulsmessung-mit-optoelektronischen-sensoren/ (Zugriff am: 8. Juni 2022).

[23] Statista, *Wearables - Marktanteile der Hersteller 2021 | Statista* (Zugriff am: 9. Juni 2022).

[24] D. Bretz, *Digitales Diktiergerät als System-on-a-Chip mit FPGA-Evaluierungsboard*. Stuttgart, Universität Stuttgart, Diplomarbeit. Stuttgart: Universitätsbibliothek der Universität Stuttgart, 2001. [Online]. Verfügbar unter: http://elib.uni-stuttgart.de/opus/volltexte/2001/769/

[25] ITWissen.info, *System-on-Chip.* [Online]. Verfügbar unter: https://www.itwissen.info/System-on-Chip-system-on-chip-SoC.html (Zugriff am: 10. Juni 2022).

[26] W. Reisig und J.-C. Freytag, Hg., *Informatik: Aktuelle Themen im historischen Kontext*. Berlin, Heidelberg, New York: Springer, 2006.

[27] T. Häberlein, *Technische Informatik: Ein Tutorium der Maschinenprogrammierung und Rechnertechnik,* 1. Aufl. Wiesbaden: Vieweg + Teubner, 2011.

[28] A. Meroth und P. Sora, *Sensornetzwerke in Theorie und Praxis: Embedded Systems-Projekte erfolgreich realisieren,* 2. Aufl. Wiesbaden, Heidelberg: Springer Vieweg, 2021.

[29] D. Wolski, *Die Technik hinter Solid State Drives (SSDs).* [Online]. Verfügbar unter: https://www.pcwelt.de/ratgeber/Die_Technik_hinter_Solid_State_Drives__SSDs_-Flash-Speicher-8387351.html (Zugriff am: 16. Juni 2022).

[30] J. Schwenk, *Sicherheit und Kryptographie im Internet: Theorie und Praxis,* 5. Aufl. Wiesbaden, Heidelberg: Springer Vieweg, 2020.

[31] A. Geschonneck, „SSH - dem Lauscher keine Chance“, *RZ-Mitteilungen*, Nr. 15, S. 43–47, 1997. [Online]. Verfügbar unter: https://core.ac.uk/display/127600625?utm_source=pdf&utm_medium=banner&utm_campaign=pdf-decoration-v1

[32] *Arbeiten mit SSH-Schlüsselpaaren Regionales Rechenzentrum : Universität Hamburg.* [Online]. Verfügbar unter: https://www.rrz.uni-hamburg.de/services/hpc/grundwissen/ssh-keys.html (Zugriff am: 10. Juni 2022).

[33] M. Kischporski, *EDI - Digitalisierung und IT-Wertbeitrag konkret umgesetzt: Eine Einführung in electronic data interchange und zur Digitalen Transformation*. Wiesbaden, Heidelberg: Springer Gabler, 2017.

[34] C. Baun, *Computer Networks: Bilingual Edition: English – German = Computernetze: zweisprachige Ausgabe: Englisch – Deutsch*. Wiesbaden, Heidelberg: Springer Vieweg, 2019. [Online]. Verfügbar unter: http://www.springer.com/

[35] dementium2.com, *Die 19 besten kostenlosen SFTP- und FTPS-Server für Windows und Linux.* [Online]. Verfügbar unter: https://dementium2.com/net-admin/die-19-besten-kostenlosen-sftp-und-ftps-server-fur/ (Zugriff am: 27. Juni 2022).

[36] C. Funk, „Xiaomi Mi Band 6: NFC-Variante geht in Europa in den Verkauf“, *NETZWELT*, 21. Okt. 2021, 2021. [Online]. Verfügbar unter: https://www.netzwelt.de/news/192600-mi-band-6-erscheint-offenbar-neuer-version-darauf-haben-xiaomi-fans-gewartet-2110.html. Zugriff am: 21. Juni 2022.

[37] *Mi Smart Band 6 - No.1 Wearable Band Brand in the World - Xiaomi Global Official.* [Online]. Verfügbar unter: https://www.mi.com/global/product/mi-smart-band-6/ (Zugriff am: 21. Juni 2022).

[38] T. Deehan, „Fitbit Inspire 2: price, features and new design officially announced“, *Trusted Reviews*, 25. Aug. 2020, 2020. [Online]. Verfügbar unter: https://www.trustedreviews.com/news/fitbit-inspire-2-4046176. Zugriff am: 21. Juni 2022.

[39] *Fitness-Tracker mit Herzfrequenzmessung | Fitbit Inspire2.* [Online]. Verfügbar unter: https://www.fitbit.com/global/de/products/trackers/inspire2 (Zugriff am: 21. Juni 2022).

[40] C. Ellis, *Garmin Forerunner 55 review.* [Online]. Verfügbar unter: https://www.techradar.com/reviews/garmin-forerunner-55 (Zugriff am: 22. Juni 2022).

[41] Garmin und Garmin Ltd. or its subsidiaries, *Forerunner® 55.* [Online]. Verfügbar unter: https://www.garmin.com/de-DE/p/741137#specs (Zugriff am: 22. Juni 2022).

[42] *Raspberry Pi 4 Model B specifications – Raspberry Pi.* [Online]. Verfügbar unter: https://www.raspberrypi.com/products/raspberry-pi-4-model-b/specifications/ (Zugriff am: 22. Juni 2022).

[43] *Raspberry Pi 4 Model B – Raspberry Pi.* [Online]. Verfügbar unter: https://www.raspberrypi.com/products/raspberry-pi-4-model-b/ (Zugriff am: 22. Juni 2022).

[44] *HP Notebook - 15-da0402ng Produktdaten | HP® Kundensupport.* [Online]. Verfügbar unter: https://support.hp.com/de-de/document/c06067530 (Zugriff am: 22. Juni 2022).

[45] Gemini BV, *Olympus SZX9 Mikroskop - Gemini BV.* [Online]. Verfügbar unter: https://www.geminibv.de/labware/olympus-szx9-mikroskop/ (Zugriff am: 22. Juni 2022).

[46] 2. C. Electronic, *TOOLCRAFT AT850D Hot air soldering Digital 550 W +100 - +480 °C | Conrad.com.* [Online]. Verfügbar unter: https://www.conrad.com/p/toolcraft-at850d-hot-air-soldering-digital-550-w-100-480-c-588074 (Zugriff am: 22. Juni 2022).

[47] INTERFLUX® ELECTRONICS N.V, „TD-IF-8300-DE: No-clean, halogenfreies, kolophoniumfreies Flussmittelgel“, *Technische Daten IF 8300*, Ver: 4.0 12-05-20. [Online]. Verfügbar unter: https://cdn.interflux.com/documents/products/IF-8300/TD-IF-8300-DE.pdf

[48] Elnec, *BeeProg2 | Universal flash programmer | Elnec.* [Online]. Verfügbar unter: https://www.elnec.com/en/products/universal-programmers/beeprog2/ (Zugriff am: 22. Juni 2022).

[49] G. Hollingworth, „Introducing Raspberry Pi Imager, our new imaging utility“, *Raspberry Pi*, 5. März 2020, 2020. [Online]. Verfügbar unter: https://www.raspberrypi.com/news/raspberry-pi-imager-imaging-utility/. Zugriff am: 26. Juni 2022.

[50] *DB Browser for SQLite.* [Online]. Verfügbar unter: https://sqlitebrowser.org/ (Zugriff am: 26. Juni 2022).

[51] JetBrains, *PyCharm: die Python-IDE von JetBrains für professionelle Entwickler.* [Online]. Verfügbar unter: https://www.jetbrains.com/de-de/pycharm/ (Zugriff am: 26. Juni 2022).

[52] *PEP 8 – Style Guide for Python Code | peps.python.org.* [Online]. Verfügbar unter: https://peps.python.org/pep-0008/ (Zugriff am: 26. Juni 2022).

[53] *FileZilla - Client Features.* [Online]. Verfügbar unter: https://filezilla-project.org/client_features.php (Zugriff am: 26. Juni 2022).

[54] *FileZilla - The free FTP solution.* [Online]. Verfügbar unter: https://filezilla-project.org/ (Zugriff am: 26. Juni 2022).

[55] Elnec, *PG4UW Software for Elnec programmers | Elnec.* [Online]. Verfügbar unter: https://www.elnec.com/en/products/software/pg4uw/ (Zugriff am: 27. Juni 2022).

[56] RUSOLUT, *Software.* [Online]. Verfügbar unter: https://rusolut.com/visual-nand-reconstructor/vnr-software/ (Zugriff am: 17. Juli 2022).

[57] M. Hörz, *HxD - Freeware Hex Editor und Disk Editor | mh-nexus.* [Online]. Verfügbar unter: https://mh-nexus.de/de/hxd/ (Zugriff am: 18. Juli 2022).

[58] Kali Linux, *binwalk | Kali Linux Tools.* [Online]. Verfügbar unter: https://www.kali.org/tools/binwalk/ (Zugriff am: 18. Juli 2022).

[59] GitHub, *GitHub - ReFirmLabs/binwalk: Firmware Analysis Tool* (Zugriff am: 18. Juli 2022).

[60] R. Ponakala und M. N. Dailey, *LineageOS Android Open Source Mobile Operating System: Strengths And Challenges*, 2020.

[61] Statista, *Android - Anteile der Versionen April 2022 | Statista.* [Online]. Verfügbar unter: https://de.statista.com/statistik/daten/studie/180113/umfrage/anteil-der-verschiedenen-android-versionen-auf-geraeten-mit-android-os/ (Zugriff am: 23. Juni 2022).

[62] LineageOS, *About.* [Online]. Verfügbar unter: https://lineageos.org/about/ (Zugriff am: 23. Juni 2022).

[63] ©. KonstaKANG, *LineageOS 18.1 (Android 11).* [Online]. Verfügbar unter: https://konstakang.com/devices/rpi4/LineageOS18/ (Zugriff am: 23. Juni 2022).

[64] *The Open GApps Project.* [Online]. Verfügbar unter: https://opengapps.org/#about-section (Zugriff am: 23. Juni 2022).

[65] Dialog Semiconductor, *Datasheet DA1469x: Multi-core BLE 5.1 SoC family with system PMU,* 3. Aufl. Verfügbar unter: https://www.mouser.de/pdfDocs/da1469x_datasheet.pdf. Zugriff am: 8. Juli 2022.

[66] Winbond Electronics Corporation, *W25Q256JW Datasheet: 1.8V 256M-BIT SERIAL FLASH MEMORY WITH DUAL/QUAD SPI*. For Industrial & Industrial Plus Grade. Verfügbar unter: https://www.winbond.com/resource-files/W25Q256JW%20SPI%20RevJ%2003102021%20Plus.pdf. Zugriff am: 28. Juni 2022.

[67] *Single vs. Dual vs. Quad SPI | Unterschiede & Ähnlichkeiten.* [Online]. Verfügbar unter: https://evision-webshop.de/Knowledge-Base/Fachartikel/Kommunikationsprotokolle/Protokollvergleiche/Was-sind-die-Unterschiede-zwischen-Single-und-Dual-und-Quad-SPI (Zugriff am: 29. Juni 2022).

[68] Elnec, *DIL8/QFN8-1 ZIF-CS SFlash-1a | Programming adapter | Elnec.* [Online]. Verfügbar unter: https://www.elnec.com/en/products/programming-adapters/DIL8_QFN8-1_ZIF-CS_SFlash-1a/ (Zugriff am: 28. Juni 2022).

[69] Mouser Electronics, *CY8C68237FM9-BLET Cypress Semiconductor | Mouser.* [Online]. Verfügbar unter: https://eu.mouser.com/ProductDetail/Cypress-Semiconductor/CY8C68237FM9-BLET?qs=BJlw7L4Cy7%2F2WJW352qdTw%3D%3D (Zugriff am: 3. Juli 2022).

[70] *Datasheet/Datenblatt CY8C68237FM9-BLET - Infineon Developer Community.* [Online]. Verfügbar unter: https://community.infineon.com/t5/PSoC-6/Datasheet-Datenblatt-CY8C68237FM9-BLET/m-p/357652#M13303 (Zugriff am: 17. Juli 2022).

[71] Oracle, *Was ist JSON?* [Online]. Verfügbar unter: https://www.oracle.com/de/database/what-is-json/ (Zugriff am: 19. Juli 2022).

[72] *Binary patterns in NAND flash memory.* [Online]. Verfügbar unter: https://support.rusolut.com/portal/en/kb/articles/binary-patterns-in-nand-flash-memory-12-3-2020 (Zugriff am: 22. Juli 2022).

[73] G. S. Choi und M. Sung, „Investigating Page Sizes in NAND Flash Memory“, S. 377–379. [Online]. Verfügbar unter: https://pdf4pro.com/amp/view/investigating-page-sizes-in-nand-flash-memory-4effe1.html

[74] Bergische Universität Wuppertal, „Diffie-Hellman-Algorithmus: Schlüsselaustausch“, *SPIONCAMP*, S. 1–2, 2012, Art. no. 4. [Online]. Verfügbar unter: https://ddi.uni-wuppertal.de/www-madin//material/spioncamp/dl/austausch-diffie-hellman-station2.pdf

[75] A. Linsner, *Xiaomi Smart Band 7 (Pro): Diese Features bietet der Fitnesstracker.* [Online]. Verfügbar unter: https://www.vodafone.de/featured/gadgets-wearables/xiaomi-mi-band-7-erscheinungsdatum-specs-alle-infos/#/ (Zugriff am: 26. Juli 2022).

[76] Datenschutz-Grundverordnung, *Art. 15 DSGVO – Auskunftsrecht der betroffenen Person - Datenschutz-Grundverordnung (DSGVO).* [Online]. Verfügbar unter: https://dsgvo-gesetz.de/art-15-dsgvo/ (Zugriff am: 26. Juli 2022).

Anlagen

Anlagen, Teil 1: Vorgehensweise - Chip-Off-Analyse - *Xiaomi Mi Smart Band 6*

Die erste Anlage enthält, unterstützend zur Vorgehensweise der Chip-Off-Analyse beim Fitnesstracker *Xiaomi Smart Band 6* im Teilkapitel 3.5.2.1, diverse Abbildungen, die den Ablauf der Analyse veranschaulichen sollen. Zum Überblick über die Einzelkomponenten sind an den benötigten Stellen gelbe Markierungen mit den jeweiligen Beschriftungen vorhanden.

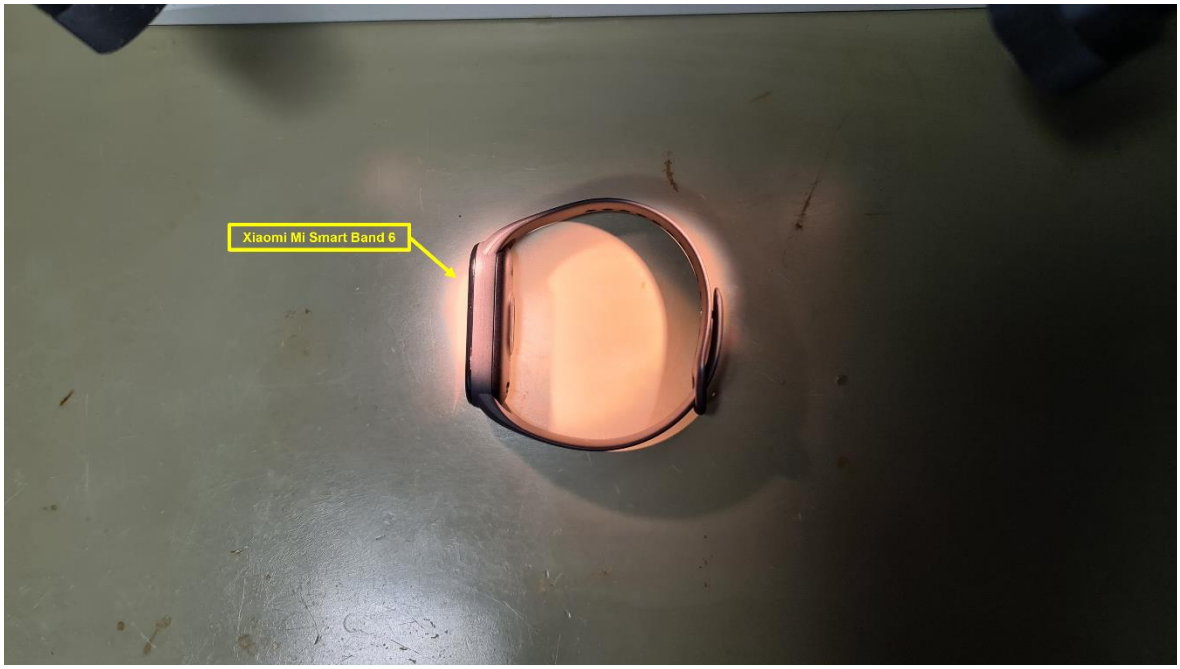


Abbildung 48: Begutachtung des Xiaomi Mi Smart Band 6 (Eigene bearbeitete und zusammengeschnittene Aufnahme, Juli 2022)

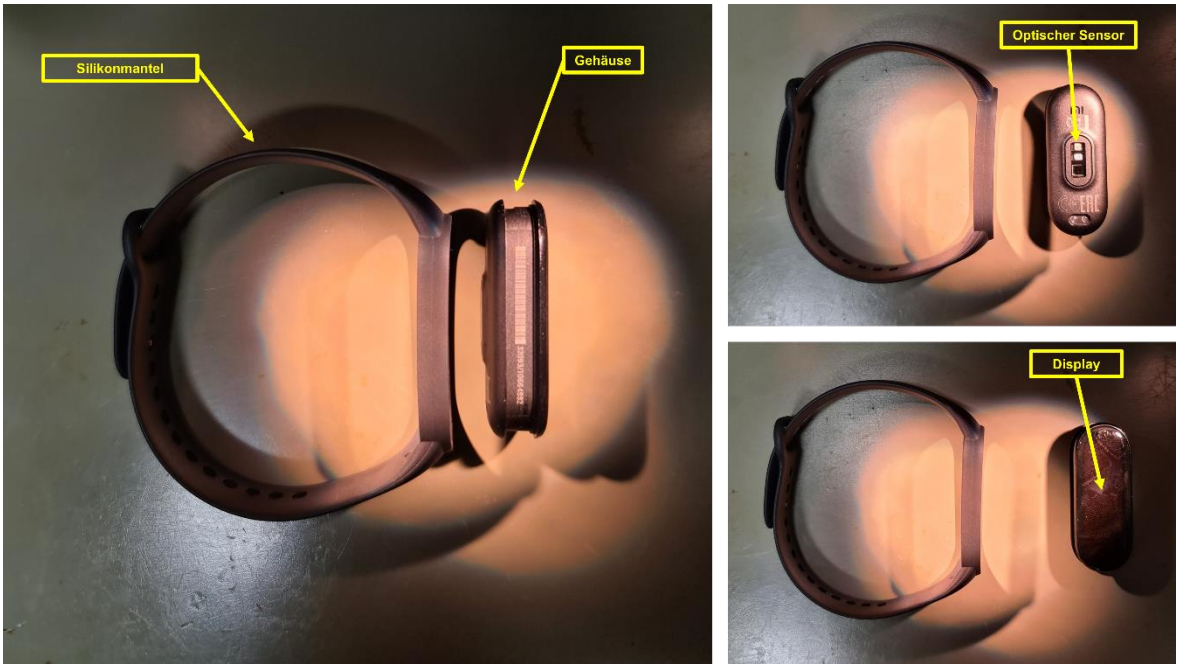


Abbildung 49: Begutachtung vom Silikonmantel und Gehäuses (Eigene bearbeitete und zusammengeschnittene Aufnahmen, Juli 2022)

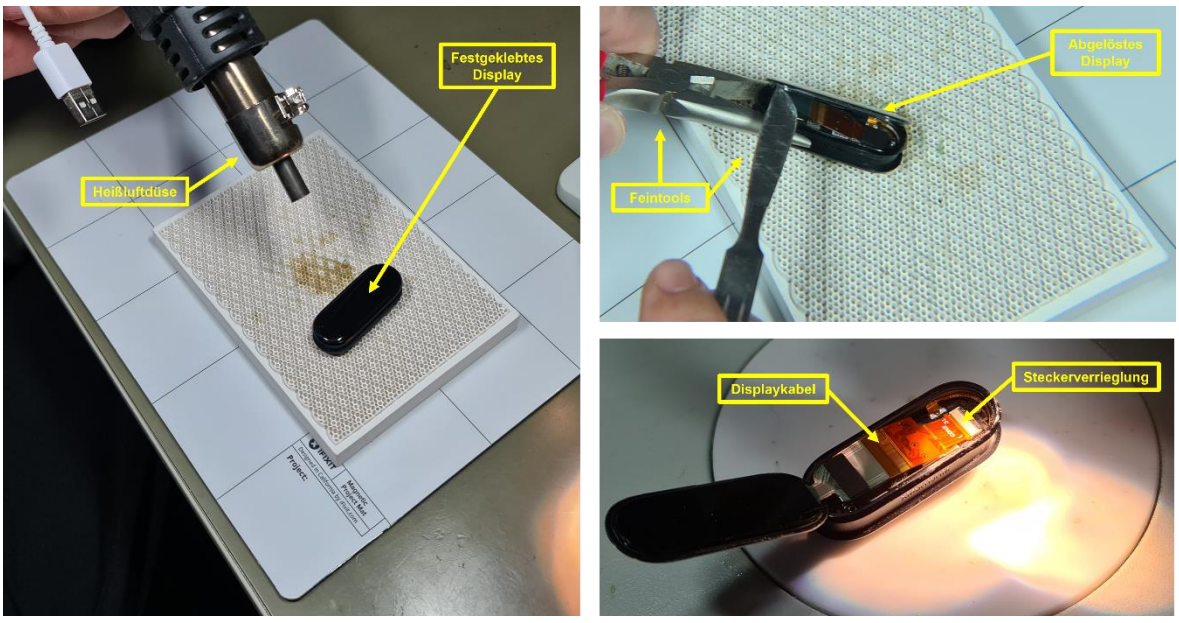


Abbildung 50: Ablösen des Displays vom Gehäuse (Eigene bearbeitete und zusammengeschnittene Aufnahmen, Juli 2022)

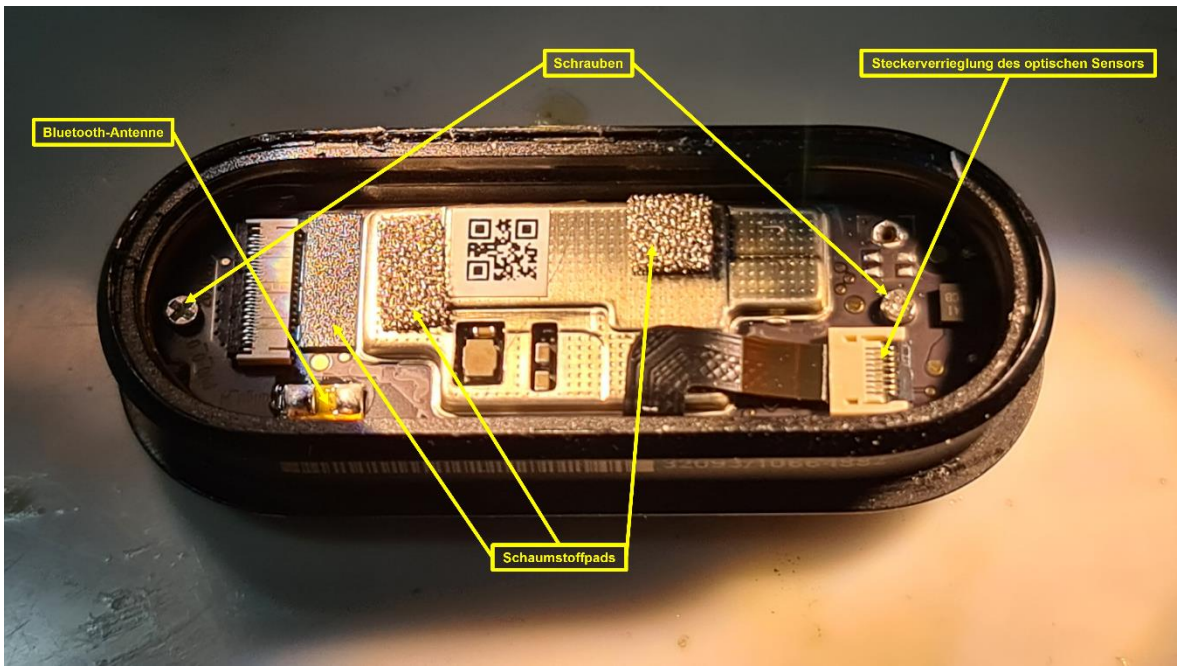


Abbildung 51: Befestigung des Mainboards am Gehäuse (Eigene bearbeitete und zusammengeschnittene Aufnahme, Juli 2022)

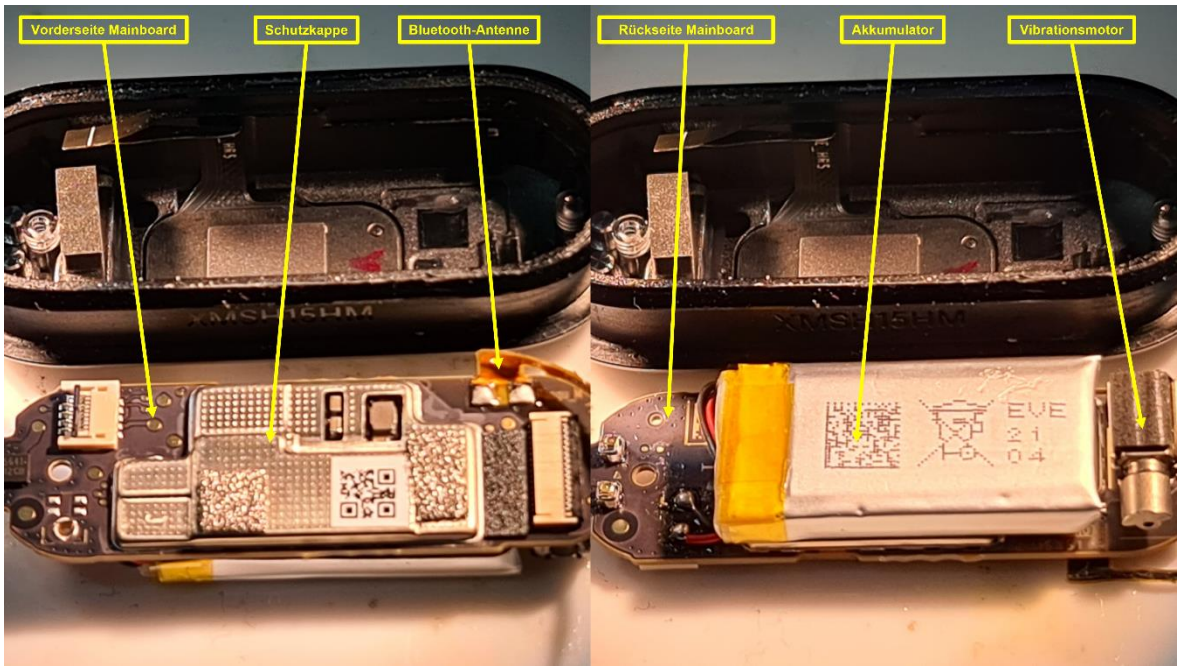


Abbildung 52: Vorder- und Rückseite des Mainboards (Eigene bearbeitete und zusammengeschnittene Aufnahmen, Juli 2022)

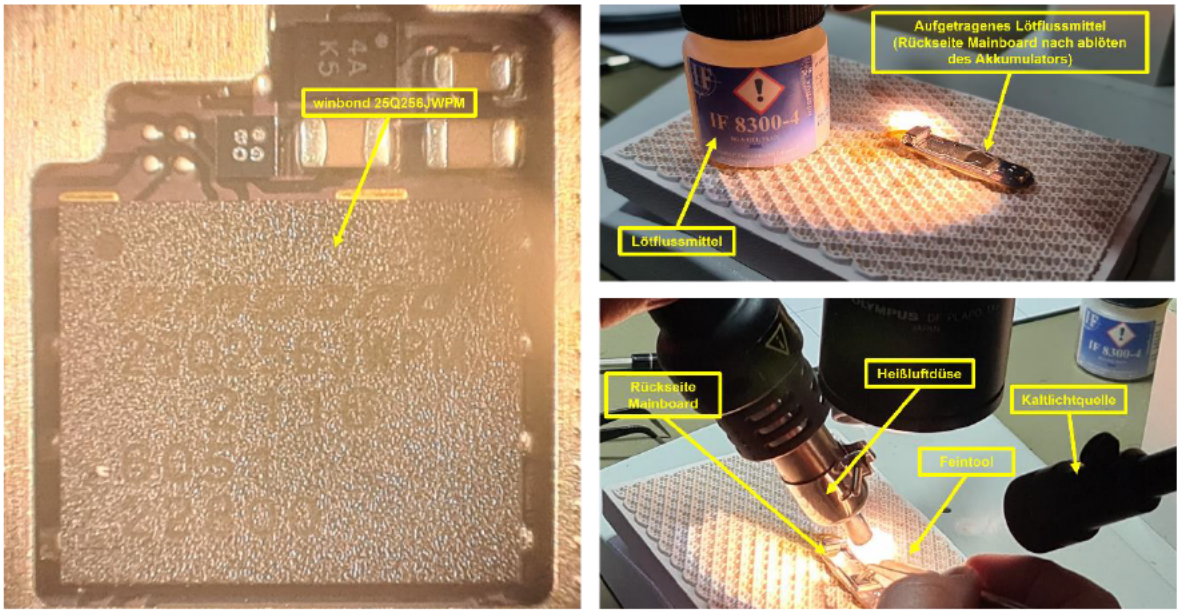


Abbildung 53: Chip-Off vom *winbond 25G256JWPM* (Eigene bearbeitete und zusammengeschnittene Aufnahmen, Juli 2022)

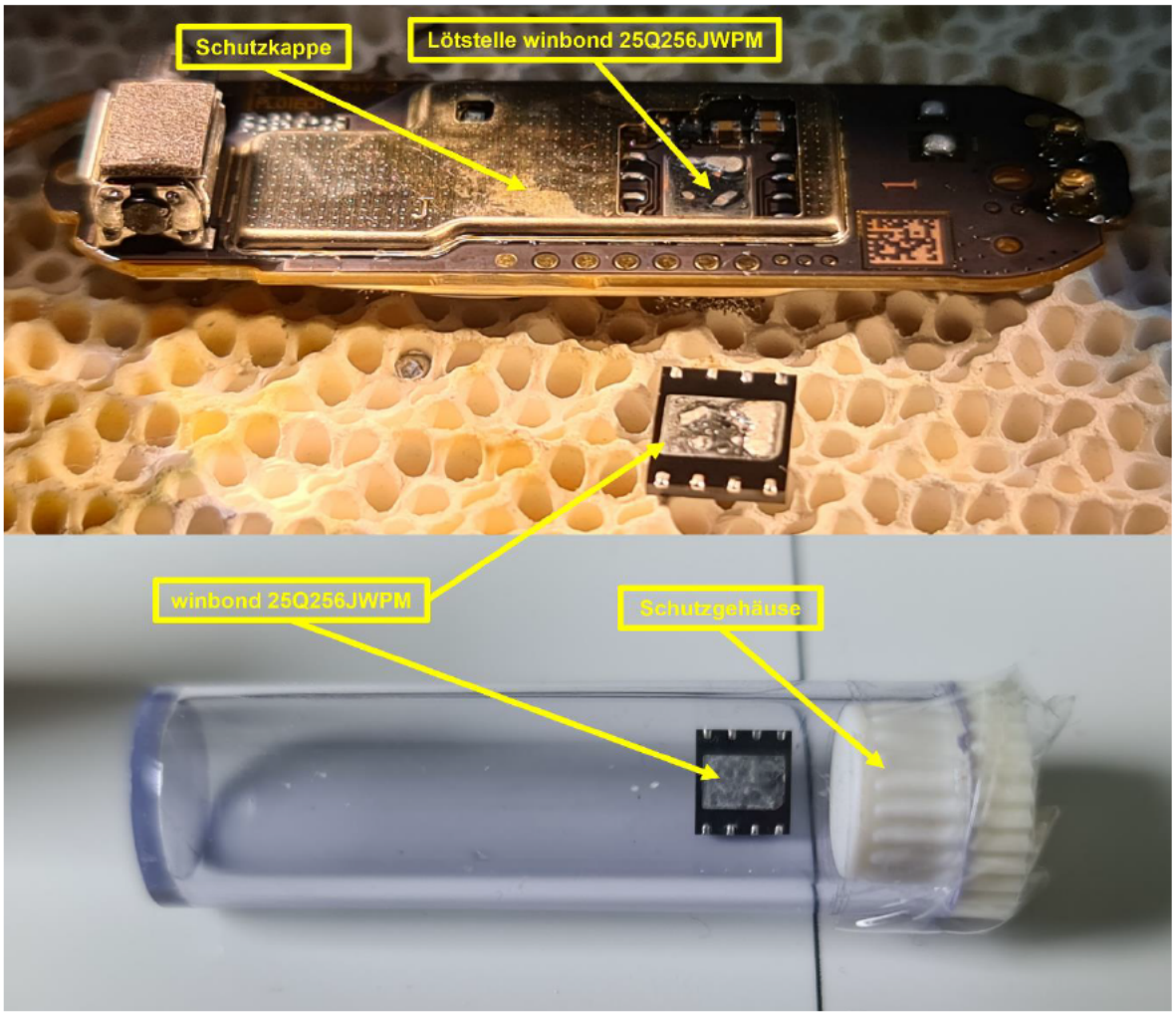


Abbildung 54: Abgelöteter *winbond 25G256JWPM* (Eigene bearbeitete und zusammengeschnittene Aufnahmen, Juli 2022)

Anlagen, Teil 2: Vorgehensweise - Chip-Off-Analyse - *Fitbit Inspire 2*

Die zweite Anlage enthält, unterstützend zur Vorgehensweise der Chip-Off-Analyse, beim Fitnesstracker *Fitbit Inspire 2* im Teilkapitel 3.5.2.2, Abbildungen, die den Ablauf der Analyse veranschaulichen sollen. Zum Überblick über die Einzelkomponenten sind an den benötigten Stellen gelbe Markierungen mit den jeweiligen Beschriftungen eingefügt.

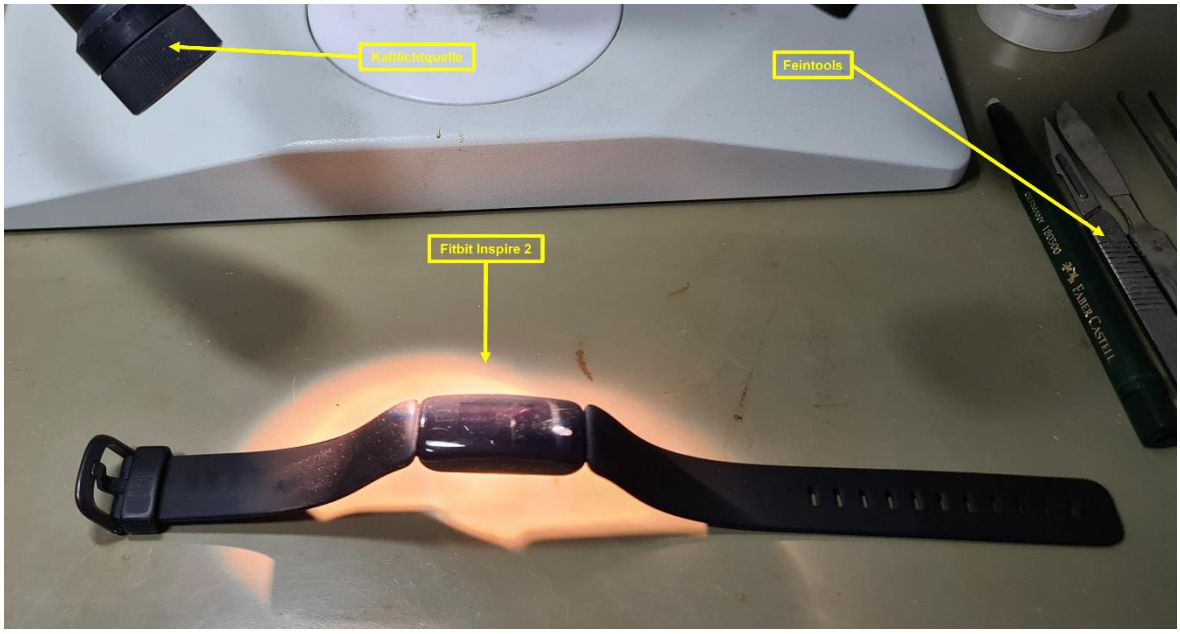


Abbildung 55: Begutachtung des *Fitbit Inspire 2* (Eigene bearbeitete und zusammengeschnittene Aufnahme, Juli 2022)

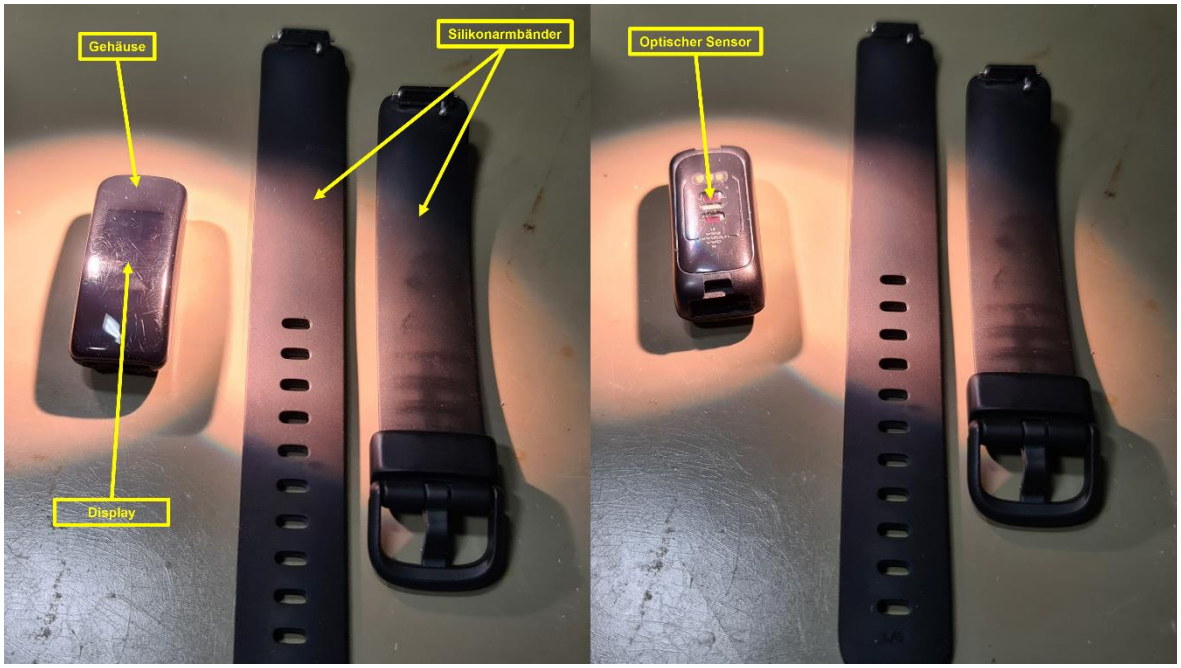


Abbildung 56: Begutachtung der Silikonarmbänder und des Gehäuses (Eigene bearbeitete und zusammengeschnittene Aufnahmen, Juli 2022)

Abbildung 57: Ablösen der Linse vom Gehäuse (Eigene bearbeitete und zusammengeschnittene Aufnahmen, Juli 2022)

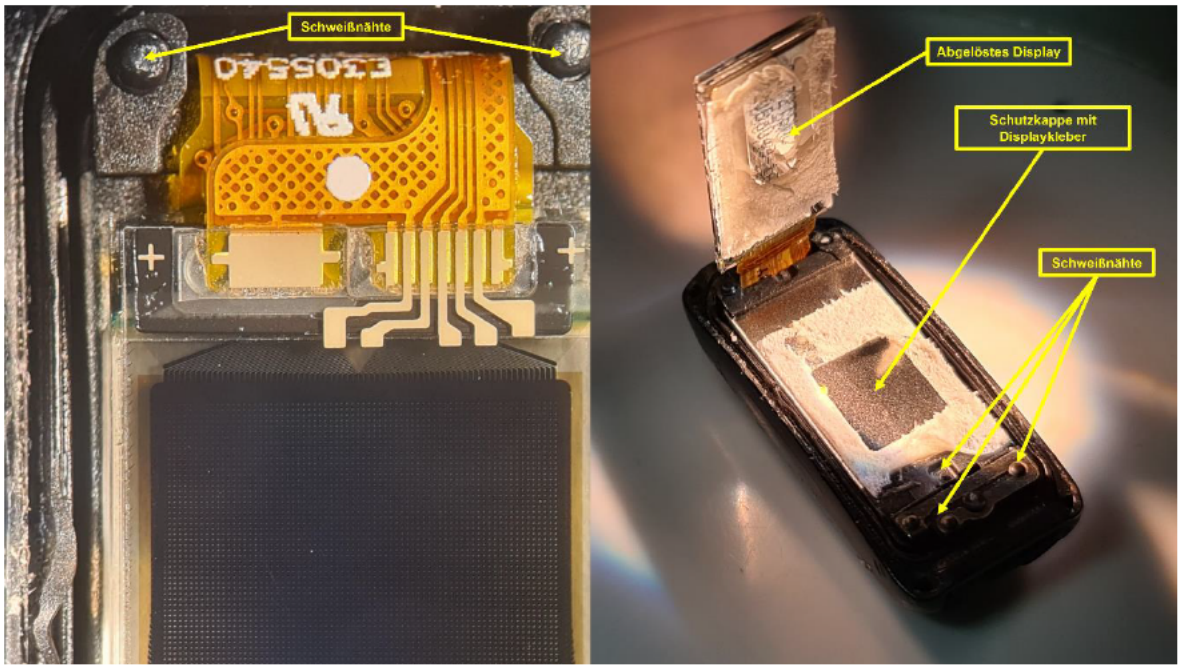


Abbildung 58: Ablösen des Displays (Eigene bearbeitete und zusammengeschnittene Aufnahmen, Juli 2022)

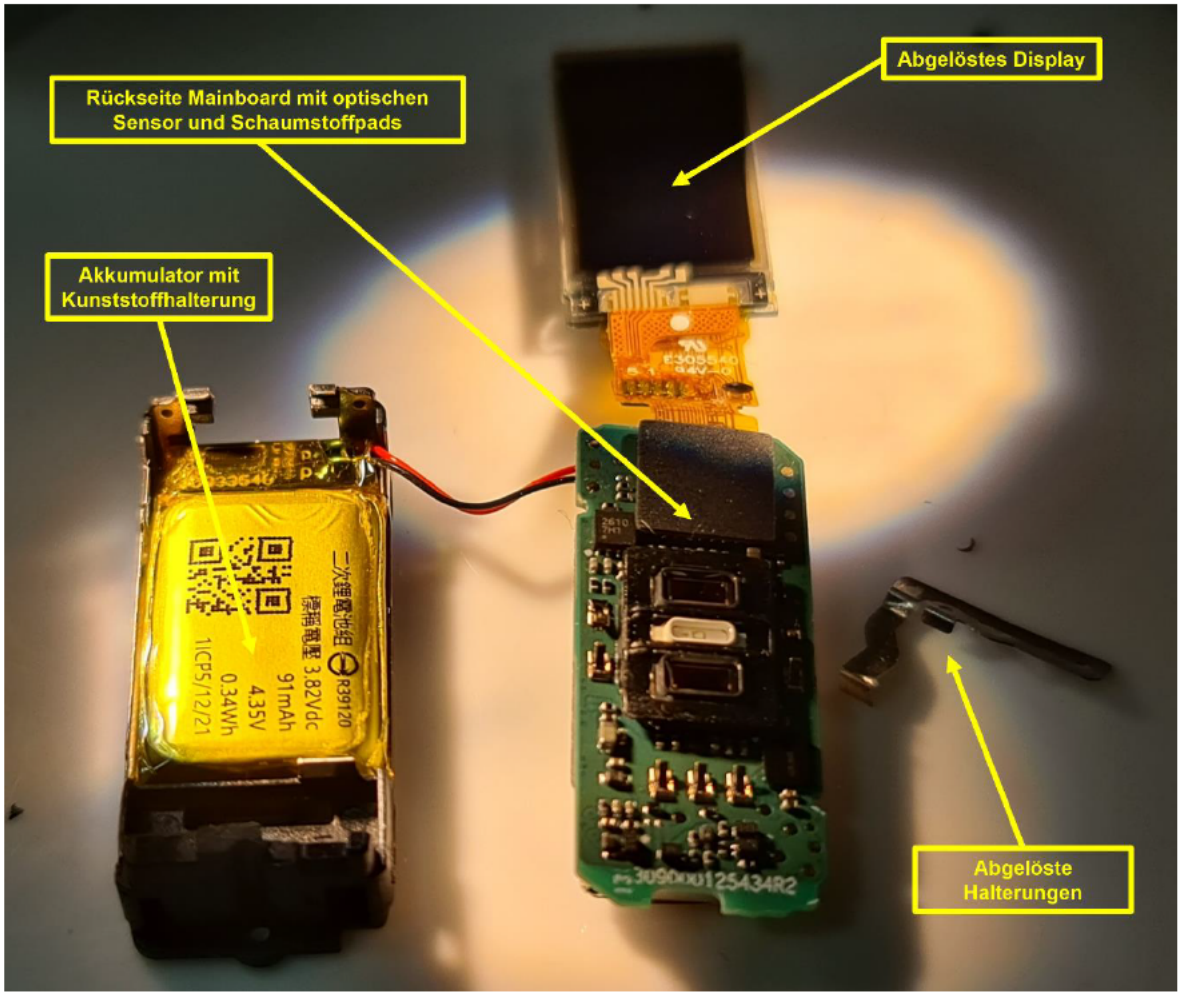


Abbildung 59: Einzelkomponenten des *Fitbit Inspire 2* (Eigene bearbeitete und zusammengeschnittene Aufnahme, Juli 2022)

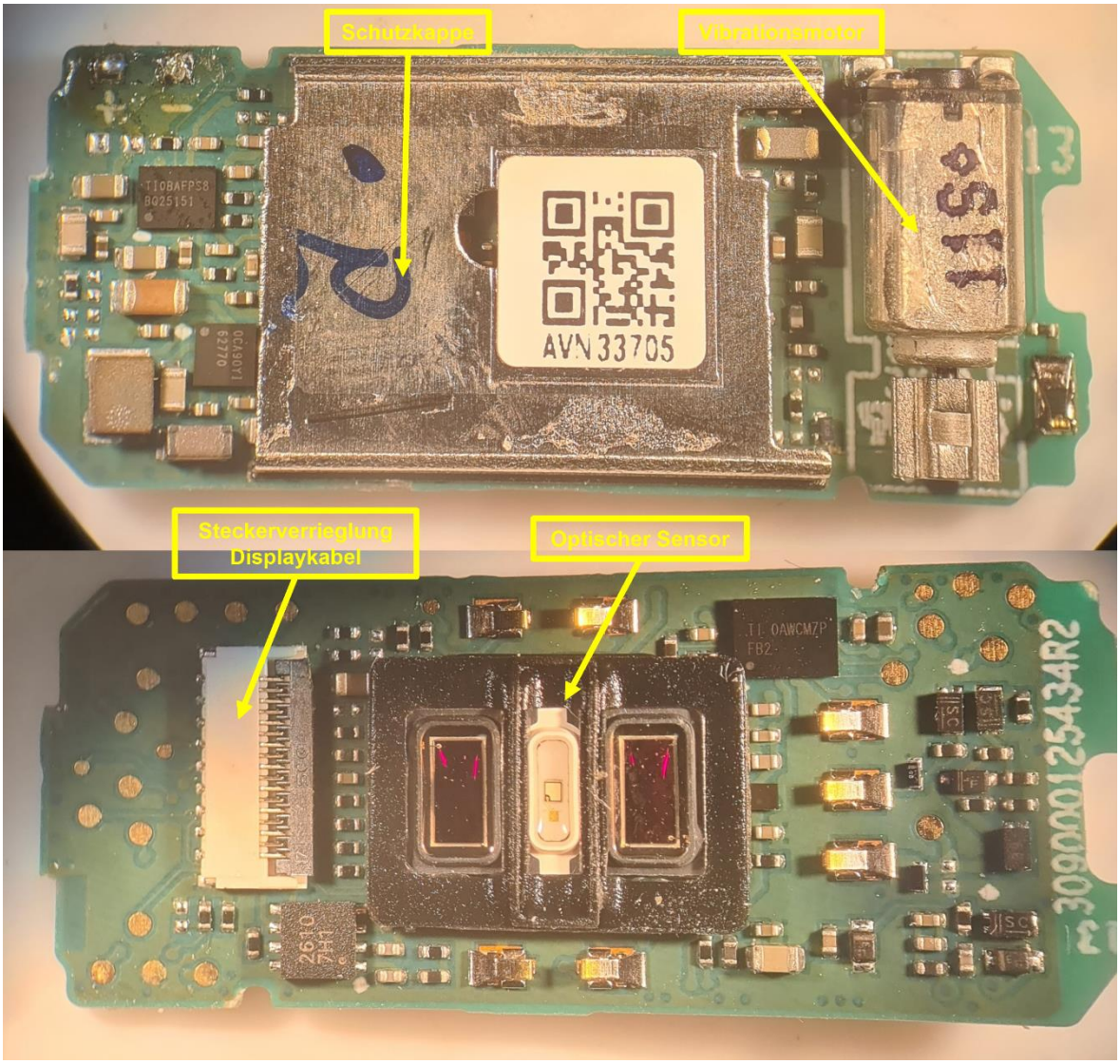


Abbildung 60: Vorder- und Rückseite des Mainboards (Eigene bearbeitete und zusammengeschnittene Aufnahmen, Juli 2022)

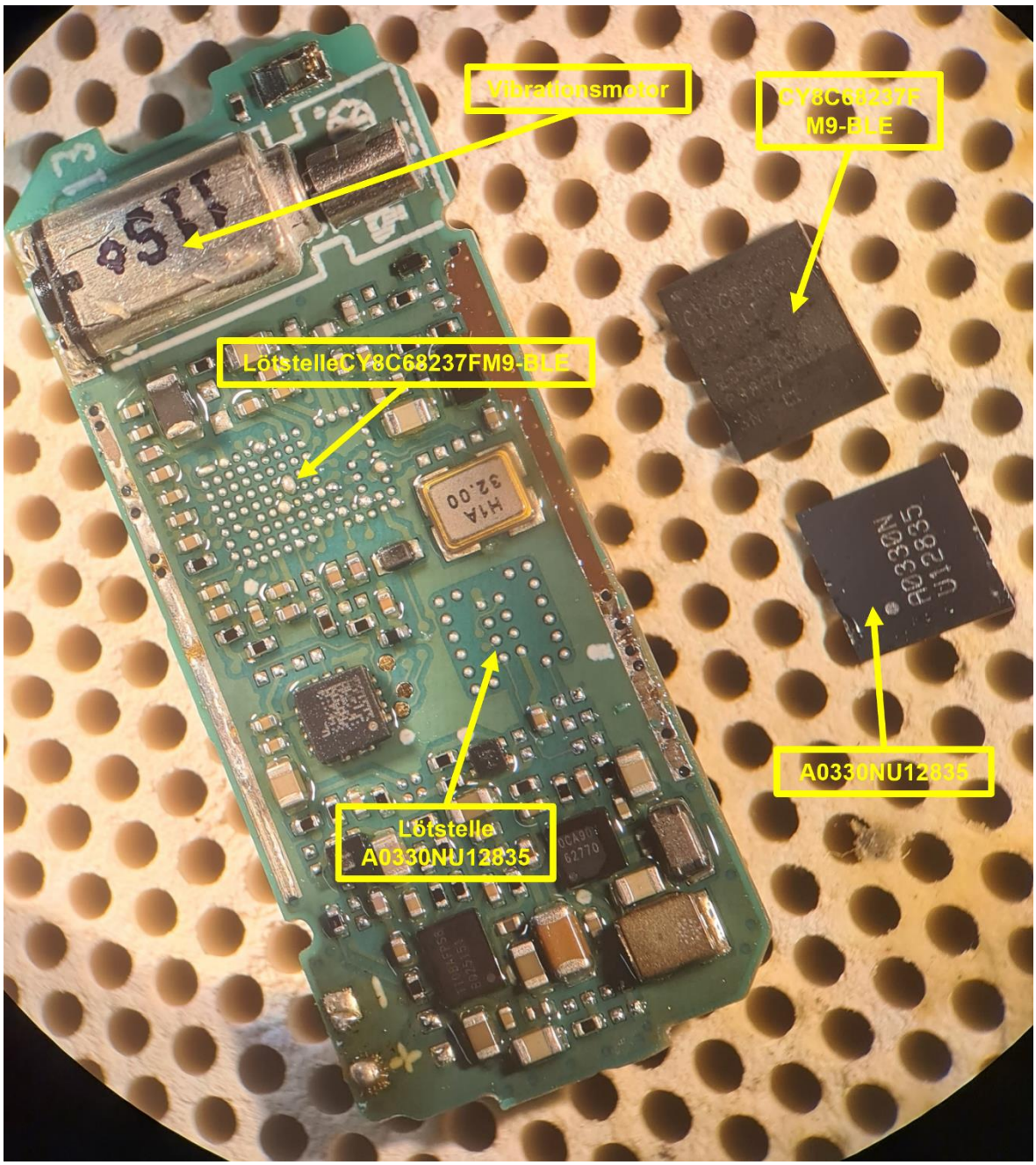


Abbildung 61: Abgelötete Chips *CY8C68237FM9-BLE* und *A0330NU12835* (Eigene bearbeitete und zusammengeschnittene Aufnahme, Juli 2022)

Anlagen, Teil 3: Python Code zur Interpretation der *Xiaomi* Herzfrequenz- und Schrittdaten

Die dritte Anlage enthält den *Python* Code zur Interpretation der Herzfrequenz- und Schrittdaten aus dem *Xiaomi Mi Smart Band 6*. Zum Nachvollziehen der Funktionsweise sind die jeweiligen Funktionen verständlich benannt, eingefärbt sowie kommentiert.

```
#############################################################################
# Imports
import csv
import json
import sqlite3
from tkinter import filedialog

from matplotlib import pyplot as plt


#############################################################################
# Hilfreiche Funktionen
# Feld Eingrenzung für Zeilenausgabe
def parse field(in value, x, y):
    in_value = str(in_value)
    return str(in_value[x:y])


# Funktion für das Konvertieren von 1440 Positionen in Minuten und Stunden
def convert min(minutes):
    hour = minutes // 60
    minutes %= 60
    return "%d:%02d" % (hour, minutes)


# Funktion für das Konvertieren von 144 Positionen in 10 Minuten Schritte und Stunden
def convert min interval(minutes):
    hour = minutes // 6
    minutes %= 6
    return "%d:%02d" % (hour, minutes * 10)


def main():

#############################################################################
    # Datenbank auswählen und Datum nach welchem selektiert werden soll angeben
    filename = filedialog.askopenfilename(initialdir="/",
                                          title="Datenbank bitte auswählen!")
    date = input("Datum bitte im Format 'YYYY-MM-TT' angeben: ")
```

```
##########################################################################
    # Einlesen der Datenbank
    connection = sqlite3.connect(filename)
    cursor = connection.cursor()


##########################################################################
    # Auswählen und Einlesen der Herzfrequenz- und Schrittdaten am einge-
gebenen Datum aus DATE DATA
    try:
        heart rate data = cursor.execute("SELECT quote(DATA HR) FROM
DATE DATA WHERE DATE=" + date).fetchone()
        heart_rate_data = str(parse_field(heart_rate_data, 4, -4))
        steps data = cursor.execute("SELECT quote(STAGE STEPS SUMMARY)
FROM DATE DATA WHERE DATE=" + date).fetchone()
        steps_data_json_string = parse_field(steps_data, 4, -5)
        # Umwandeln des JSON-Ausdrucks in ein Python-Dictionary
        steps data list = json.loads(steps data json string)
    except:
        print("Datum nicht vorhanden. Format überprüfen!")
        exit(1)

    print("################################Herz-
rate#####################################")


##########################################################################
    # Umformatiere der Hexadezimalen Byte-Sequenz der Herzfrequenzdaten
in eine Dezimalzahl-Liste
    heart rate list = []
    temp = 0
    for i in range(0, int(len(heart_rate_data) / 2)):
        # Gehe durch den 1440 langen Byte-String und wandle Hex in Dezi-
mal um (2er Schritte für jedes Byte)
        heart_rate_dec = int(str(heart_rate_data[i * 2:i * 2 + 2]), 16)
        if heart rate dec < 220:
            temp = heart_rate_dec
        heart_rate_list.append(temp)


##########################################################################
    # Konvertieren und Anheften der passenden Uhrzeit zu den 1440 Positi-
onen der erstellten heart_rate_list
    time_list = []
    for i in range(0, len(heart rate list)):
        print(convert_min(i))
        print(heart_rate_list[i])
        time list.append(convert min(i))


##########################################################################
    # Herzrate als Grafik speichern
    f = plt.figure()
    f.set figwidth(50)
    f.set_figheight(6)
    plt.plot(time_list, heart_rate_list, "-r")
    plt.fill between(time list, 0, heart rate list, color='red', al-
pha=.1)
```

```
    plt.savefig(date + 'Herzrate.png')


##########################################################################
    # Herzrate als Tabelle speichern
    with open(date + 'Herzrate.csv', 'w', newline='') as hr_file:
        writer = csv.writer(hr file)
        for i in range(0, len(heart rate list)):
            writer.writerow([time_list[i], heart_rate_list[i]])


print("################################Schritte#############################
##########")


##########################################################################
    # Aufstellen der Schrittliste mit Zeitvermerk
    step_list = []
    for i in range(0, len(steps_data_list) - 1):
        time list.append(steps data list[i]["time"])
        step_list.append(steps_data_list[i]["step"])


##########################################################################
    # Konvertieren und Anheften der passenden Uhrzeit zu den 144 Positio-
nen und Gesamtausgabe Schritte
    time_list = []
    summed steps = 0
    for i in range(0, len(step list)):
        print(convert_min_interval(i))
        print(step_list[i])
        summed steps += step list[i]
        time_list.append(convert_min_interval(i))
    print("Gesamtschritte: " + str(summed_steps))


##########################################################################
    # Schritte als Grafik speichern
    f = plt.figure()
    f.set_figwidth(300)
    f.set figheight(6)
    plt.plot(time_list, step_list, "-b")
    plt.fill_between(time_list, 0, step_list, color='blue', alpha=.1)
    plt.savefig(date + 'Schritte.png')


##########################################################################
    # Schritte als Tabelle speichern
    with open(date + 'Schritte.csv', 'w', newline='') as s_file:
        writer = csv.writer(s file)
        for i in range(0, len(step_list)):
            writer.writerow([time_list[i], step_list[i]])
    connection.close()


if   name   == "  main  ":
    main()
```

Anlagen, Teil 4: Handlungsempfehlung für die IT-Forensik

Die vierte Anlage beinhaltet eine Handlungsempfehlung, die einem IT-Forensiker als Ergebnis dieser Bachelorarbeit dabei unterstützen soll, bezugnehmend auf jeden Hersteller, möglichst effektiv bei der Sicherung und Extraktion ermittlungsrelevanter Daten vorzugehen. Unter der Konstellation einer Einzelsicherung (keine Zugriffsmöglichkeit auf das ursprünglich gekoppelte Smartphone), soll zu Beginn der Handlungsempfehlung eingegrenzt werden, welche Methodik bei den hier untersuchten Fitnesstrackern/Fitness-Smartwatch die besten Ergebnisse hervorbrachte. Hierbei wird auf die Methodenauswahl der Mobilfunkforensik von Kostadinov [13] in Form einer Pyramide (vgl. Teilkapitel 2.1.3) zurückgegriffen. Die Abbildung 62 veranschaulicht die selbst erstellten Pyramiden mit den jeweiligen grafischen Einordnungen für jeden Hersteller. Es wird dabei mithilfe von Piktogrammen zwischen der Untersuchung mit bekannten- und unbekannten Nutzerdaten unterschieden. Welche Methodik die besten Ergebnisse zeigte, kann anhand der Piktogramme abgelesen werden, die in den jeweiligen Ebenen eingeordnet sind.

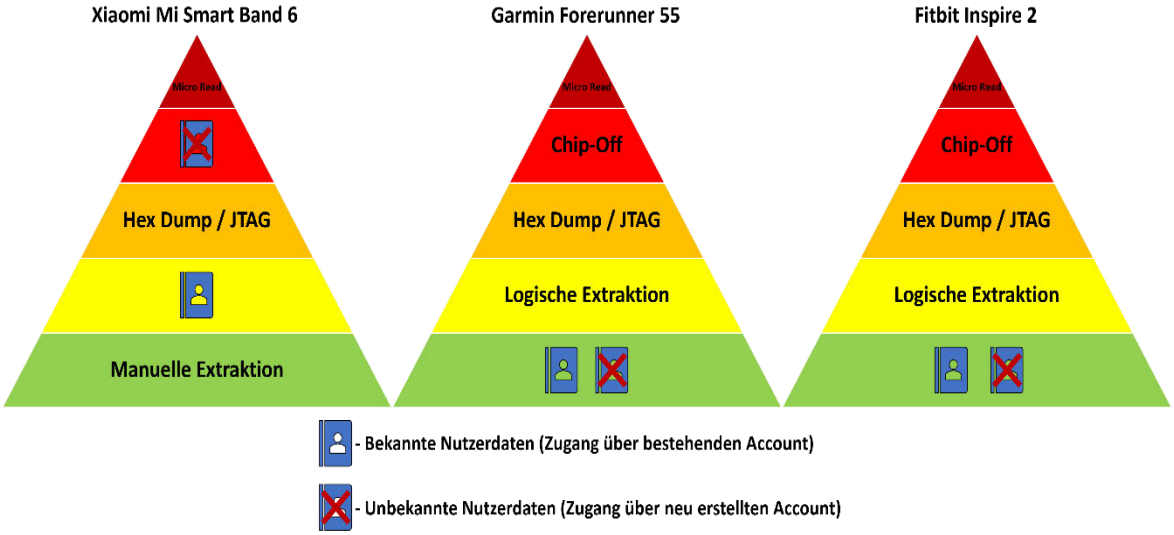


Abbildung 62: Einordnung der Ergebnisse in die Methoden-Klassifikations-Pyramide für jeden Hersteller (Eigene Darstellung basierend auf [13], August 2022)

<u>Für eine erfolgreiche Datensicherung- und Extraktion muss folgendes beachtet werden:</u>

- ✓ **Datensicherung- und Extraktion innerhalb von sieben Tagen vornehmen!**
- ✓ **Eine konstante Internetverbindung auf dem Simulationsgerät gewährleisten!**
- ✓ **Untersuchungsgerät nicht ausschalten (Akku ggf. aufladen)!**

Tabelle 4: Handlungsempfehlung – *Xiaomi Mi Smart Band 6*

Wenn eine Zugriffsmöglichkeit auf das ursprünglich gekoppelte Smartphone besteht, ist eine Betrachtung der verbliebenen Datenbanken empfehlenswert. In diesem Zusammenhang ist auf die Bachelorarbeit von Julian Jacoby zu verweisen. <u>Zugriff über:</u>
https://monami.hs-mittweida.de/frontdoor/index/index/docId/11480

Besteht zum ursprünglich gekoppelten Smartphone keine Zugriffsmöglichkeit, so ist eine Simulation zu einem vergleichbaren Gerät empfehlenswert. Es wird dabei unterschieden, ob die Nutzerdaten der Fitnessapplikation bekannt oder unbekannt sind. Gelingt es nicht, über diesen Weg ermittlungsrelevante Daten zu erlangen, so muss auf eine Chip-Off-Analyse der vorhandenen Speicherchips zurückgegriffen werden. Die folgende Handlungsempfehlung geht auf den besten Verfahrensweg bei bekannten- oder unbekannten Nutzerdaten ein.

Ausgangssituation	
Bekannte Nutzerdaten	Unbekannte Nutzerdaten
Materialien	
Raspberry Pi Model 4 B, Android 11 Custom ROM mit erweiterten Zugriffsrechten (vgl. Teilkapitel 3.4), Untersuchungsgerät (Laptop)	Olympus SZX9 Forschungsstereomikroskop, TOOLCRAFT AT850D Heißluftstation, Interflux IF 8300, BeeProg2, Feintools
Datensicherung	
Logische Datensicherung mittels *FileZilla* (vgl. Teilkapitel 3.5.1)	<u>Chip-Off-Analyse</u>: 1. Speicherchiptypologie erkennen (vgl. Teilkapitel 3.6.2), 2. Physikalische Entnahme des Chips (vgl. Teilkapitel 3.5.2.1)
Datenextraktion	
Extraktion der in der Datenbanktabelle enthaltenen Daten mittels des Python-Skripts (vgl. Teilkapitel 3.7.2.1, Anhang Teil 3)	3. Chips mithilfe von Lese-/Programmiertools (BeeProg2 und PG4UW) auslesen und Daten an Untersuchungsgerät übertragen (vgl. Teilkapitel 3.7.3), 4. Interpretation der extrahierten Daten (vgl. Teilkapitel 4.3)
Zu erwartende ermittlungsrelevante Daten	
Herzfrequenzdaten eines beliebigen Tages und Schrittdaten seit letzter Synchronisierung (Vorraussetzung = Gerät wurde auch dann getragen).	Die Herzfrequenzdaten "der mindestens letzten 24 Stunden", wenn das sichergestellte Gerät auch dann getragen wurde

Als Alternative zu den vorgestellten Handlungsempfehlungen wird eine Datenherausgabe durch den Hersteller empfohlen. Dies kann einerseits durch den Weg der Rechtshilfe, andererseits über die Ausgabe der personenbezogenen Daten umgesetzt werden. Letzteres bedarf jedoch einer rechtlichen Klärung.

<u>Die personenbezogenen Daten der Nutzerkonten können abgerufen werden über:</u>

- ***Xiaomi* = https://privacy.mi.com/support/?locale=en**

Tabelle 5: Handlungsempfehlung – *Garmin Forerunner 55*

Wenn eine Zugriffsmöglichkeit auf das ursprünglich gekoppelte Smartphone besteht, ist eine Betrachtung der verbliebenen Datenbanken empfehlenswert. In diesem Zusammenhang ist auf die Bachelorarbeit von Julian Jacoby zu verweisen. <u>Zugriff über:</u>
https://monami.hs-mittweida.de/frontdoor/index/index/docId/11480

Besteht zum ursprünglich gekoppelten Smartphone keine Zugriffsmöglichkeit, so ist eine Simulation zu einem vergleichbaren Gerät empfehlenswert. Es wird dabei unterschieden, ob die Nutzerdaten der Fitnessapplikation bekannt oder unbekannt sind. Gelingt es nicht, über diesen Weg ermittlungsrelevante Daten zu erlangen, so muss auf eine Chip-Off-Analyse der vorhandenen Speicherchips zurückgegriffen werden. Die folgende Handlungsempfehlung geht auf den besten Verfahrensweg bei bekannten- oder unbekannten Nutzerdaten ein.

Ausgangssituation	
Bekannte Nutzerdaten	Unbekannte Nutzerdaten
Materialien	
Raspberry Pi Model 4 B, Android 11 Custom ROM mit erweiterten Zugriffsrechten und Google-Apps-Paket (vgl. Teilkapitel 3.4)	Raspberry Pi Model 4 B, Android 11 Custom ROM mit erweiterten Zugriffsrechten und Google-Apps-Paket (vgl. Teilkapitel 3.4)
Datensicherung	
Nicht nötig, da eine manuelle Extraktion nach der Anmeldung und Synchronisierung auf dem Simulationsgerät die besten Ergebnisse erzielt	Nicht nötig, da eine manuelle Extraktion nach der Anmeldung und Synchronisierung auf dem Simulationsgerät die besten Ergebnisse erzielt
Datenextraktion	
Manuelle Extraktion der Daten über die Benutzeroberfläche der Fitnessapplikation nach erfolgter Anmeldung (vgl. Teilkapitel 4 2.1.2)	Manuelle Extraktion der Daten über die Benutzeroberfläche der Fitnessapplikation nach erfolgter Anmeldung(vgl. Teilkapitel 4.2.2.2)
Zu erwartende ermittlungsrelevante Daten	
Alle mit dem verknüpften Account erzeugten Daten (Feingranulare grafische Übersicht der Herzfrequenz- und Schrittdaten)	Sämtliche Daten, die seit dem Zeitpunkt der letzten Synchronisierung erzeugt wurden (Feingranulare grafische Übersicht der Herzfrequenz- und Schrittdaten)

Als Alternative zu den vorgestellten Handlungsempfehlungen wird eine Datenherausgabe durch den Hersteller empfohlen. Dies kann einerseits durch den Weg der Rechtshilfe, andererseits über die Ausgabe der personenbezogenen Daten umgesetzt werden. Letzteres bedarf jedoch einer rechtlichen Klärung.

<u>Die personenbezogenen Daten der Nutzerkonten können abgerufen werden über:</u>

- ***Garmin* = https://support.garmin.com/de-DE/?faq=W1TvTPW8JZ6LfJSfK512Q8**

Tabelle 6: Handlungsempfehlung – *Fitbit Inspire 2*

Wenn eine Zugriffsmöglichkeit auf das ursprünglich gekoppelte Smartphone besteht, ist eine Betrachtung der verbliebenen Datenbanken empfehlenswert. In diesem Zusammenhang ist auf die Bachelorarbeit von Julian Jacoby zu verweisen. Zugriff über: https://monami.hs-mittweida.de/frontdoor/index/index/docId/11480

Besteht zum ursprünglich gekoppelten Smartphone keine Zugriffsmöglichkeit, so ist eine Simulation zu einem vergleichbaren Gerät empfehlenswert. Es wird dabei unterschieden, ob die Nutzerdaten der Fitnessapplikation bekannt oder unbekannt sind. Gelingt es nicht, über diesen Weg ermittlungsrelevante Daten zu erlangen, so muss auf eine Chip-Off-Analyse der vorhandenen Speicherchips zurückgegriffen werden. Die folgende Handlungsempfehlung geht auf den besten Verfahrensweg bei bekannten- oder unbekannten Nutzerdaten ein.

Ausgangssituation	
Bekannte Nutzerdaten	Unbekannte Nutzerdaten
Materialien	
Raspberry Pi Model 4 B, Android 11 Custom ROM mit erweiterten Zugriffsrechten und Google-Apps-Paket (vgl. Teilkapitel 3.4)	Raspberry Pi Model 4 B, Android 11 Custom ROM mit erweiterten Zugriffsrechten und Google-Apps-Paket (vgl. Teilkapitel 3.4)
Datensicherung	
Nicht nötig, da eine manuelle Extraktion nach der Anmeldung und Synchronisierung auf dem Simulationsgerät die besten Ergebnisse erzielt	Nicht nötig, da eine manuelle Extraktion nach der Anmeldung und Synchronisierung auf dem Simulationsgerät die besten Ergebnisse erzielt
Datenextraktion	
Manuelle Extraktion der Daten über die Benutzeroberfläche der Fitnessapplikation nach erfolgter Anmeldung (vgl. Teilkapitel 4.2.1 3)	Manuelle Extraktion der Daten über die Benutzeroberfläche der Fitnessapplikation nach erfolgter Anmeldung (vgl. Teilkapitel 4.2.2 3)
Zu erwartende ermittlungsrelevante Daten	
Alle mit dem verknüpften Account erzeugten Daten (Feingranulare grafische Übersicht der Herzfrequenz- und Schrittdaten)	Schrittdaten, die seit dem Zeitpunkt der letzten Synchronisierung erzeugt wurden (Feingranulare grafische Übersicht der Schrittdaten)

Als Alternative zu den vorgestellten Handlungsempfehlungen wird eine Datenherausgabe durch den Hersteller empfohlen. Dies kann einerseits durch den Weg der Rechtshilfe, andererseits über die Ausgabe der personenbezogenen Daten umgesetzt werden. Letzteres bedarf jedoch einer rechtlichen Klärung.

Die personenbezogenen Daten der Nutzerkonten können abgerufen werden über:

- ***Fitbit* = https://help.fitbit.com/articles/en_US/Help_article/1133.htm**

Selbstständigkeitserklärung

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

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

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

Mittweida, den 26.09.2022

Leander Hoßfeld

Nutzungs- und Verwertungsrechte

Ich übertrage zusätzliche Nutzungs- und Verwertungsrechte für die vorliegende Arbeit und allen damit in Zusammenhang stehenden Daten auf Grundlage der *Creative Commons Lizenz* "*CC0*" an alle genannten Betreuer dieser Arbeit.

Mittweida, den 26.09.2022

Leander Hoßfeld