HOCHSCHULE
MITTWEIDA
University of Applied Sciences

BACHELORARBEIT

Frau
Sandra Schmidt

Forensische Analyse von WLAN Routern im Hinblick auf die Ermittlung flüchtiger Daten

Mittweida, August 2023

Fakultät **Angewandte Computer- und Biowissenschaften**

BACHELORARBEIT

Forensische Analyse von WLAN Routern im Hinblick auf die Ermittlung flüchtiger Daten

Autorin:
Sandra Schmidt

Studiengang:
IT-Forensik / Cybercrime

Seminargruppe:
CC19w1B

Erstprüfer:
Prof. Dipl.-Ing. (BA) Ronny Bodach

Zweitprüfer:
Dipl. Inf. Andreas Sommer

Einreichung:
Mittweida, 21.08.2023

Verteidigung/Bewertung:
Mittweida, 2023

Faculty of **Applied Computer Sciences and Biosciences**

BACHELOR THESIS

Forensic analysis of WiFi routers in order to identify volatile Data

Author:
Sandra Schmidt

Course of Study:
IT-Forensics / Cybercrime

Seminar Group:
CC19w1B

First Examiner:
Prof. Dipl.-Ing. (BA) Ronny Bodach

Second Examiner:
Dipl. Inf. Andreas Sommer

Submission:
Mittweida, 21.08.2023

Defense/Evaluation:
Mittweida, 2023

Bibliografische Beschreibung:

Schmidt, Sandra:
Forensische Analyse von WLAN Routern im Hinblick auf die Ermittlung flüchtiger Daten. – 2023. – 60 S.
Mittweida, Hochschule Mittweida – University of Applied Sciences, Fakultät Angewandte Computer- und Biowissenschaften, Bachelorarbeit, 2023.

Referat:

Die vorliegende Arbeit beschäftigt sich mit der Erforschung des Datenvorkommens im Hinblick auf die Ermittlung flüchtiger Daten an ausgewählten Wireless Local Area Network (WLAN)-Routern. Diese werden im Hinblick auf strafrechtlich relevante Fragestellungen untersucht. Es werden die Möglichkeiten der methodisch und systematischen Datensicherung eruiert und wie diese gewonnen und ausgewertet werden können.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

A . . . . . Ampere | Stromstärke

AP . . . . . Access Point

ARP . . . . . Address Resolution Protocol

AuthMode . . . . . Authentifizierungs Modus

AVM . . . . . Audiovisuelles Marketing

BGA . . . . . Ball Grid Array | Kugelgitteranordnung

bsp. . . . . . Beispiel

bzw. . . . . . beziehungsweise

CLK . . . . . Clock | dt. Takt

CMD . . . . . Command and Response | dt. Befehl und Antwort (Steuerpin der SD-Karte)

cmd . . . . . Command Prompt

COM . . . . . Communication

CPU . . . . . Prozessor

CSV . . . . . Comma-separated values

Dat0 . . . . . Datenleitung [Bit 0]

DC . . . . . Direct Current

dd . . . . . convert and copy

DDR . . . . . Double Data Rate

DECT . . . . . Digital Enhanced Cordless Telecommunications

DHCP . . . . . Dynamic Host Configuration Protocol

DSL . . . . . Digital Subscriber Line

eMMC . . . . . embedded MultiMedia Card

GB . . . . . Gigabyte

GbE . . . . . Gigabit-Ethernet

Gbps . . . . . Gigabit pro Sekunde

GHz . . . . . Gigahertz

GND . . . . . Erdung

HTERM . . . . . HyperTerminal

I/O . . . . . Input / Output

IDC . . . . . International Data Corporation

IEEE . . . . . Institute of Electrical and Electronics Engineers

IoT . . . . . Internet of Things

IP . . . . . Internet Protokoll

JTAG . . . . . Joint Test Action Group

K . . . . . Kilo

kB . . . . . Kilobyte

kiB . . . . . Kebibyte

KML . . . . . Keyhole Markup Language

LAN . . . . . Local Area Network

LED . . . . . light-emitting diode, dt. Leuchtdiode

ls . . . . . list

LTE . . . . . Long Term Evolution

m . . . . . Meter

mA . . . . . Milliampere

MAC . . . . . Media-Access-Control

Mbit/s . . . . . Megabits per Second

MEZ . . . . . Mitteleuropäische Zeit

MHz . . . . . Megahertz

MiB . . . . . Mebibyte

mm . . . . . Millimeter

MU-MIMO . . . . . Multiuser Multiple Input, Multiple Output

NAS . . . . . Network Attached Storage

NAT . . . . . Network Adress Translation

OSI . . . . . Open Systems Interconnection model

PC . . . . . Personal Computer

PSK . . . . . Pre-shared key

QoS . . . . . Quality of Service

RAM . . . . . Random Access Memory, dt. Arbeitsspeicher

RX . . . . . Receive Data

SATA . . . . . Serial ATA

SD Card . . . . . Secure Digital Memory Card, dt. sichere digitale Speicherkarte

SoC . . . . . System on a chip

SSH . . . . . Secure Socket Shell

SSID . . . . . Service Set Identifier

TCP . . . . . Transmission Control Protocol

Telnet . . . . . Teletye network

TFTP . . . . . Trivial File Transfer Protocol

TX . . . . . Transmit Data

UART . . . . . Universal Asynchronous Receiver / Transmitter

UMTS . . . . . Universal Mobile Telecommunications System

USB . . . . . Universal Serial Bus

V . . . . . Spannung

VCC . . . . . Voltage at the common collector

VDC . . . . . Volt Direct Current

VoIP . . . . . Voice over IP | Internettelefonie

VPN . . . . . Virtual Private Network

WAN . . . . . Wide Area Network

Wi-Fi . . . . . Wireless Local Area Network

WiGLE . . . . . Wireless Geographic Logging Engine

WLAN . . . . . Wireless Local Area Network

WPA . . . . . Wi-Fi Protected Access [Wi-Fi-geschützter Zugriff]

WPS . . . . . Wi-Fi Protected Setup

www . . . . . World Wide Web

1 Einleitung

Als Gegenstand des täglichen Lebens hat sich unter vielen technischen Errungenschaften das Smartphone als ständiger Begleiter des Menschen manifestiert. Hierbei stellt das fernmündliche Gespräch nicht mehr das ausschlaggebende Beschreibungsmerkmal eines mobilen Telefongerätes dar. Die Nutzung dessen verkörpert eine Vielfalt an Möglichkeiten. Aus der Studie 'Anteil der Onliner, mobilen Internetnutzer und Nutzungsplaner in Deutschland im Jahr 2021' kann eruiert werden, dass 91% dafür stimmen das Internet zu nutzen. Hiervon konnten nochmals 82% als mobile Internetnutzer herauskristalisiert werden [1].

Mit dem Smartphone in der Hand, ein Browser geöffnet und schnell in den Weiten des World Wide Web (www) nach Informationen recherchiert oder dem Freund / der Freundin eine Nachricht zukommen lassen. Durchschnittlich verbringt der Mensch bis zu 138 Minuten je Tag [2] allein mit seinem Smartphone. Für die Nutzung des Internets lag der 'Anteil der mobilen Internetnutzer in Deutschland in den Jahren 2015 bis 2021' 2015 bei noch 54%. 2021 konnte bereits ein Anstieg auf 82% verzeichnet werden [3].

Immerzu ist der Mensch überall erreichbar und muss es unter Umständen auch sein. Umso deutlicher wird dies mit der Feststellung, dass '2018 erstmals häufiger das Smartphone als der PC / LapTop' [3] zur mobilen Internetnutzung gewählt wurde. Zu der neuen Freiheit der ständigen Erreichbarkeit hat sich neben der fernmündlichen Kommunikation der auf dem elektronischen Wege schriftliche Kommunikationsaustausch weiter denn je in den Tagesablauf eines jeden Einzelnen integriert [4]. Hierzu gehört, dass eine Verbindung zu Kommunikationspartnern via einer Internetverbindung eine schnelle und einfache Lösung für viele Menschen geworden ist. Laut einer Umfrage liegt der 'Anteil der Personen in Deutschland, die das Internet zum Telefonieren oder für Videoanrufe nutzen, in den Jahren 2008 bis 2022' im steigenden Trend. Der Umfrage kann entnommen werden, dass im Vergleich zum Jahr 2008 15% zum Jahr 2022 59% der Nutzung zusagten [5].

Wo unterwegs für die Internetnutzung noch überwiegend LTE genutzt wird, gestaltet sich im privaten Heimbereich, aber auch dem beruflichen Umfeld, die verfügbare kabellose Internetverbindung über WLAN. Mit einer kabelungebundenen Internetverbindung über WLAN zu einem Router, welche die Datenpakete auf dem schnellsten Weg beziehungsweise (bzw.) der schnellsten Route über das www verschickt, ergibt sich die Option, das WLAN am Endgerät eingeschaltet zu lassen und sich mit bereits ausgehandelten Routern jederzeit unkompliziert zu verbinden. Dies stellt dabei eine neu gewonnene Freiheit dar, deren Bequemlichkeit der Mensch sich gern bedient. Das WLAN am Smartphone bei Nichterreichbarkeit des potenziell zur Verfügung stehenden WLAN-Routers auszuschalten, wird von der Mehrheit der Smartphonebesitzer nicht durchgeführt. Mit der Einstellung der aktiven WLAN-Verbindung durch das mobile Endgerät ist dieses unterwegs zu jeder Zeit auf der Suche nach einem bereits bekannten Router.

1.1 Problemstellung

Die Einstellung der aktiven WLAN-Verbindung durch das mobile Endgerät mag für den Benutzer Bequemlichkeit sein, für Strafverfolgungsbehörden kann diese Einstellung jedoch ein Anhaltspunkt für die Präsenz des Smartphones an einem bestimmten Ort, zu einer bestimmten Zeit werden. Doch

warum sollten ausgerechnet Daten eines WLAN-Routers strafrechtliche Relevanz bieten? In diesem werden keine Suchverläufe gespeichert, auch ist diesem keine Benutzerhistorie zum Verhalten im www zu erforschen. Ab wann greift ein polizeilicher Kontext? Die Möglichkeiten, weshalb ein Interesse seitens der Strafverfolgungsbehörden an vorliegenden Daten bestehen könnte, sind vielfältig und bedürfen einer stetigen Prüfung des einzelnen Sachverhaltes. Für die forensische Analyse eines WLAN-Routers sind verschiedene Fragestellungen denkbar:

- Welche Endgeräte haben sich am Tattag mit dem dortigen WLAN-Router verbunden?
- Wann haben sich Endgeräte aus dem Umkreis des WLAN Bereiches von diesem entfernt?
- Können Aussagen darüber getroffen werden, dass sich Endgeräte an der Tatörtlichkeit befunden haben ohne eine Registrierung mit dem WLAN-Router beabsichtigt zu haben?
- Gibt es Endgeräte, welche sich ohne Erfolg mit dem WLAN-Router verbinden wollten?

Dabei können die Fragestellungen unabhängig des Deliktes ebenso gleich oder ähnlich erscheinen. Ab hier stellt sich den eintreffenden Polizeibeamten und Kriminaltechnikern ebenso die Frage ob Daten verändert werden, wenn diese an ihren persönlichen Endgeräten die WLAN-Konnektivität im eingeschalteten Modus belassen. Würde in so einem Fall die bloße Anwesenheit des Endgerätes Daten auf dem WLAN-Router schreiben? Für die Herangehensweise der forensischen Datensicherung ist ergänzend auf folgende Fragestellungen einzugehen:

- Muss der WLAN-Router für eine forensische Analyse im Labor als Asservat von der Örtlichkeit entnommen werden?
- Besteht die Möglichkeit der forensischen Analyse vor Ort?
- Muss der WLAN-Router im eingeschalteten Zustand verbleiben?
- In welchen Speicherbereichen können sachverhaltsbezogene Daten vorgefunden werden?
- Unter Zuhilfenahme welcher Schnittstellen können Daten extrahiert werden?

Forschungen, welche sich mit den zuvor benannten Fragestellungen auseinander setzen, wurden bisher nicht durchgeführt. Es gibt verschiedene Ansätze, unter welchen WLAN-Router einer Analyse unterzogen wurden. So wurden bereits Forschungen in der Live-Analyse [6] getätigt. Der Fokus während dieser Forschungsarbeit wurde auf die sich aktuell ändernden Daten am System gelegt. Aber auch Forschungen zu WLAN-Routern, unter welchen Gegebenheiten Daten geschrieben bzw. geändert werden können [7].

1.2 Zielsetzung

Es ist die Frage, welche Daten in Routern und in welcher Form diese abgespeichert werden, zu analysieren. In Betracht kommt entweder ein Datenvorkommen von persistenter oder flüchtiger Natur. Während persistente Daten über eine Unterbrechung der Stromzufuhr erhalten bleiben, verlieren die der flüchtigen Natur ihren Wert und gehen mit der Unterbrechung der Stromzufuhr gänzlich verloren.

Die vorliegende Arbeit beschäftigt sich mit der Erforschung des Datenvorkommens im Hinblick auf die Ermittlung flüchtiger Daten an ausgewählten WLAN-Routern. Diese werden im Hinblick auf die zuvor benannten Fragestellungen untersucht. Es werden die Möglichkeiten der methodischen und systematischen Datensicherung eruiert und wie diese gewonnen und ausgewertet werden können.

2 Grundlagen

Für die Untersuchung der erforderlichen Hard- und Software ist vordergründig zu erklären, inwieweit Netzwerke untereinander kommunizieren und welche Daten hierzu von den einzelnen Komponenten gespeichert werden. Zur Beantwortung der zuvor gestellten Fragestellungen bedarf es einer vorherigen Erklärung einiger Begrifflichkeiten, welche anschließend erläutert werden sollen.

2.1 Aufbau internes Netzwerk

Als internes Netzwerk, auch Heimnetzwerk genannt, wird ein solches betrachtet, welches zur Nutzung des Datenaustausches der darin befugten Geräte innerhalb eines definierten Bereiches genutzt wird. Dabei ist die räumliche Ausdehnung ebenso wie der Personenkreis, welcher Zugriff auf das Netzwerk erhält, beschränkt. Der Datenverkehr außerhalb des lokalen Verbundes wird als externes Netzwerk, auch Internet benannt, definiert.

2.1.1 Das Netzwerk

Das Netzwerk verdankt seine Namensgebung aufgrund des Verbundes mehrerer verschiedener Endgeräte bzw. Teilnehmer, welche das gemeinsame Ziel des Datenaustausches bzw. der Nutzung von Ressourcen (Speicherplatz, Nutzung gemeinsamer Programme, Internet) haben. Während die Varianten der Endgeräte zu Beginn noch überschaubar definiert werden konnten, nimmt deren Vorkommen stetig zu. Ob der Personal Computer (PC), der Laptop, das Tablet, das Smartphone oder die Smartwatch, so ist nun auch die Möglichkeit gegeben, die Kamera oder den Fernseher in das Netzwerk mit einzubinden. Durch das Aufleben der Internet of Things (IoT) wird eine schier endlos mögliche Variation an verbundenen Geräten ermöglicht [8].

Zur Identifizierung jedes einzelnen Gerätes verfügen diese über eine eigens im internen Netzwerk vergebene IP-Adresse. Während im externen Netzwerk, dem Internet, die IP-Adressen automatisch an einen Router vergeben werden, können die IP-Adressen des internen Netzwerkes benutzerdefiniert zugewiesen werden.

2.1.2 Kommunikationspartner und Kommunikationsverlauf

Um WLAN nutzen zu können benötigt der Anwender ein WLAN-fähiges Empfangsgerät (PC, Laptop, Tablet, Smartphone, Smartwatch ...) sowie einen Verbindungspunkt (Router, Access Point (AP), Repeater ...), welcher das WLAN-Signal sendet bzw. weitersendet. Kommunikationsgeräte, welche sich kabellos mit dem Verbindungspunkt zu verbinden versuchen, müssen in dem Fall mit einem Drahtlosadapter ausgestattet sein, um Signale sowohl empfangen als auch Signale senden zu können.

Zu Beginn sind sich sowohl die Verbindungspunkte als auch das Empfangsgerät fremd zueinander. Kein Gerät kennt das andere. Um beide Geräte miteinander bekannt zu machen und eine drahtlose Internetverbindung herzustellen und aufrechtzuerhalten, ist ein bekannt machen von Nöten. Das Kennenlernen beider Geräte stellt sich dabei wie folgt dar:

Der Router versendet automatisch in einem fest definierten Zeitintervall Pakete, sogenannte Beacons. Ein Beacon stellt hierbei ein kleines Datenpaket dar, welches mit der Service Set Identifier (SSID), einer Liste der unterstützten Übertragungsraten und der Art der Verschlüsselung beschrieben ist. Als SSID wird der Name des Gerätes bezeichnet unter welchem das Gerät im Netzwerk aufgefunden werden kann. Die Beacons werden kontinuierlich versendet ohne dass diese einem Gerät speziell zugeordnet werden. Mit dem Versenden eines Beacons wartet der Router keine Antwort ab, sondern sendet diese ungeachtet weiter aus, auch wenn zwischenzeitlich ein erfolgreicher Verbindungsaufbau stattgefunden haben sollte. In der Regel erhalten alle Endgeräte die vom Router versandten Beacons, sobald diese die WLAN Aktivität eingeschalten haben und sich in dessen Frequenzbereich und Reichweite befinden. Ein erfolgreicher Verbindungsaufbau kommt zustande indem ein Kommunikationsgerät auf den Erhalt des Beacons mit dem entsprechend korrekten Sicherheitsschlüssel antwortet [8].

2.2 Modem

Das Modem ist ein elektronisches Bauteil der Kommunikationstechnik, welches den Austausch der Signale zwischen dem Router des Heimnetzwerkes und dessen Gegenstelle, dem Internetprovider, umsetzt. Zum Stand der heutigen Technik ist das Modem bereits in den Router integriert. Dennoch sind weiterhin Geräte auch für den speziellen Bedarf separat erhältlich. Der Austausch der Signale erfolgt je nach dessen Übertragungsweg mit optischen Lichtsignalen im Bereich der Glasfasertechnik bzw. den analogen oder digitalen Signalen im Bereich der Funk-, DSL- oder Kabel-Technik. Das Modem und der Router untereinander tauschen die Signale auf dem elektrischen Weg aus. Zusammenfassend stellt das Modem die Verbindung für die internetfähigen Geräte wie auch der Telefonanlage her [9].

2.2.1 Übertragungsweg: Kabel

Kabelrouter nutzen für die Übertragung der Signale das Kabelfernsehnetz. Bekannte Vertreter sind Modelle des Unternehmens Vodafone mit integriertem Kabelmodem [9].

2.2.2 Übertragungsweg: DSL

DSL Modems nutzen zur Übertragung die Kupferleitungen des herkömmlichen Telefons. Auf diese wird das hochfrequente DSL Signal aufmoduliert und beide Signale werden auf dem elektronischen Weg auf derselben Leitung übermittelt. Am Endanschluss wird das DSL Signal mit einem Hoch-/Tiefpassfilter wieder vom Telefonsignal getrennt. Seit der Umstellung der Sprachtelefonie auf Voice over IP | Internettelefonie (VoIP) ist diese Trennung nicht mehr notwendig. Bekannte Vertreter sind Modelle des Unternehmens Audiovisuelles Marketing (AVM) Fritz!Box mit integriertem VDSL-Modem und DSL-Modem sowie Modelle des Unternehmens TP-Link.

2.2.3 Übertragungsweg: LTE-/ UMTS-Mobilfunk

LTE- bzw. UMTS-Router nutzen zur Übertragung der Signale den Mobilfunkbereich. Hierzu werden die elektronischen Signale aus dem Heimnetzwerk vorher in Funksignale umgewandelt um die Kommunikation anschließend über das Mobilfunknetz ins Internet transferieren zu können. Bekannte Vertreter sind Modelle des Unternehmens AVM Fritz!Box mit integriertem LTE-Router [9].

2.2.4 Router ohne Modem

Ein Router ohne Modem wird in der Regel verwendet, wenn ein Modem bereits zur Verfügung steht. Hierbei kann der Internetanbieter bereits sein eigenes Modem bereitgestellt haben, wodurch sich die Verwendung eines Routers mit integriertem Modem erübrigt. Bekannte Vertreter sind Modelle des Unternehmens TP-Link [9].

2.2.5 Übertragungsweg: Glasfaser

Bei der Datenübertragung via Glasfaser werden die Informationen optisch per Licht auf den einzelnen Glasfasern übertragen. Hierzu werden die elektronischen Signale aus dem Heimnetzwerk vorher in optische Signale umgewandelt, um die Daten anschließend über Glasfaser ins Internet transferieren zu können. Bekannte Vertreter sind Modelle des Unternehmens AVM Fritz!Box [9].

2.3 Router

Der Router ist ein elektronisches Bauteil der Kommunikationstechnik, welches für den Austausch der Signale zwischen Netzwerken Verwendung findet. Hierzu stellt dieses eine Verbindung von mindestens zwei Netzwerken her. Mit dem Router und der hergestellten Verbindung können alle Geräte im Heimnetzwerk an dieses angebunden werden. Solch einen Verbund bezeichnet man als heimisches Local Area Network (LAN) bzw. WLAN. In dem heimischen LAN / WLAN wird mittels des Routers die Möglichkeit geschaffen, dass alle Geräte untereinander problemlos Daten austauschen können. Da der Router seine Aufgabe in der Verbindung von Netzwerken versieht, stellt dieser ebenso eine Kopplung des Heimnetzwerkes zum öffentlichen Internet her und ist damit auch für den Internetzugang zuständig [9].

Mit dem Datenversand in einem Netzwerk müssen alle Clients, welche sich mit dem Netzwerk verbinden, miteinander koordiniert werden. Ähnlich wie in einem Telefonbuch werden hier numerische Werte je Client vergeben, welche diesen im aktuellen Netzwerk eindeutig identifizieren können. Der Router vergibt folglich jedem Client eine interne IP-Adresse. Die IP-Adresse ist zur eindeutigen Zuordnung der zu transferierenden Datenpakete notwendig. In das öffentliche Netzwerk agiert der Router nach außen hin mit einer einzigen IP-Adresse. Diese IP-Adresse ist auf den Router adressiert. Die Übersetzung der öffentlichen IP-Adresse in die private IP-Adresse wird durch die Network Adress Translation (NAT) Tabelle durchgeführt.

Ein Router arbeitet nach dem Server-Client-Modell. Hier agiert der Router als Server und das Endgerät als Client. Ein Client repräsentiert eine Endbenutzerstelle, zu welchen der PC, Laptop, Tablet, Smartphone, aber auch die Geräte der IoT zählen. Der Router stellt als zentraler Punkt den Netzwerkknoten dar und koordiniert die Verbindung mehrerer Teilnehmer. Zu den Aufgaben des Routers zählen neben dem Transfer der Datenpakete ebenso die Wahl der dafür besten Route. Ziel ist es, den besten Weg eines Eingangsnetzes zu seinem Zielnetz zu finden. Daher verdankt der Router seinen Namen und bedient sich hierzu einer Routingtabelle.

Für den Transfer der Daten stehen neben der kabelgebundenen Übertragungsmöglichkeit via Ethernet (siehe Punkt '3.5.5 Ethernet') die der kabelungebundenen Übertragung via WLAN zur Auswahl. Auf die Hardware betrachtet beinaltet der Router eine Kombination aus Telefonanlage, Wireless AP, Switch, eine Verbindung zum Network Attached Storage (NAS), der Netzwerkgeräte, als Smart Home Zentrale und fungiert damit als eine Art Verbundmodell.

2.3.1 Local Area Network

Unter einem LAN-Verbund wird ein lokales kabelgebundenes und damit physisches Netzwerk verstanden. Dieses steht einem kleinen, geschlossenen Nutzerkreis zur Verfügung. Kennzeichnend ist die räumliche Begrenzung des Verbundes an Geräten [8] [10].

2.3.2 Wireless Local Area Network

Unter einem WLAN-Verbund wird ein lokales kabelungebundenes und damit logisches Netzwerk verstanden. Dieses steht per Funk einem kleinen, geschlossenen Nutzerkreis zur Verfügung [8] [10]
.

2.3.3 IEEE 802.11 - Standard

Um das lokal vorhandene Netzwerk netzwerkübergreifend in einem gleichen Standard halten zu können, wurden für diese von dem IEEE Normen in 802.11 entworfen. Nach diesen Normen setzt die drahtlose Netzwerkkommunikation auf der Bitübertragungsschicht (physischer Layer, Layer 1) sowie auf der Sicherungsschicht (Mediumzugriff (MAC-Layer), Layer 2) des OSI-Referenzmodells auf [11].

2.3.4 OSI-Referenzmodell

Die Kommunikation eines Netzwerkes bedarf für seine unterschiedlichen Haltestellen genau abgestimmte Zustelloptionen, sogenannte Protokolle. Diese regeln in welcher Form und unter welchen Regeln ein Datenpaket von seinem aktuellen Haltepunkt zum nächsten transferiert wird, um von dort als solches problemlos gelesen und interpretiert werden zu können [8] [12].

In der Informatik wird diese Abfolge mithilfe eines Referenzmodells beschrieben. Dieses fungiert als OSI-Referenzmodell, welches in einer Schichtenarchitektur für Netzwerkprotokolle entworfen wurde. Der Aufbau des Modells wird in sieben Schichten definiert, wovon eine Schicht auf der anderen aufbaut. Der Tabelle '2.1 OSI-Referenzmodell' kann dessen Aufbau entnommen werden.

2.3.5 Sendeleistung und Reichweite WLAN

Grundsätzlich sind zwei Frequenzbänder vorhanden, mit welchem ein Datentransfer über die WLAN Verbindung vorgenommen werden kann. Hierzu stehen dem Anwender neben dem Frequenzband auf 2,4 Gigahertz (GHz) das Frequenzband auf 5 GHz zur Verfügung. Die Unterschiede beider

Layer	Schicht	Protokoll	Hardware
1	Bitübertragung	IEEE 802.3 Ethernet	Hub, Repeater Netzwerkkabel
2	Daten/ Sicherung	ARP, MAC, LLC IEEE 802.3 Ethernet IEEE 802.11 WLAN	Bridge, Switch Wireless Access Point
3	Vermittlung	ICMP, IP	Router
4	Transport	UDP, TCP	
5	Sitzung	DNS, VPN	
6	Darstellung	Proxy, Web, HTTPS	
7	Anwendung	HTTP, TFP, SMTP, DHCP	

Tabelle 2.1: OSI-Referenzmodell, Quelle: Autor

Bänder liegen neben deren Reichweite auch auf dessen Datenraten. Während das Band auf 2,4 GHz eine höhere Reichweite bei geringerer Datenrate bietet, verhält sich das Band auf 5 GHz zu dem des 2,4 GHz gegensätzlich und bietet auf eine kürzere Distanz höhere Datenraten.

Die Reichweite hängt von dem verwendeten Standard (IEEE), dessen Frequenz im GHz-Bereich sowie der Örtlichkeit ab. Dabei kann innerhalb geschlossener Räumlichkeiten die Reichweite enorm beschränkt sein, außerhalb geschlossener Räumlichkeiten jedoch eine beträchtlichere Reichweitenerhöhung vorliegen. Die Werte bewegen sich innerhalb geschlossener Räumlichkeiten auf wenigen Meter (m)n und außerhalb geschlossener Räumlichkeiten mit handelsüblichen Geräten bis zu 100 m. Die Reichweiten sollen jedoch lediglich als Anhaltspunkte und nicht als Richtwerte betrachtet werden. Viele Faktoren können sowohl die Reichweite als auch die Datenrate beeinträchtigen. So wirken sich neben geschlossenen Räumen, anderen physischen Hindernissen, ebenso die unterschiedlichen Arten und Formen von Bebauungen auf dessen Intensität aus. Hierzu spielen Faktoren wie die Dämmung, Stahl, Beton, Wasserleitungen, sowie der Ständerbau eine ausschlaggebende Rolle. So können sich bereits die elektrischen Leitfähigkeiten des Materials nochmals verstärkend auf die Dämpfung des Signals auswirken.

Je nach Größe des Areals kann die Sendeleistung des WLAN Sendegerätes variieren. Um Qualitätseinbrüche einer aktiven Internetverbindung zu umgehen, können verschiedene Hardwaremodule in das interne Netzwerk implementiert werden und die Sendeleistung auf ein höheren Pegel bzw. bestenfalls dem Ausgangssignal zu setzen. Bei solchen Hardwaremodulen kann es sich um APs, Repeater bzw. Mesh-Systeme handeln.

2.4 Weitere Hardware im Netzwerk

Um das Netzwerk im lokalen Bereich ausweiten zu können und somit auch weiter entfernten Geräten den Zugang zum Internet zu ermöglichen, kann weitere Hardware hinzugenommen werden. Diese verfolgen alle dasselbe Ziel: jede Hardware möchte ein verbessertes Internetsignal und eine vergrößerte Netzabdeckung ermöglichen.

2.4.1 Access Point

Der AP dient als Zugriffspunkt des hausinternen Internetsignals und erhöht somit die Reichweite im Heimnetzwerk. Bereiche, welche durch den Router bisher nicht ausreichend oder überhaupt gedeckt werden konnten, können somit mittels eines Internetsignals abgedeckt werden. Der Empfang und das Versenden von Daten charakterisieren den AP neben der Koordination aller Clients miteinander und dem Internet. Bei der Reichweitenerhöhung des Internetsignals erfolgt eine gleichmäßige Verteilung kraftvoller Signale, was zu einer erhöhten Datenauslastung führt. APs müssen mit einem Ethernetkabel mit dem Router verbunden werden, erst dann kann eine Erhöhung der Reichweite, der Stabilität und der Schnelligkeit realisiert werden. Er selbst kann alle anderen Stationen im Funkbereich kontaktieren und diesen Beacons zusenden. Das Intervall hierzu kann manuell eingestellt werden. Bei Versand der Beacons kann dieses von einem im Funkbereich befindlichen Client angetroffen und von diesem aufgenommen werden. Der Client muss das WLAN im aktiven Modus geschalten haben. Mit dieser Einstellung sucht der Client in regelmäßigen Intervallen eine Basisstation, mit welcher dieser eine Verbindung eingehen kann [13]. Der AP stellt im Heimnetzwerk einen für sich separaten Zugriffspunkt dar. Aufgrund dessen besitzt dieser eine eigene Benutzeroberfläche, welche für dessen Konfiguration aufgerufen werden kann. Unter dieser können die SSID sowie ein eigenes Sicherheitskennwort festgesetzt werden.

Zusammengefasst haben APs hauptsächlich dieselben Aufgaben wie Switche oder Bridges, sie verbinden verschiedene Geräte auf hardwarenahem Niveau.

2.4.2 Repeater

Im Gegensatz zu dem AP muss der Repeater nicht mit einem Ethernetkabel mit dem Router verbunden werden. Dieser empfängt das Sendesignal des WLAN-Routers und sendet dieses verstärkt in seinem Umkreis weiter. Hierdurch erfolgt eine Vergrößerung des Umfangs der Netzabdeckung.

2.4.3 Mesh-System

Unter einem Mesh-System bzw. ein Mesh-Netz wird ein Verbund mehrerer APs / Repeater verstanden, welche aufgrund ihrer lokalen Örtlichkeit miteinander verknüpft sind und untereinander kommunizieren. Für die Netzwerkteilnehmer ergeben sich somit für die Datenübertragung innerhalb des Netzwerkes verschiedene Wege. Hierbei sind den Mesh-System-Komponenten die Standpunkte der jeweils anderen bekannt, sodass für jedes Datenpaket die schnellste Route gewählt werden kann. Die Übertragungsrate bleibt während der gesamten Örtlichkeit konstant.

Aufgrund des netzartigen Verbundes und der untereinander erfolgten Kommunikation ist für das Mesh-System kennzeichnend, dass dieses für den Nutzer mit einer einzigen SSID und einem Sicherheitskennwort ausgestattet ist. Für den Nutzer nicht einsehbar bleibt die gerade verbundene Mesh-Komponente.

3 Methoden

Für die Extraktion relevanter Daten muss zunächst festgelegt werden, welche Daten im konkreten Sachverhalt von Interesse sind. Als nächstes ist in Erfahrung zu bringen auf welchen Wegen diese gewonnen werden können.

3.1 Mögliche Spuren in einem Router

Bei der Analyse von Routern ist die Erwartung auf die Datenhaltung groß. Hoffnungen zu Informationen, welche für den strafrechtlichen Kontext sachdienlich sind, bestehen fortwährend. Doch welche Datenlage kann bei der Datensicherung erwartet werden?

Je nach Router kann die Möglichkeit bestehen, diesen im Bereich der Telefonie zu verwenden. So kann ein Router mitunter Daten zu VoIP, der Internettelefonie, aufweisen. Auch kann der Router als Digital Enhanced Cordless Telecommunications (DECT)-Basisstation dienen und somit eine Schnurlostelefonie im Heimbereich ermöglichen. Wenn das Gerät die Möglichkeit der Telefonie beinhaltet, ist die Wahrscheinlichkeit eine Kontaktliste vorzufinden vorhanden. Der Router kann als Mediaserver fungieren oder diverse USB Geräte für einen Datentransfer im Netzwerk beinhalten. Speichergeräte können als NAS-Netzwerkspeicher an den Router angeschlossen werden. Neben den Funktionen der Telefonie und der Speichernutzung fungiert der Router mit Netzwerkdaten. Hierzu können Systemlogs, Logdateien oder Events abgelegt sein. Aus den Daten können neben den Netzwerkverbindungen auch der Netzwerkstatus, die Prozesse und Umgebungsvariablen ermittelt werden. Im Bereich des Netzwerkstatus ist eine Überprüfung zum Zustand der Ports möglich. Wichtigster Punkt für eine Analyse im Bereich der Router Forensik sind die verbundenen bzw. registrierten Geräte. Diese werden von einem Router in Lease-Listen geführt und beinhalten für die jeweiligen Endgeräte neben den IP-Adressen die zugehörigen MAC-Adressen.

Neben diesen Informationen sind Daten zu dem Betriebssystem, Dateisystem und der Systemzeit von Interesse. Es ist zu überprüfen in welcher Form welche Daten vorliegen. Die Beständigkeit stellt einen Analysepunkt dar. Hier sind die Optionen der Flüchtigkeit und Persistenz vorhanden. Flüchtig sind Daten, wenn diese mit dem Beenden der Stromzufuhr ihre Existenz verlieren. Persistent sind Daten, wenn diese über das Beenden der Stromzufuhr erhalten bleiben und mit dem nächsten Neustart erneut aufgerufen werden können. Die Eindeutigkeit stellt einen weiteren Analysepunkt dar. Daten können statisch oder dynamisch sein. Statisch sind Daten, wenn diese unveränderbar vorliegen. Diese Daten liegen überwiegend im persistenten Speicher. Dynamisch sind Daten, wenn diese regelmäßigen Änderungen unterliegen. Diese Daten liegen überwiegend im flüchtigen Speicher.

3.2 Zugriffmöglichkeit

Unter dem Punkt Zugriffmöglichkeit sollen die Daten, welche sich innerhalb des internen Netzwerkes bewegen, analysiert werden. Die Untersuchungen beziehen sich auf Daten, welche der Router aufnimmt, speichert und gegebenfalls den Blicken Dritter verbirgt.

Der Hauptuntersuchungspunkt dieser Arbeit befindet sich im Bereich der live-forensischen Analysemethoden. Aufgrund des Zustandes der Flüchtigkeit von Daten sind diese an dem zu untersuchenden Gerät zu sichern, bevor diese mit der Unterbrechung der Stromzufuhr unwiederbringlich verloren gehen.

Für die Datensicherung am laufenden System ergibt sich eine überschaubare Anzahl an potenziellen Möglichkeiten. Den ersten Ansatzpunkt stellt die grafische Benutzeroberfläche des Routers dar. Diese kann unter seiner ihm hinterlegten IP-Adresse in einem Webbrowser aufgerufen werden. Das Gerät selbst muss sich im selben Netzwerk befinden. Für diesen Punkt ist die Kenntnis des Gerätekennwortes unabdingbar. Dieses kann an vielen Geräten auf der Rückseite des Gehäuses entnommen werden. Einige Modelle von Routern haben weiterhin Standartkennwörter inne. Möglich wäre auch ein Erfragen der anwesenden bzw. betroffenen Personen oder eine Nachschau in den Unterlagen. Ist jedoch jede dieser Möglichkeiten erschöpft, besteht die Möglichkeit sich mittels einer seriellen Verbindung die Datenströme auf der Konsole ausgeben zu lassen. Softwarelösungen wie 'Putty' oder 'HyperTerminal (HTERM)' können für die Herstellung der seriellen Verbindung Verwendung finden. Dabei soll die Aufzählung nicht als abschließend betrachtet werden.

3.3 Sicherungsmöglichkeiten

Der Sicherung von Daten stehen verschiedene Optionen zur Verfügung. Für eine bitgenaue Datensicherung eignet sich der Linux Befehl 'convert and copy (dd)' sowie die Übertragung über das Protokoll 'TFTP'. Die Datensicherung repräsentiert anschließend eine forensische Duplikation. Ein Spiegelbild seines Ursprungs.

3.4 Analysemöglichkeiten

Eine Reihenfolge der Datensicherungen ist aufgrund der Natur der Persistenz bzw. Flüchtigkeit der Daten einzuhalten. Flüchtige Daten sind persistenten Daten vorzuziehen. Für eine Nachvollziehbarkeit sind die Zeitstempel der Geräte mit denen einer vergleichbaren Zeitquelle zu überprüfen. Auf potentiell vorhandene Netzwerkverbindungen mit einer möglichen Option der Fernlöschung bzw. Datenveränderung ist zu achten.

3.4.1 Live-Analyse

Für eine Datensicherung der flüchtigen Daten ist eine Live-Analyse von Nöten. Hierfür muss der Router in physischer Form vorliegen und sich weiterhin im angeschalteten Zustand befinden. Es sind die verschiedenen Methoden bzw. Schnittstellen zu überprüfen, durch welche Daten extrahiert werden können.

Möglich wäre das Vorhandensein von Debug-Schnittstellen, mit welchen ein Zugriff auf die Prozessablaufstruktur und den Datenspeicher vorgenommen werden kann. Hier stellen die seriellen Debug-Schnittstellen JTAG und UART Varianten dar, mit welchen jeweils eine serielle Verbindung zu dem Gerät hergestellt werden kann. Im Fall, dass mindestens eine dieser Schnittstellen vorhanden ist, ist zu prüfen, in welcher Form Schnittstellen für das Ausleiten der Daten vorhanden sind. Hier können sich neben den USB-Schnittstellen auch die Ethernet-Anschlüsse als Schnittstellen zu dem Netzwerkzugriff erweisen.

3.4.2 Post-Mortem-Analyse

Die eben benannten Schnittstellen sind für eine Post-Mortem-Analyse gleichwertig bedienbar, erfassen dann jedoch nicht mehr die flüchtige Datenbasis.

Sollte keine Schnittstelle vorhanden sein, bzw. ein Zugriff auf diese nicht zu dem erwünschten Erfolg geführt haben, so besteht als finale Lösung die Methode des Chip-Offs, dem manuellen Entfernen des Speicherchips. Dies bedingt jedoch, dass jegliche Zugriffsmöglichkeiten und die Bedienung des Gerätes fortan ausgeschlossen werden. Nach dem Entfernen das Speicherchips kann dieses mit spezieller Programmer Hard- und Software ausgelesen werden. Eine Analyse der Binärdaten ist anschließend möglich.

3.5 Schnittstellen und Protokolle

Für das Lesen und Ausleiten von Daten am laufenden System werden Schnittstellen bzw. Protokolle benötigt. Diese können in verschiedenen Formen vorliegen. Ein Gerät kann dabei eine, mehrere bzw. keine Schnittstelle aufweisen. Im Folgenden werden häufig vertretene Schnittstellen und Protokolle vorgestellt.

3.5.1 SSH

Bei dem Dienst SSH handelt es sich um einen sicheren Ende-zu-Ende-verschlüsselten Verbindungsaufbau zu einem entfernten Rechner. Die Kommunikation verläuft auf der Netzwerkprotokollebene. Dabei kann eine Verbindung textbasiert über die Kommandozeile oder mittels speziell entwickelter Softwarelösungen wie Putty, aufgebaut werden.

Für den Verbindungsaufbau ist eine Authentifizierung notwendig. SSH ermöglicht somit neben der Authentizität eine verschlüsselte Übertragung des Datenaustausches.

Bei Ausführung des Dienstes fungiert der Untersuchungs- bzw. zu verwendende PC als Client und der Router als Server. Die Verbindung wird in der Regel über Port 22 hergestellt. Nach Aufbau der Verbindung kann mit der Eingabe von Befehlen auf Dateien zugegriffen werden. Das Bearbeiten von Dateien und Ausführen von Programmen ist möglich. Verwendet wird SSH für den Datenverkehr, die Administration und Fernwartung sowie dem Erstellen von BackUps entfernter Geräte.

Die Bedienung von SSH unter Winwows 10 kann über die Kommandozeile wie folgt ausgeführt werden:
→ Powershell | Command Prompt (cmd):
→ SSH Benutzerkennung@IP_Adresse_des_Servers

3.5.2 Telnet

Bei der Verwendung des Dienstes Telnet handelt es sich um ein auf Transmission Control Protocol (TCP)-basiertes Netzwerkprotokoll. Mittels Remote-Zugriff kann über einen Client, dem zu bedienenden PC, mit dem anzusteuernden Gerät, dem Server, eine textbasierte bidirektionale Kommunikation

hergestellt werden. Die Eingabe des Benutzernamens, einschließlich des Passworts vom Server, ist notwendig. Die Verbindung wird in der Regel über Port 23 hergestellt. Eine virtuelle Fernsteuerung des entfernten Servers ist somit möglich.

Nach Aufbau der Verbindung kann mit der Eingabe von Befehlen auf Dateien zugegriffen werden. Das Bearbeiten von Dateien und Ausführen von Programmen ist möglich. Der gesamte Datenverkehr wird unverschlüsselt übertragen [14] [15].

Telnet kann über die Kommandozeile, aber auch über Softwarelösungen wie Putty, bedient werden. Mit dem Fortschreiten verschlüsselter Kommunikation findet Telnet immer weniger Verwendung.

Die Bedienung von Telnet unter Winwows 10 kann über die Kommandozeile wie folgt ausgeführt werden:
→ Systemsteuerung | Tastaturkombination [Windows Taste] + [X]
→ Apps und Features → Optionale Features → mehr Windows Funktionen
→ Telnet aktivieren → cmd → Telnet → o IP-Adresse → Nutzername → Passwort

3.5.3 UART

Bei einer Analyse der Leiterplatine auf vorhandene Schnittstellen kann das Vorkommen dieser von Gerät zu Gerät variieren. Eine UART Schnittstelle, welche eine serielle Verbindung mit dem Gerät zulässt, transferiert die digitalen Daten bitweise von einem Gerät zum anderen. Bei der Art des Zugangs handelt es sich um Kontaktierpunkte, welche in verschiedenen Formen vorgefunden werden können. So kann die Erscheinungsform als Lötpunkte, Through Hole (durch die Leiterplatine gehend) oder Surface Mount (mittels Pins auf der Leiterplatine) erscheinen. Die Erscheinungsform kann von Gerät zu Gerät auch unter der selben Herstellerreihe variieren.

Mittels der seriellen Schnittstelle UART werden Signale bidirektional (sowohl sendend als auch empfangend) im Full-Duplex, dem gleichzeitigen Senden und Empfangen von Daten, transferiert. Der Datentransfer erfolgt asynchron. Das bedeutet, dass das Taktsignal für die Datenübertragung vom Sender und Empfänger nicht geteilt wird. Durch die Einstellung der Datenübertragungsgeschwindigkeit, auch Baudrate genannt, kann eine Kommunikation zwischen dem Router und einem weiteren datenverarbeitenden Gerät umgesetzt werden [16].

3.5.3.1 Erscheinung und Einstellungen

Für die Bedienung der UART-Schnittstelle im forensischen Sinn wird ein USB zu UART Wandler benötigt. Dieser wird mit dem USB Anschluss an einem PC und mit den UART Verbindungsleitungen Receive Data (RX), Transmit Data (TX) und Erdung (GND) über Verbindungskabel, sogenannte Jumperkabel, auf dem Gerät an seinen Kontaktierpunkten verbunden. Die Jumperkabel vom USB zu UART Wandler müssen zum Gerät über Kreuz angelegt werden. Das bedeutet, dass RX und TX am USB zu UART Wandler auf dem Gerät in gekreuzter Weise belegt wird. Aus RX am zum untersuchenden Gerät wird TX auf dem USB zu UART Adapter und aus TX am zum untersuchenden Gerät wird RX auf dem USB zu UART Adapter.

Die Konfiguration der Datenpakete muss für beide Teilnehmer denselben Parametern entsprechen. Hierbei ist auf folgende Einstellung zu achten:

Konfiguration	Bedeutung
Start-Bit (Anzahl: 1)	Signalisierung des Beginns vom Datenframe
Datenbit (Anzahl: 5-9)	Übertragungsgröße der Daten
Paritätsbit (Anzahl: 1)	Fehlerbehebung, optional
Stop-Bit (Anzahl: 1-2)	Signalisierung des Endes vom Frame
Baudrate	gängig: 4800, 9600, 19.2K, 57.6K und 115.2K

Tabelle 3.1: UART Einstellungen

Als gängige Einstellung kann 1 Start-Bit, 8 Datenbits, kein Paritätsbit sowie 1 Stop-Bit gewählt werden [17]. Die Baudrate unterscheidet sich von Hersteller zu Hersteller und von Modell zu Modell. Ein Beispielbild kann der Anlage 'A UART Einstellungen - Putty Standardeingabe' entnommen werden.

3.5.3.2 Lokalisation der Kontaktierpunkte

Für das Lokalisieren der Kontaktierpunkte wird ein Multimeter verwendet. An diesem befinden sich zwei Messspitzen. Eine Messspitze fungiert als Erdungsspitze (Communication (COM)), die andere misst die Spannung (V).

Konfiguration	Bedeutung	Erläuterung
COM	GND	Erdungspunkt
V	Volt	Spannung
DC	Direct Current	Gleichspannung

Tabelle 3.2: Begriffe am Multimeter

3.5.3.3 Eingeschaltetes Gerät

Für die Lokalisation der Kontaktierpunkte am Gerät ist es von Nöten, dass das Gerät mit der Stromversorgung verbunden ist. Die Eingangsspannung des Netzteils, welches den Router mit Spannung versorgt, beträgt in der Regel 12 V. Am Multimeter werden die Einstellungen DC V 20 vorgenommen. Dabei stellen 20 V den nächsthöheren Messwert am Multimeter dar, welche größer 12 V ist.

Konfiguration	Messbereich (optional)	Erläuterung
DC	20 V	> 12 V Spannung

Tabelle 3.3: Lokalisation der Kontaktierpunkte mit Spannung am Gerät

Mit der Kontaktiernadel COM wird ein Erdungspunkt auf der Leiterplatine kontaktiert. Dieser kann in Form eines Massepunktes oder einer Antennenabschirmung vorliegen. Auf der Leiterplatine weisen die Spannungspunkte einen Wert von 3,3 V auf. Mit der Kontaktiernadel V werden die einzelnen UART-Kontaktierpunkte abgetastet. Als Ergebnis sollten die Werte wie in Tabelle '3.4 Messergebnis mit Spannung am Gerät 3,3 V' ermittelt werden.

Sollte der Spannungspunkt am Stromausgang des Netzteils gewählt werden, muss beachtet werden, dass an diesem Punkt eine Erdung für eine Spannung von 12 V vorgenommen wird. Der Tabelle '3.5 Messergebnis mit Spannung am Gerät 12 V' können die Werte entnommen werden, welche sich im folgenden Bereich befinden sollten.

Kontaktierpunkt	Bedeutung	Messergebnis
TX	Transmit Data (sendend)	2,5 V
RX	Receive Data (empfangend)	0 V
GND	Erdung	0 V
V	Spannung	3,3 V

Tabelle 3.4: Messergebnis mit Spannung am Gerät 3,3 V

Kontaktierpunkt	Messergebnis
TX	12 V - 3,3 V - 2,5 V = ca. 6,2 V
RX	12 V - 3,3 V - 0,0 V = ca. 8,7 V
GND	12 V - 3,3 V - 0,0 V = ca. 8,7 V
V	12 V - 3,3 V - 3,3 V = ca. 5,4 V

Tabelle 3.5: Messergebnis mit Spannung am Gerät 12 V

TX weißt einen Spannungswert auf, welcher durch die datentransferierende Funktion erklärt wird. Je nach Art der gesendeten Daten variiert der Wert zwischen wenigen Millivolt und Voltage at the common collector (VCC). In der Praxis liegt der Wert meist in der Nähe von 2,5 V. Zur Unterscheidung der Punkte GND und RX kann mittels Messung einer Durchgangsleitung durch Erzeugung eines akustischen Signals der GND Punkt ermittelt werden. Bei wechseln der Einstellungen auf dem Multimeter wird bei Anlegen der Messnadeln an der UART Schnittstelle der Leiterplatine an dem Punkt GND und einem beliebigen Erdungspunkt GND ein Piepton am Multimeter ausgegeben.

3.5.3.4 Ausgeschaltetes Gerät

Sollte das Gerät im ausgeschalteten Zustand vorliegen, kann für die Wertermittlung in den Bereich des Ohmchen Widerstandes gewechselt werden. Es bleibt anzumerken, dass im ausgeschalteten Zustand nur die Ermittlung des Erdungspunktes vorgenommen werden kann. Am Multimeter werden die Einstellungen Ohm 2 Kilo (K) oder weniger vorgenommen. Als Messergebnis sollte ein niedriger Wert nahe null ermittelt werden. Bei diesem handelt es sich um den Erdungspunkt GND. Da es sich bei dem Spannungspunkt VCC um einen digitalen DC/DC-Wandler handelt, sollte der Wert konstant sein und nicht schwanken.

3.5.4 USB

Bei einer USB-Schnittstelle wird die Verbindung zwischen zwei Geräten hergestellt. Hierbei können Daten bitweise übertragen werden. Die Datenübertragung erfolgt in einem Datenfluss. Bei diesem Datentransfer wird auch von einer seriellen Datenübertragung gesprochen. Weiterhin handelt es sich um eine Input / Output (I/O)-Schnittstelle, bei welcher die Daten in beide Richtungen sowohl gesendet als auch empfangen werden können.

Eine USB-Schnittstelle wird durch die Stromversorgung und der Übertragungsgeschwindigkeit gekennzeichnet. Letzteres wirkt sich auf die Dauer der Datenübertragung aus [18].

Im Bereich der Routergeräte werden USB-Schnittstellen für den Anschluss von USB-Datenträger verwendet. Diese fungieren als Speichermedium und beinhalten einen Flash Speicher. Bei dem Flash Speicher handelt es sich um ein elektronisches Speichermedium, in welchem sich im Gegensatz zu einem magnetischen Speicher, keine beweglichen Teile befinden.

Für Router wird in der Regel ein USB-Stecker des Typs A verwendet. Hier beträgt die Stromversorgung zwischen 100 Milliampere (mA) und 500 mA und die Übertragungsgeschwindigkeit befindet sich bei 480 Megabits per Second (Mbit/s) [19].

3.5.5 Ethernet

Bei der Schnittstelle Ethernet wird ein LAN-Kabel mit RJ45-Stecker verwendet. Dieses stellt die Verbindung von mindestens zwei Geräten her. Für die Geräte wird ein kabelgebundener Netzwerkzugang innerhalb eines lokalen geschlossenen Netzwerkes oder die Nutzung des Internets ermöglicht. Weiterhin wird eine Kommunikation bzw. ein Datenaustausch untereinander realisiert.

Bei dem zu verwendenden LAN-Kabel handelt es sich um ein Kupferkabel mit verdrillten Adernpaaren, welches als Twisted-Pair-Kabel benannt wird. Die Arbeitsweise wird im Full-Duplex realisiert. Das bedeutet, dass der Kanal zum Senden und Empfangen der Daten unabhängig voneinander genutzt wird.

Für die Datenübertragung mittels Ethernet wurde von der IEEE ein einheitlicher Standard definiert. Dieser regelt mittels des Protokolls IEEE 802.3 einheitlich die Weiterleitung der Daten. Die Datenübertragungsgeschwindigkeit kann sich bis auf 1.000 Mbit/s belaufen.

Bezugnehmend auf Punkt '2.3.4 OSI - Referenzmodell' findet Ethernet auf der Schicht 1 und 2 Anwendung. Dabei wird die Adressierung und die Zugriffskontrolle unterschiedlicher Übertragungsmedien umgesetzt [20] [21] [22].

3.5.6 Alternative Kommunikationswege - TFTP

Wird die Problematik erkannt, dass an einem Gerät keine USB-Schnittstelle zur Datenextraktion vorhanden ist, muss ein alternativer Lösungsweg gefunden werden. Ein alternativer Kommunikationsweg stellt hierbei das Protokoll 'TFTP' dar. Eine Datenübertragung kann unter Verwendung der Ethernet Schnittstelle oder der WLAN Verbindung durchgeführt werden. Mithilfe des folgenden Befehls und seiner aufgeführten Syntax kann ein Datentransfer auf einem Zielrechner realisiert werden:

```
tftp -l 'lokale_Datei' -p -r 'remote_Datei' 'IP_Remote_PC:Port'
```

Definition Befehl	Bedeutung
TFTP	Protokoll TFTP
-l	lokale Datei
-p	put - kopiere Datei
-r	remote - benenne Datei mit
IP_Remote_PC:Port	IP-Adresse des sichernden PCs mit Portangabe

Tabelle 3.6: Alternativer Kommunikationsweg - TFTP

Die Datenübertragung erfolgt im Octet Mode als 8-bit Strom im Binärformat. Eine Konvertierung in ein anderes Format ist ausgeschlossen. Die Natur der Daten bleibt erhalten. Die Integrität der Daten wird gewährleistet.

Es bleibt zu beachten, dass mit dem Verbinden des Zielrechners zwangsläufig Daten auf dem untersuchten Gerät in Form von der Geräteerfassung verändert werden. Dies gilt für einen lückenlosen Nachweis zu protokollieren.

4 Analysegeräte

Die zu anvisierenden Untersuchungen sollen Beispielhaft an bewusst gewählten Geräten durchgeführt werden. Um die für diese Analyse zu differenzierenden Geräte zu kristallisieren, werden vorerst Recherchen und Untersuchungen durchgeführt. Anschließend kann zu den betreffenden Geräten eine Wahl getroffen werden.

4.1 Marktrecherche

Zum Differenzieren der zu untersuchenden Geräte wurde die Recherche auf mehrere Punkte gelegt. Zum einen wurde ein Überblick über verfügbare Statistiken geschaffen, zum anderen wurden mittels einer Softwarelösung lokal die in unmittelbarer Umgebung befindlichen Geräte analysiert. Die finale Entscheidung der gewählten Geräte umfasst ein Zusammenspiel der Statistiken, der Auswertung der aus der Umgebung mitgeschnittenen Geräte und der Geräte, welche überwiegend im strafrechtlichen Kontext vertreten sind.

4.1.1 Internetrecherche

Mithilfe der Internetrecherche soll ein Überblick über verschiedene Marktvorkommen geschaffen werden. So wird, neben dem lokalen, auch das globale Vorkommen auf statistischen Ebenen betrachtet.

4.1.1.1 Statista

Den veröffentlichten Statistiken des Unternehmens 'Statista' können vielerlei wissenschaftliche Daten zu statistischen Inhalten entnommen werden. Für einen Eindruck auf den derzeitigen Marktanteil konnte mit der Recherche 'Marktanteile von Router-Herstellern an den Verkäufen auf Amazon.com im 1. Quartal 2015' entnommen werden, dass die Hersteller 'TP-Link' zu 28%, 'Asus' zu 24% und 'Netgear' zu 23% am häufigsten vertreten sind. Hervorstechend wirkt die annähernd gleiche Marktpräsenz [23].

4.1.1.2 Amazon

Unter Verweis auf die Bestseller der Internetverkaufsplattform 'Amazon.de' können unter der Kategorie 'Computer und Zubehör → Netzwerk → Wireless Access Points' als Vorreiter das Unternehmen 'TP-Link' [24] und unter der Kategorie 'Computer und Zubehör → Netzwerk → Router' als Vorreiter das Unternehmen 'AVM' mit ihren Modellen der Fritz!Box-Reihe entnommen werden. Als weitere Vertreter unter den Beststellern folgen Geräte der Netzbetreiber Telekom und des Unternehmens 'TP-Link', wobei das Unternehmen 'TP-Link' mit dem Unternehmen 'AVM' in enger Konkurrenz zueinander steht.

Als Vertreter des Unternehmens 'TP-Link' wird unter anderem das Modell 'TP-Link Archer C6 Dualband Gigabit WLAN-Router (867 Mbit/s 5 GHz + 300 Mbit/s 2,4 GHz, 4 Gigabit LAN-Port, Multiuser Multiple Input, Multiple Output (MU-MIMO), IPTV, Unterstützt keine DSL-Funktion' [25] an 16. Position

der Bestsellerliste geführt. Vorherige Modelle beinhalten ein LTE-Modem, fungieren als Nano-Router oder erweisen sich als ältere Modelle [25]. Dabei handelt es sich bei Nano-Routern um Geräte, welche durch ihre Eigenschaft als tragbare Zwischenknoten fungieren.

Einen Bezug zu dem Zeitraum, in welcher aufgezeigte Geräte statistisch erfasst worden sind, konnten der Homepage nicht entnommen werden.

4.1.1.3 TP-Link

Dem Internetauftritt des Unternehmens TP-Link kann dem Konzernprofil entnommen werden, dass es sich bei diesem um einen weltweit führenden Hersteller handelt, welcher für den Verkauf von Smart-Home- und Netzwerkinfrastruktur-Produkten wirbt. Zum Stand 2021 sollen bereits 1,2 Milliarden Verbraucher aus über 170 Ländern ein Produkt des Unternehmens in Anspruch genommen haben [26].

Das International Data Corporation (IDC) Worldwide Quarterly Wireless LAN Tracker benennt, dass TP-Link im 4. Quartal 2020 18 Millionen WLAN-Produkte ausgeliefert hat. Damit habe TP-Link einen weltweiten Marktanteil von 17,8%. IDC tritt in seiner Funktion als Markforschungs- und Beratungsunternehmen auf. TP-Link benennt weiter, dass von der IDC das Unternehmen TP-Link im 4. Quartal des Jahres 2022 zum zwölften Mal in Folge als Nummer 1 unter den weltweiten Anbietern von WLAN-Geräten geführt werden konnte [27].

Mit seinen WLAN-Produkten führe das Unternehmen in den Bereichen Wi-Fi 5 bis Wi-Fi 6 die vergangenen Jahre konsequent die Marktführerschaft. Die Ergebnisse beziehen sich auf weltweite Sendungen.

4.1.1.4 Breitbandinternet

Analysierend auf die deutschen großen Breitbandinternetanbieter stehen die Unternehmen Telekom, Vodafone, 1&1 und O2 als Vorreiter von Internetdiensten bereit. Dabei lässt sich ein steigender Trend bei Kabelroutern erkennen [28]. Aus der Marktanalyse geht hervor, dass der Bedarf an Kabelroutern steigt, gleichsam weist der Markt an DSL-Routern einen absteigenden Trend auf. Als Vorreiter von Breitbandinternetanbietern rangieren die Unternehmen Vodafone und Telekom annähernd auf gleicher Ebene [29].

4.1.2 WiGLE

Zur Verifizierung der meistverwendeten Modelle wurde eine örtlich und zeitlich begrenzte WLAN-Analyse durchgeführt. Bei dieser Untersuchung werden mittels einer Softwareapplikation Signale und Datenpakete aus der unmittelbaren Umgebung aufgezeichnet und in einer Datenbank abgelegt. Hierzu wird sich der Datenpakete, welche von WLAN-Routern versandt werden, bedient. Die Datenpakete, auch als Beacons bezeichnet, werden durch ein zuvor eingestelltes Intervall an die Broadcastadresse versendet. Somit erhalten alle Geräte in unmittelbarer Umgebung ein Datenpaket und können dieses verarbeiten. Der Versand der Beacons erfolgt in der Regel alle 30 Sekunden. An dieser Stelle sei nochmals auf den Punkt ’2.1.2 Kommunikationspartner und Kommunikationsverlauf’ verwiesen.

4.1.2.1 Datensammlung

Als Softwarelösung wurde die Applikation 'WiGLE' gewählt. Bei diesem Tool handelt es sich um ein kostenfreies Produkt, welches ohne Registrierung eines Benutzerkontos bedient werden kann. Ursprünglich wurde diese Art der WLAN-Analyse zur Detektion nicht verschlüsselter WLAN-Bereiche genutzt. Ziel war die Nutzung unentgeltlicher Bandbreite. Durch die immer populärer werdende und sich weit verbreitende Verschlüsselungstechnologie wird der ursprüngliche Gedanke verdrängt. Das detektieren der Umgebung eignet sich mit dieser Variante weiterhin gut zum Erstellen einer Übersicht der WLAN-Umgebung. Aufgezeichnet werden die MAC-Adressen, die SSID sowie die verwendete Verschlüsselungsmethode der Geräte. Des weiteren wird eine Bluetooth-Erkennung, Notation von Sendeleistung und der GPS-Daten geführt.

Die gesammelten Daten können in Form von Keyhole Markup Language (KML)- oder Comma-separated values (CSV)-Dateien heruntergeladen und eingesehen werden. Weiter werden die global gesammelten Daten aller Softwarenutzer auf ein von der Homepage geführtem Kartenmaterial grafisch dargestellt und können von den Nutzern online eingesehen werden.

Das für diese Untersuchung durchgeführte Aufzeichnen von WLAN-Signalen der unmittelbaren Umgebung beschränkte sich auf kleine lokale Bereiche innerhalb der Bundesrepublik Deutschland. Diese umfassen die Umgebung München, Erfurt, den südländischen Raum des Bundeslandes Thüringen, Wiesbaden und Freiburg im Breisgau. Die Aufzeichnung wurde je Aufzeichnungsort über eine Dauer von drei Tagen durchgeführt.

4.1.2.2 Auswertung

Der gesammelte Datenbestand wurde in ein Tabellenkalkulationsprogramm geladen und tabellarisch aufgezeigt. Es wurden die relevanten Reiter 'MAC', 'SSID', 'Authentifizierungs Modus (AuthMode)' und 'Type' zur Ansicht gewählt. Für den Reiter 'Type' wurde der Typ auf WLAN beschränkt. Nach aufsteigender Sortierung der MAC-Adressen und filtern der Duplikate, wurden mittels der Softwarelösung 'MACAdressView' die MAC-Adressen nach seinen Hersteller aufgelöst. Anschließend erfolgte die Zählung der Hersteller. Mit diesen Parametern wurde anschließend ein Ranking der Hersteller durchgeführt und die für den Analysezeitpunkt meistvertretenen Hersteller von Routern ermittelt. Das Ergebnis wird im Anhang 'B Marktrecherche: 'WiGLE" aufgezeigt.

Mit dem anschließend durchgeführten Ranking der Hersteller konnte festgestellt werden, dass eine Auflistung namhafter Breitbandinternetanbieter nicht geführt wird. Durch die Beauftragung der Provider zur Herstellung der Router an Unternehmen, werden entsprechend deren Unternehmensbezeichnung bei der Zuweisung der MAC-Adresse vergeben.

Datenbank WiGLE	Werte
Gesamtanzahl Geräte	22.913
Mit Filter 'Wi-Fi'	10.388
Entfernen der Duplikate	5.254
Anzahl Hersteller	86

Tabelle 4.1: Auswertung Datensammlung: Wigle

4.1.3 Zu analysierende Geräte

Unter Bezug auf die Ergebnisse der durchgeführten Statistiken, in Verbindung mit in strafrechtlichem Kontext vorgefundenen WLAN-Routern, wurden folgende Geräte gewählt:

1. Vodafone Station Arris TG3442DE
2. TP-Link AC1200 Mesh Wi-Fi Router

Modelle des Unternehmens TP-Link stellen die global am meisten vertriebenen Routergeräte dar. Aufgrund des Ergebnisses des lokal durchgeführten Mitschneidens der räumlichen Umgebung über die Softwarelösung WiGLE mit einem Gerätevorkommen in Höhe von 86 Vertretern und dem Vorkommen in strafrechtlich relevanten Sachverhalten, wurde als Referenzmodell ein Router des Unternehmens TP-Link gewählt.

Für Modelle des Unternehmens Vodafone werden folgend geführte Hersteller mit der Produktion von Basisgeräten beauftragt. Die anschließende Anzahl an Geräten stellen die im Aufzeichnungszeitraum ermittelten Router dar.

Hersteller	WiGLE: Anzahl
Arris	54
Compal	74
Sagemcom	9
Technicolor	57

Tabelle 4.2: Hersteller Vodafone-Router

Hierbei konnten bei dem lokal durchgeführten Mitschneiden der räumlichen Umgebung Geräte aller benannten Hersteller ermittelt werden. In Bezug zu strafrechtlich relevanten Sachverhalten konnten Geräte der Hersteller Arris vermehrt notiert werden.

Bevor mit der eigentlichen Untersuchung und der Ermittlung potentieller Datenextraktionsmöglichkeiten begonnen werden kann, wurde unter Laborbedingungen ein Netzwerk mit dem gewählten Router erstellt. Hierzu wurde das Netzwerk über einen Zeitraum von sieben Tagen im Normalbetrieb verwendet. Der hierauf erzeugte Datenstrom soll für die weiterführende forensische Analyse untersucht und extrahiert werden.

4.2 Vodafone Station Arris TG3442DE

Aus der Kombination der Ergebnisse von Statista, den Ergebnissen der mitgeschnittenen lokal begrenzten Örtlichkeiten mit WiGLE und dem Vorkommen an WLAN-Routern, welche im strafrechtlichen Kontext vorgefunden werden konnten, wurde für die anschließende Analyse ein WLAN-Router des Unternehmens 'Arris' gewählt. Bei dem Modell handelt es sich um das Gerät 'TG3442DE'. In diesem Router ist wie unter Punkt '2.2.1 Übertragungsweg: Kabel' beschrieben ein Modem für die Verwendung im Kabelfernsehnetz verbaut. Zur Kommunikation mit dem Internetprovider muss folglich kein extra Modem vorgesetzt werden. Weiter ist das gewählte Modell Mesh-fähig und fungiert als analoges Telefon-Gateway [30]. Die besonderen Eigenschaften der Mesh-Funktion sind unter Punkt '2.4.3 Mesh-System' benannt.

Das Unternehmen 'Arris' ist ein global agierender Hersteller für Kabelnetzgeräte, Ausrüster für Modems und Set-Top-Boxen. Im Jahr 2018 wurde das Unternehmen von 'Commscope' übernommen. Zusammen hält das Unternehmen weltweit eine führende Position im Bereich der Kabelnetzbetreiber inne [31].

In dem Analysegerät 'Vodafone Station Arris TG3442DE' ist eine Leiterplatine mit der Bezeichnung TG3442 (S/CE) verbaut. Die gewählte Variante wird durch den deutschen Anbieter Vodafone Kabel vertrieben. Die FCC Zulassung hierzu ist seit dem 13. Juli 2020 vorhanden [32].

Abbildung 4.1: Vodafone Station Arris TG3442DE- Vorderseite und Rückseite

Bei dem zu untersuchenden Gerät handelt es sich um eine Neuanschaffung. Daten wurden auf diesem zuvor nicht geschrieben. Eine Datenmanipulation kann zum Analysebeginn ausgeschlossen werden. Das Gerät ist an den Provider gebunden und kann erst nach dessen Freischaltung für den Internetzugang verwendet werden.

Zur Einrichtung des WLAN-Routers wird die grafische Benutzeroberfläche aufgerufen. Dies kann in Form der Default Gateway IP-Adresse '192.168.0.1' oder des Domainnamens 'kabelbox.local' erfolgen. Das für die Anmeldung an der grafischen Benutzeroberfläche benötigte voreingestellte Passwort ist auf einem Aufkleber notiert. Dieser ist auf der Rückseite des Gerätes angebracht. Ein Standard-Kennwort wird nicht vergeben. Mit dem erstmaligen Aufruf wird der Benutzer zum Ändern des voreingestellten Passwortes aufgefordert. Eine Umsetzung wird nicht erzwungen.

Nach der durchgeführten Einrichtung erfolgte noch vor der ersten Nutzung durch Endgeräte das Freilegen der Leiterplatine. Bei dem Gehäuse handelt es sich um zwei mit 22 Haltenasen und drei Schrauben befestigte Gehäuseteile. Zwei Schrauben sind auf der Rückseite des Gehäuses klar erkennbar. Eine Schraube befindet sich an der seitlichen Verkleidung unter einem Klebesiegel, welches als Garantiesiegel fungiert. Die Haltenasen sind schwer unbeschädigt zu öffnen. Für das Öffnen des Gerätes muss die Stromversorgung nicht unterbrochen werden. Da sich das Öffnen der Haltenasen als schwerfällig darstellt, ist im Bereich der Stromversorgung mit äußerster Vorsicht zu arbeiten. An der Leiterplatine des WLAN-Routers sind weder äußere noch innere Antennen erkennbar.

4.2.1 Technische Eigenschaften

Im Folgenden wird eine Reihe an technischen Eigenschaften aufgeführt, welche das Gerät genauer an seinen Funktionalitäten beschreibt. Zu der Benennung erfolgen die inneren Eigenschaften sowie äußeren Eigenschaften. Äußerlich erkennbar ist das Gerät mit 5x light-emitting diode, dt. Leuchtdiode (LED)s, 4x 1 Gigabit-Ethernet (GbE)-LAN Ethernet-Ports, 1x USB-Anschluss 3.1 (Gen1), 2x VoIP-Ports [30] sowie mit einer Eingangsspannung von 12 Volt Direct Current (VDC) und 2,5 Ampere | Stromstärke (A). Auf der Leiterplatine können diverse Module, wie der RAM, Wi-Fi Protected Setup (WPS)- und Wide Area Network (WAN)-Komponenten, erkannt werden. Diese werden im Folgenden tabellarisch zusammengefasst:

Ausstattung	Beschreibung
Board-ID	ARCT04789
LED	5x LEDs: Betrieb, WLAN, WPS, Internet, Telefon
CPU (SoC)	Intel Puma FHCE2752M 2,5 GHz 2 Kerne
NAND Flash	Toshiba TC58NVG2S0HBAI4, 512 MiB
RAM	Micron FBGA Code: D9SHD Part Number: MT41K256M16TW-107:P, 2x 4GB, DDR3-1866
NAND-Controller eMMC 4.5	Phison PS8211-0
Radio	2,4 GHz, 1200 Mbit/s (802.11 b/g/n) Celeno CL2432 (MU-MIMO Status 3x3) 5 GHz, 4800 Mbit/s (802.11 a/n/ac) Celeno CL2440 (MU-MIMO Status 4x4)
Schalter	1x An/Aus-Schalter, 1x WPS, 1x WLAN

Tabelle 4.3: Vodafone Station Arris TG3442DE - Technische Eigenschaften [33] [30] [34] [32]

Eine implementierte Eigenschaft ist das Band Steering. Mit der Option Band Steering wird die Dualband-Eigenschaft unterstützt. Dabei können zwei Frequenzbänder gleichzeitig abgedeckt werden. Der Router kann die optimale Frequenz auf das Endgerät zuweisen und somit eine optimale Integration von Geräten in das WLAN erzeugen. Die kabelgebundene Datenübertragungsrate beläuft sich im Gigabit Bereich und unterstützt damit besonders hohe Geschwindigkeiten. Durch die

MU-MIMO Eigenschaft können zudem bis zu zwei mal schnellere Verbindungen realisiert werden. Genauer beschrieben ist eine Kommunikation mit zwei Endgeräten zur selben Zeit möglich. Ein Überschneiden der Bandbreite wird damit ausgeschlossen. Schnittstellen wie Serial ATA (SATA), Video oder Audio sind nicht implementiert.

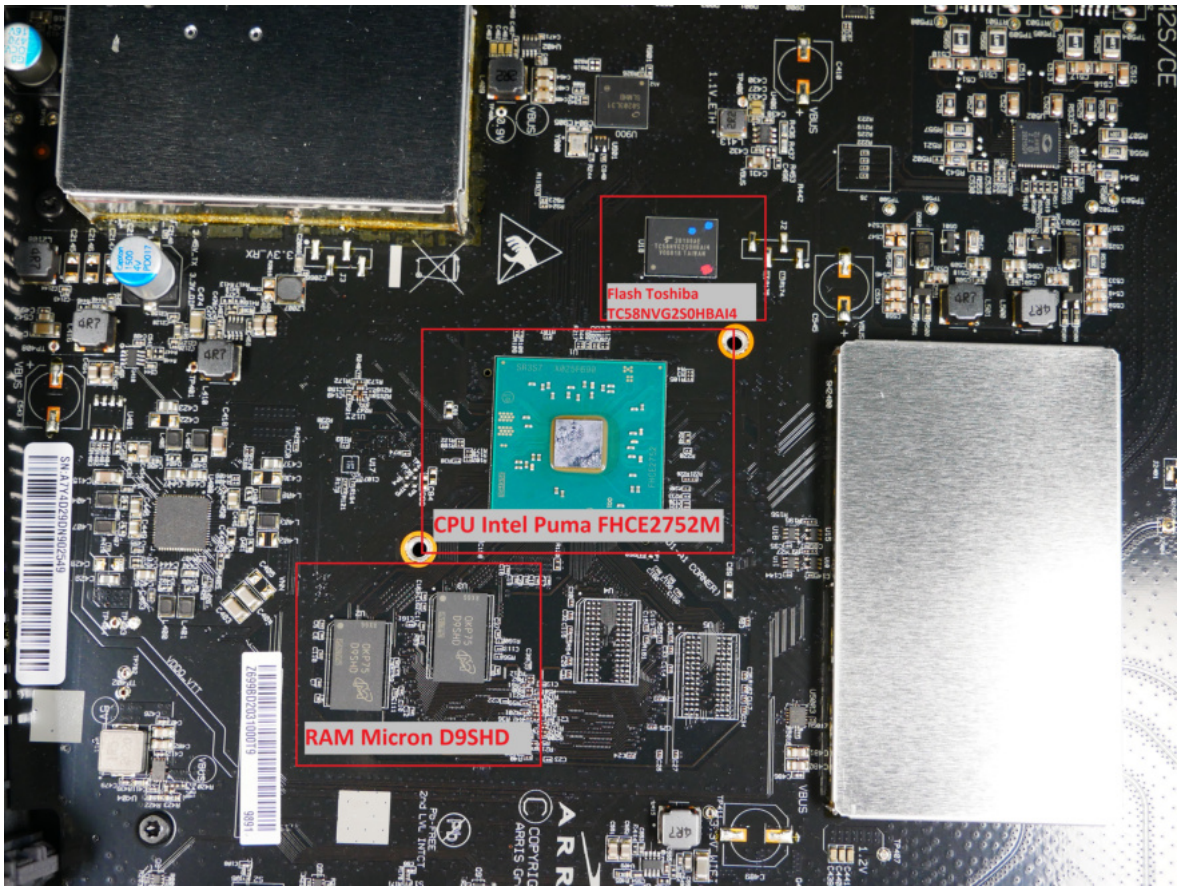

Abbildung 4.2: Vodafone Station Arris TG3442DE - Leiterplatine

4.2.2 Grafische Benutzeroberfläche

Wie unter Punkt '4.2 Vodafone Station Arris TG3442DE' benannt, erfolgt zunächst die Anmeldung auf der grafischen Benutzeroberfläche. Tabellarisch betrachtet kann in dem oberen rechten Bereich die Wahlmöglichkeit zwischen den Reitern 'Standard-Modus' und 'Experten Modus' gewählt werden. Zu Beginn wird der 'Standard-Modus' dargestellt. Für forensische Untersuchungen empfiehlt es sich, in den 'Experten Modus' zu navigieren.

Zur Auswahl stehen in der Reihenansicht nun die folgenden Reiter 'Übersicht', 'Telefon', 'Internet', 'WLAN', 'Einstellungen', sowie 'Status & Hilfe'. Die Spaltenauswahl der linken Ansicht ändert sich je nach gewähltem Reiter der Reihenansicht. Auf der Hauptseite kann unter dem Reiter 'Übersicht' ein erster Überblick über die wichtigsten Informationen gesammelt werden. Auf dieser Seite werden Daten zu den momentan mit dem Router verbundenen Geräten erfasst. Es werden Daten zu den Geräten im WLAN, LAN und der Telefonanschlüsse visuell dargestellt. Die drei benannten Felder bieten weitere Datenbereiche. Mit dem Anklicken eines Gerätes werden Informationen zur SSID, der IPv4 bzw. IPv6 Adresse, der MAC-Adresse, dem WLAN und der Link rate dargestellt. Zeitstempel für den Beginn der aktiven Verbindung werden nicht angezeigt.

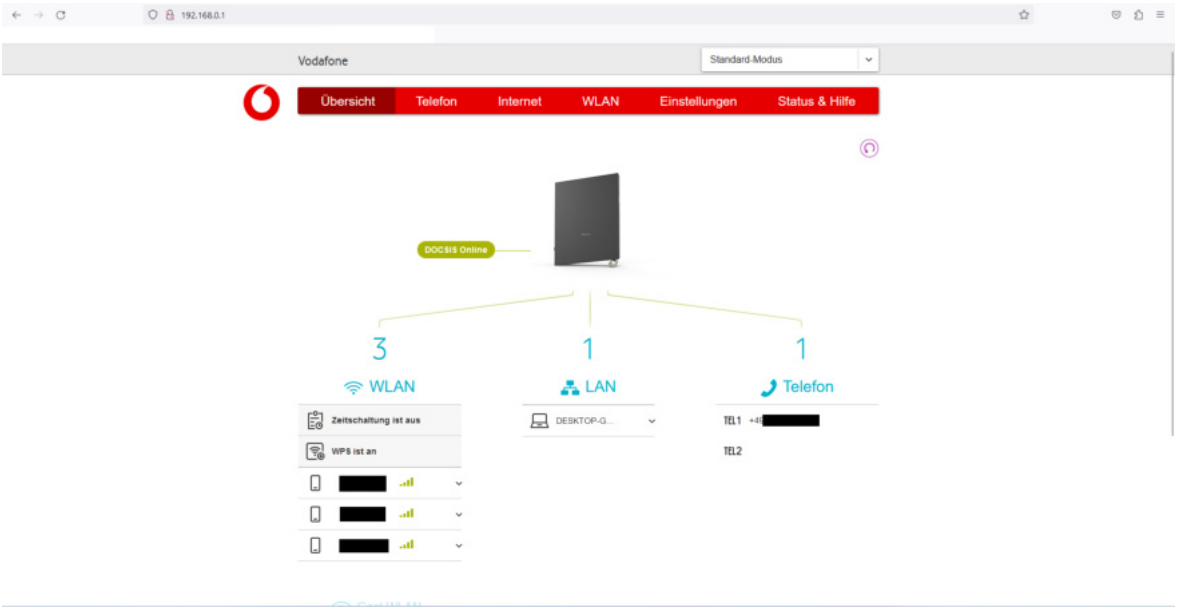

Abbildung 4.3: Vodafone Station Arris TG3442DE - Grafische Benutzeroberfläche

Für die Untersuchung der flüchtigen und persistenten Datenbasis werden Datensicherungen von der Erstinbetriebnahme, einer Laufzeit von 8 Tagen sowie der Datenansicht nach Entfernen der Stromzufuhr vorgenommen und miteinander verglichen. Hierzu können nachfolgende Erkenntnisse aus der Ansicht der grafischen Benutzeroberfläche gewonnen werden:

4.2.2.1 Flüchtige Datenbasis

Für die Navigation wird der 'Experten Modus' gewählt. Anhand folgender Punkte kann eine flüchtige Datenbasis ermittelt werden:

1. Unter dem Punkt
   Telefon → Anrufliste → Telefon-Einstellungen
   kann die Historie eingehender und ausgehender Telefonate eingesehen werden. Informationen wie Datum, Uhrzeit, Rufnummer und Dauer lassen einen Überblick dazu gewinnen, wann welche Rufnummer gewählt, empfangen oder verpasst wurde.
2. Unter dem Punkt
   Einstellungen → WAN
   können Informationen zur IP- und MAC-Adresse sowie der Laufzeitdauer des Routers entnommen werden. Die Laufzeitdauer bezieht sich auf den Betrieb des Gerätes seit der letzten Stromunterbrechung. Für die Testzeit der Analyse kann die Betriebszeit des Gerätes an diesem Punkt nachvollzogen werden.
3. Unter dem Punkt
   Status & Hilfe → Status
   wird ein zweites Zeitfenster der Laufzeitdauer dargestellt. Dieses wird ebenfalls mit der Dauer seit dem letzten Neustart geführt. Es folgt eine Anzeige des aktuellen Zeitstempels mit Datum und Uhrzeit.

4. Unter dem Punkt

Status & Hilfe → Status → LAN Status

   kann eine tabellarische Übersicht der Geräte aus der DHCP Geräteliste eingesehen werden. Es werden Informationen zu den Geräten in Form der SSID, der MAC-Adresse, IP-Adresse, der Art der Verbindung (DHCP) sowie dem Status (inaktiv / aktiv) des Teilnehmers dargestellt. Zeiten zu Log-in bzw. Log-out Daten von Geräten werden nicht geführt. Die Auflistung erlischt mit dem Entzug der Stromversorgung.
5. Unter dem Punkt

Status & Hilfe → Ereignisprotokoll

   kann eine Auflistung zu Logeinträgen entnommen werden. Das Ereignisprotokoll kann als Logdatei gedownloadet werden. Die Logeinträge werden mit den Reitern 'Datum, Uhrzeit, [info], Kategorie (WLAN), Ereignis' geführt.
   Aus dem gesicherten Datenbestand des Ereignisprotokolls können die von dem Router an die Endgeräte zugewiesenen IP-Adressen erkannt werden. Ein Zeitstempel wird angegeben. Die Anzeige des Zeitstempels erfolgt in der mitteleuropäischen Sommerzeit. Ein nachträgliches Anpassen der Zeitrechnung muss nicht vorgenommen werden. Die Zeit für das Einloggen eines Gerätes auf dem Router kann dem Ereignisprotokoll entnommen werden.

Eine erste Sicherung zum Datenbestand des Ereignisprotokolls ist nach acht Tagen Aufzeichnungszeitraum erfolgt. Die Sichtung dessen ergab ein gesichertes Datenvorkommen von 4,5 Stunden, zurückgerechnet ab dem Abfragezeitpunkt. Die Dateigröße beträgt 16 Kilobyte (kB). Für eine bessere Bewertung des Ereignisprotokolls wurden anschließend vier weitere Datensicherungen in einem Zeitraum von sieben Tagen durchgeführt. Die gesicherten Ereignisprotokolle der 3. und 4. Datensicherung, beginnend mit dem Analysezeitpunkt, weisen eine Überschneidung der Ereigniseinträge auf. Alle weiteren Ereignisprotokolle lassen einen Bezug zur Speicherdauer nicht erkennen. Mit der vierten Datensicherung kann ermittelt werden, dass es sich bei der Datenablage zu diesem Modell um einen Ringspeicher handelt. In der Datenablage werden die ältesten Einträge zuerst überschrieben. Eine definierte Dateigröße kann nicht erkannt werden. Die Dateigrößen aller gesicherter Ereignissprotokolle befinden sich zwischen 12 kB und 23 kB. Die durchschnittliche Dateigröße beträgt 15 kB. Bei der Protokollierung des zeitlichen Rahmens sind gesicherte Datenbestände zwischen 00:24 Stunden und 12:17 Stunden vorhanden. Eine Syntax zur Aufzeichnung der Daten kann nicht erkannt werden. Eine detaillierte Auflistung der einzelnen Ereignisprotokollsicherungen ist in dem Anhang 'C Vodafone Station Arris TG3442DE - Analyse Ereignisprotokoll' einsehbar.

Zu beachten ist, dass das Analysemodell aufgrund eines Darstellungsfehlers die zwischen dem Reiter 'Einstellungen → WAN' und dem Reiter 'Status & Hilfe → Status' befindlichen Zeitangaben jeweils um eine Stelle versetzt sind. Daraus ergibt sich, dass die Tage bei Stunden und die Stunden bei Minuten abzulesen sind. Ob diese Erkenntnis auf andere Versionen der Herstellerreihe zutreffen ist nicht bekannt.

In der 3. Datensicherung zu Anhang 'C Tabelle C.1 Vodafone Station Arris TG3442DE - Analyse Ereignisprotokoll' kann ermittelt werden, dass ein Verlust der Stromzufuhr mit dem nächsten Neustart zu Verlust von bestehender Datenbasis führt. Dies beruht auf den neu geladenen Konfigurationsabläufen. Diese werden teilweise im Ereignisprotokoll verzeichnet. Dabei kann es sich um Inhalte wie

Configuration Changed : Set Device.WiFi.AccessPoint.2.X_CISCO_COM_KickAssocDevices to true from CLIENTTOOL,old value is : false,result: Set successfully.

oder

Configuration Changed : Set Device.WiFi.AccessPoint.1.X_CISCO_COM_KickAssocDevices to true from CLIENTTOOL,old value is : false,result: Set successfully.

handeln. Eine bildliche Darstellung kann folgender Grafik entnommen werden:

Abbildung 4.4: Vodafone Station Arris TG3442DE - Ereignisprotokoll Stromverlust → Verlust von Datenbasis

Der Inhalt eines Verbindungsaufbaus eines Gerätes mit dem Router wird im Ereignisprotokoll unter folgendem Aufbau abgelegt:

Datum	Uhrzeit	[Info WLAN] — [Warnung Firewall]	MAC Teilnehmer	Authentifizierung verbinden mit	SSID Router	MAC Router	Interface

Tabelle 4.4: Vodafone Station Arris TG3442DE - Syntax Verbindungsaufbau Teilnehmer - Router

Für den Aufbau einer Verbindung authentifiziert sich der Teilnehmer mit seiner MAC-Adresse bei dem Router. Für die Kommunikation wählt der Teilnehmer die MAC-Adresse des Routers, dessen SSID und das zu verwendende Interface. Mit der erfolgreichen Authentifizierung wird das Verbinden des Teilnehmers unter Verwendung der mitgeteilten MAC-Adresse und der SSID mit dem Router realisiert.

Es folgt ein Paket mit allen ausgehandelten Inhalten. Dabei werden die MAC-Adresse des Routers im Folgenden unter der Bezeichnung 'WG-MAC' und die des Teilnehmers unter 'STA-MAC' geführt. Es folgt das verwendete Interface, die SSID des Routers, der Verbindungsstatus (verbunden, nicht verbunden) sowie der WLAN Modus über dem verwendeten Standard. Hier sei auf das Kapitel '2.3.3 IEEE 802.11 - Standard' verwiesen. Daten zu Geschwindigkeitsraten, der verwendeten Verschlüsselungsmethode, dem Authentifizierungsmodus sowie Daten zu dem Frequenzband folgen abschließend in dem Datenpaket.

Bei einem Verbindungsabbruch erfolgt die Meldung:

DEAUTH - MAC=XX:XX:XX:XX:XX:XX, Reason=1; WG-MAC=XX:XX:XX:XX:XX:XX; IF=wlan1_0 DISASSOC-MAC=XX:XX:XX:XX:XX:XX, Reason=34; WG-MAC=XX:XX:XX:XX:XX:XX;IF=wlan1_-0

Zusammenfassend besteht ein Verbindungsaufbau und Verbindungsabbau aus den Ereignissen 'authentication', 'associated', 'ConnectionState', 'REASON-CODE-DESCR', 'DEAUTH' und 'DISASSOC'.

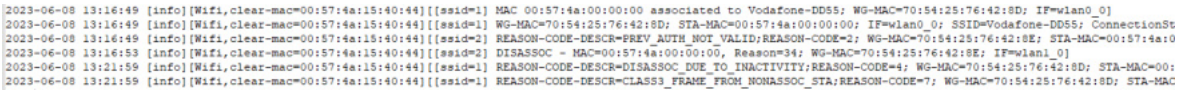

Abbildung 4.5: Vodafone Station Arris TG3442DE - An und Abmeldung Client

Dem Ereignisprotokoll können eine Vielzahl an Wechsel der Datenübertragungsrate IEEE 802.11 n und dem IEEE 802.11 ac sowie dem Frequenzband 2,4 GHz oder 5 GHz einzelner Geräte entnommen werden. Möglich ist, dass die Position des Gerätes sich an der Grenze der Reichweite zum derzeitigen Frequenzband befindet oder dieses durch andere Störquellen wie unter Punkt '2.3.5 Sendeleistung und Reichweite WLAN' benannt, den momentanen Verbindungen anpasst.

4.2.2.2 Persistente Datenbasis

Als persistente Datenbasis können sämtliche Konfigurationsdaten erkannt werden. Das betrifft für diesen Router alle Daten bis auf die im Punkt '4.2.2.1 Flüchtige Datenbasis' benannten. Auf der grafischen Benutzeroberfläche stellen Daten mit Bezug zu Geräten durchweg flüchtige Daten dar.

4.2.3 SSH

Für die Überprüfung des Dienstes SSH erfolgt mittels Portscans eine Durchsicht auf offene Ports.

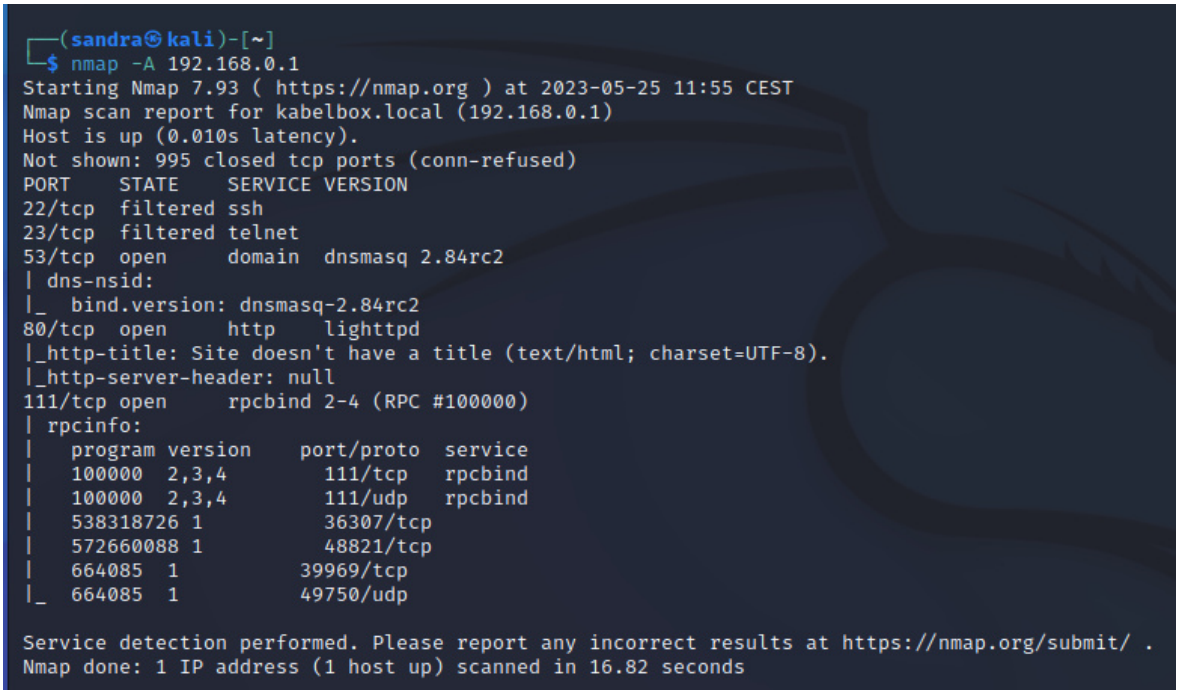

Abbildung 4.6: Vodafone Station Arris TG3442DE - Portscan

Für den Dienst SSH kann bei der Überprüfung des Dienstes ein gefilteter offener Port festgestellt werden. Der Dienst ist auf diesem Router gefiltert freigegeben. Es besteht die Annahme, dass dieser ansprechbar sein könnte. Ein Zugriff zu diesem Dienst konnte nicht hergestellt werden. Bei Ansprechen des Dienstes unter dem entsprechenden Port wird die Fehlermeldung 'ssh: connect to host 192.168.0.1 port 22: Connection time out' ausgegeben.

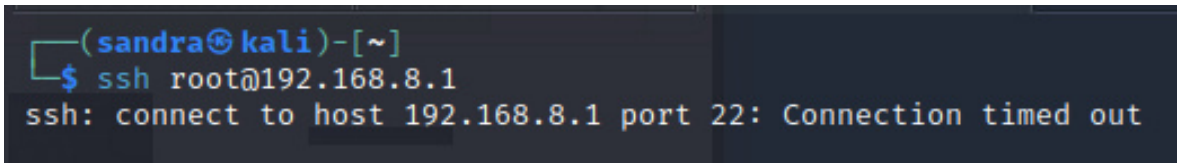

Abbildung 4.7: Vodafone Station Arris TG3442DE - SSH

4.2.4 Telnet

Für die Überprüfung des Dienstes Telnet erfolgt mittels Portscans eine Durchsicht auf offene Ports. Für den Dienst Telnet kann bei der Überprüfung des Dienstes ein gefilteter offener Port festgestellt werden. Es besteht die Annahme das dieser ansprechbar sein könnte. Ein Zugriff zu diesem Dienst konnte nicht hergestellt werden. Bei Ansprechen des Dienstes unter dem entsprechenden Port wird die Fehlermeldung 'telnet: Unable to connect to remote host: Die Wartezeit der Verbindung ist abgelaufen' ausgegeben.

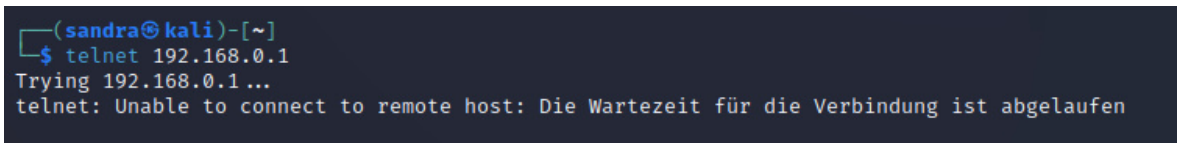

Abbildung 4.8: Vodafone Station Arris TG3442DE - Telnet

4.2.5 UART

Nach dem Entfernen des Gehäuses und der ersten Durchsicht der Leiterplatine kann offensichtlich keine UART-Schnittstelle lokalisiert werden. Daraufhin erfolgte die Recherche, in welchen WLAN-Routern dieselbe Leiterplatine Verwendung gefunden hat. Ebenso erfolgte eine Recherche, ob zu dem Prozessor die Funktion der UART-Schnittstelle vorhanden ist.

4.2.5.1 Andere Modelle mit derselben Leiterplatine - ARCT04789

Auf dem WLAN-Router Arris TG3452 kann eine bauähnliche Leiterplatine erkannt werden [35].

4.2.5.2 Andere Modelle mit dem selben Prozessor - Intel Puma FHCE2752M

Durch erfolgte Internetrecherche kann entnommen werden, dass es sich bei dem Prozessor um eine Sonderbestellung ab Werk handelt [36]. Ein Datenblatt wird nicht zur Verfügung gestellt. Weiter kann die Erkenntnis gewonnen werden, dass vier WLAN-Router mit diesem Prozessor ausgestattet wurden [37]. Der erste Vertreter der WLAN-Router stellt der Arris TG3442 [30] dar, in der vorliegenden Untersuchung das zu analysierende Gerät. Als zweiter Vertreter sei der Arris DG3450 zu benennen.

Dieser besitzt ebenfalls keine UART-Schnittstelle [38]. Dritter Vertreter ist der Arris SBG8300 [39]. Eine UART-Schnittstelle ist auf diesem ebenso nicht implementiert. An dem Modell Arris TG3452, als vierten Vertreter, kann eine UART-Schnittstelle als 4-Pin-Anschluss auf der Leiterplatine ermittelt werden [35]. Jedes dieser Modelle ist ein WLAN-Router mit Kabelmodem.

4.2.5.3 Zusammenfassung aus Abschnitt 4.2.5.1 und 4.2.5.2

Zu dem Untersuchungsgerät Vodafone Station Arris TG3442DE kann das Modell Arris TG3452 als bauähnliches Modell eruiert werden. Beide weisen dieselbe Leiterplatine und denselben Prozessor auf. Während auf dem Untersuchungsmodell keine UART-Schnittstelle aufgefunden werden kann, ist an dem Modell Arris TG3452 eine UART-Schnittstelle vorhanden. Ein Vergleich der Leiterplatinen zum Arris TG3452 Anhang D, Arris TG3442 Anhang E und Vodafone Station Arris TG3442DE Anhang F wird in den eben benannten Anhängen grafisch dargestellt.

4.2.6 Versuchsaufbau

Für eine Bestimmung der seriellen Schnittstellen und einen damit verbundenen Abzug der Daten, fernab der grafischen Benutzeroberfläche, kommen folgende Möglichkeiten in Betracht:

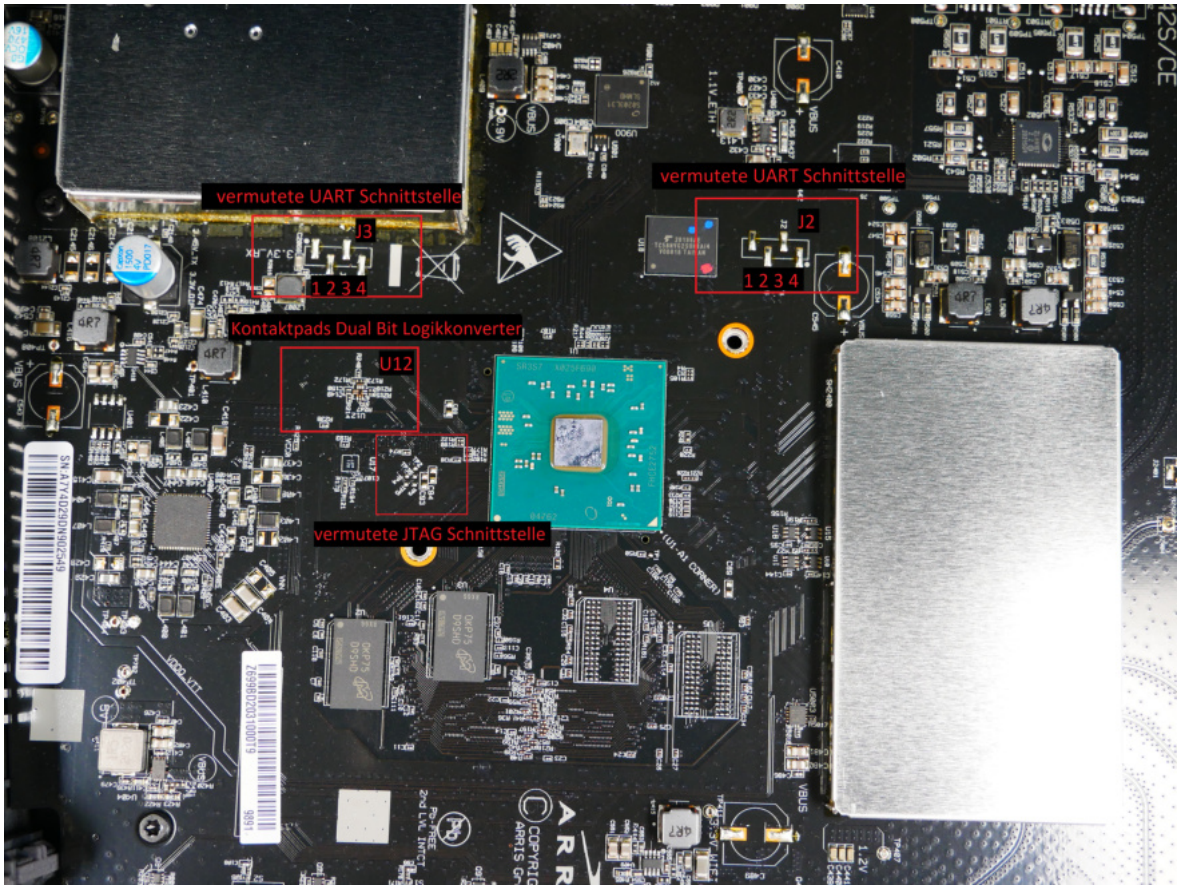

Abbildung 4.9: Vodafone Station Arris TG3442DE - Versuchsaufbau

Möglichkeit 1: Es sind die auf den möglichen Schnittstellen führenden Leiterbahnen und Durchkontaktierungen zu ermitteln. Hierzu besteht die Option die Leiterbahnen mittels Röntgenaufnahmen zu lokalisieren.

Möglichkeit 2: Zur Überprüfung des Vorliegens einer UART-Schnittstelle müssen die möglichen Schnittstellen genau untersucht und bestimmt werden. Aufgrund der unterschiedlichen Spannungsversorgung der UART-Schnittstelle und des Prozessors könnte ein Bauteil benötigt werden, welches die unterschiedlichen Niveaus ausgleicht. Hierfür wäre ein Dual-Bit-Logikkonverter geeignet [40]. Der Dual-Bit-Logikkonverter wandelt die vom Prozessor ausgesandten 1,8 V auf die von der UART-Schnittstelle benötigten 3,3 V um und folglich die ausgesandten 3,3 V der UART-Schnittstelle in die von dem Prozessor benötigten 1,8 V [41]. Es besteht die Möglichkeit, dass ein Dual-Bit-Logikkonverter benötigt wird. Dieser stellt die physische Verbindung des Prozessors mit der UART-Schnittstelle her.

Möglichkeit 3: Auf der Leiterplatine befinden sich 5 aneinanderreihende Testpunkte (T1, T2, T3, T4 und T5). Es könnte sich bei diesen um eine JTAG Schnittstelle handeln. Hierzu sind die Punkte zu lokalisieren und zu bestimmen.

Möglichkeit 4: Es ist die Möglichkeit einen Datenabzug des Flash Speichers über den eMMC Controller zu überprüfen.

Möglichkeit 5: Es ist die Möglichkeit einen Datenabzug des Flash Speichers mittels der Chip-Off Methode, dem Entfernen des Speichermoduls von der Leiterplatine, zu überprüfen.

4.2.6.1 Versuch Möglichkeit 1:

Für das mildeste Mittel mit der geringsten Beschädigungswahrscheinlichkeit wird zunächst der Versuchsaufbau der Möglichkeit 1 gewählt. Hierzu wird von der Leiterplatine eine Röntgenaufnahme aus der Vorder- und Rückansicht erstellt. Die Röntgenaufnahmen sind im Anhang 'G Vodafone Station Arris TG3442DE - Röntgenansicht' angefügt und können dort eingesehen werden. Anhand der gefertigten Röntgenaufnahmen konnte keine detaillierte Führung der Leiterbahnen erkannt werden. Die Leiterbahnen sind ineinander zu verschwommen oder wirken auf den Röntgenaufnahmen für eine gute Ansicht zu schwach. Die im Anhang gewählten Röntgenaufnahmen stellen die am Besten visualisierten Ansichten dar. Es wurden mehrere Versuche zu verschiedenen Einstellungen getätigt. Die Ermittlung Daten-führender Leiterbahnen über Röntgenaufnahmen führt zu keinem Erfolg.

Aufgrund der nicht zu lokalisierenden Leiterbahnen wird die Möglichkeit 2 erprobt.

4.2.6.2 Versuch Möglichkeit 2:

Auf der Leiterplatine des Arris TG3452 können zwei auf dem Gerät verbaute Lötpunktsätze erkannt werden. Diese befinden sich ebenfalls an der zu analysierenden Leiterplatine (Anhang 'H.1 Arris TG3442DE - UART Schnittstellenanalyse'). Es erfolgte wie unter Punkt '3.5.3 UART' die Kontaktierung der Lötpunktstellen. Diese wurden unter Zuhilfenahme eines Multimeters sowie eines Oszilloskops kontaktiert und deren Werte ermittelt. Die genauen Messergebnisse können dem Anhang 'H.1 Arris TG3442DE - Schnittstelle 1' und 'H.2 Arris TG3442DE - Schnittstelle 2' entnommen werden. Aufgrund der ermittelten Werte liegt die Vermutung nahe, dass es sich bei der Schnittstelle 1 um eine UART-Schnittstelle handeln könnte. Beide lokalisierte möglichen UART Schnittstellen wurden mit Brückenkabeln verlötet (Anhang 'I.1 Arris TG3442DE - Lokalisierte Schnittstelle 1' und

'I.2 Arris TG3442DE - Lokalisierte Schnittstelle 2') und mit der Hardware des Logik Analysators 'saneae' verbunden. Durch die weiterführende Analyse, Grafik 'J.1 Vodafone Station Arris TG3442DE - Softwareausgabe Logik Analysator' und 'J.2 Vodafone Station Arris TG3442DE - Hardwareverbund Logik Analysator' kann der UART-Schnittstelle kein Datenstrom entnommen werden.

Für die Kontaktierung der UART-Schnittstelle könnte wie bereits notiert ein Dual-Bit-Logikkonverter benötigt werden. Nach Überprüfung der potentiellen UART-Schnittstellen wurden an die Lötpunkte der Lötpunktstelle U12 Kupferlackdrähte angelötet (Anhang 'J.3 Arris TG3442DE - Lokalisierter Logikkonverter) und mit dem Logikanalysator 'saneae' verbunden. Mit dem Versuchsaufbau kann mittels der Softwareausgabe des Logik Analysators kein Datenstrom entnommen werden.

Für eine finale Überprüfung der Lötpunktstelle U12 wird ein Anlöten des Bauteils vorgenommen. Im vorliegenden Sachverhalt könnte es sich bei dem Dual-Bit Logikkonverter um das Modell 'SN74AVC2T245RSWR' handeln [42] [43]. An die Kontaktierposition des Dual-Bit-Logikkonverters wurde anschließend der Konverter mit der Bezeichnung 'SN74AVC2T245RSWR' mittels der Chip-On Methode mit der Leiterplatine verlötet (Anhang 'K Vodafone Station Arris TG3442DE - Versuchsaufbau Möglichkeit 2'). Eine darauf erfolgte Kommunikation mit der Softwarelösung 'Putty' ergab ebenfalls keinen Datenausgang. Eine Eingabe konnte nicht überführt werden.

Ein Ansprechen der UART Schnittstelle ist mit den analysierten Methoden nicht möglich.

4.2.6.3 Versuch Möglichkeit 3:

Für den Versuchsaufbau der Möglichkeit 3 müssen zunächst die fünf lokalisierten Testlötpunkte mittels Kupferlackdrähten verlötet werden. Anschließend erfolgt eine Auswertung mit dem Logikanalysator 'saneae'. Nach Durchführung der zuvor benannten Punkte kann über die Softwareausgabe kein Datenstrom entnommen werden (Anhang 'J.4 Arris TG3442DE - Lokalisierte JTAG Schnittstelle').

Eine Ausleitung der Daten über die JTAG Schnittstelle ist nicht möglich.

4.2.6.4 Versuch Möglichkeit 4:

Für die Kontaktierung des eMMC Controllers Phison PS8211-0 an der Lötpadstelle U6 wurde zunächst der um die Kontaktpunkte befindliche Lötstoplack mechanisch entfernt. Anschließend konnten die Kontaktierpunkte 'Clock | dt. Takt (CLK)', Datenleitung [Bit 0] (Dat0)', 'Command and Response | dt. Befehl und Antwort (Steuerpin der SD-Karte) (CMD)', 'VCC 3,3 V' und 'GND' [41] [44] mittels Kupferlackdraht kontaktiert werden (Anhang 'L.1 Vodafone Station Arris TG3442DE - Versuchsaufbau Möglichkeit 4 | Anlöten von Kupferlackdrähten'). Für die Gegenstelle wurde ein SD Card Kartenadapter gewählt. Von diesem wurde das Gehäuseteil entfernt und ebenfalls die Kontaktierpunkte 'CLK', Dat0', 'CMD', 'VCC 3,3 V' und 'GND' mittels Kupferlackdraht kontaktiert (Anhang 'L.2 Vodafone Station Arris TG3442DE - Versuchsaufbau Möglichkeit 4 | Anlöten von Kupferlackdrähten an eMMC Modul'). Anschließend konnte der SD Card Adapter wie ein übliches Speichermedium mit dem Untersuchungs PC verbunden werden (Anhang 'L.3 Vodafone Station Arris TG3442DE - Versuchsaufbau Möglichkeit 4 | verbundener SD Card Kartendapter mit Lödpadstelle U6, eMMC Modul

Phison PS8211-0'). Mit dem Verbinden am Untersuchungs PC wurde von diesem kein neues Gerät erkannt. Die Durchführung wurde sowohl am ausgeschalteten, am laufenden als auch am startenden System durchgeführt.

Ein Zugriff auf die Dateistruktur über den eMMC Controller des Flash Speicherchips ist nicht möglich.

4.2.6.5 Versuch Möglichkeit 5:

Für die Datenextraktion wird der Flash Speicher von der Leiterplatine mittels der Chip-Off Methode entfernt (Anhang 'M.1 Vodafone Station Arris TG3442DE - Versuchsaufbau Möglichkeit 5 | Chip-Off Flash Speicher'). Die Umsetzung wurde durch manuelles Entfernen des Speicherchips von der Leiterplatine mittels der Chip-Off Methode durch eine Reworkstation durchgeführt. Bei dem entlöteten Flash Speicher handelt es sich um einen Ball Grid Array | Kugelgitteranordnung (BGA) 63 Chip (Anhang 'M.2 Vodafone Station Arris TG3442DE - Versuchsaufbau Möglichkeit 5 | Chip-Off BGA Chip'). Auf diesem sind 63 Lotkügeln angebracht. Zum Auslesen der Daten wird ein Adapter mit den passenden Abmessungen und Lötkugeln benötigt. Hierfür passend ist der A0-4457 des Universal Programmers für BGA Chips UP2008. Das Speicherabbild liegt im Image Format vor. Die Auswertung der Daten ergibt eine verwürfelte Datenbasis. Diese kann mittels der forensischen Softwarelösung 'Rusolut' sortiert werden.

Der Speicherdump wurde mittels der Softwarelösung 'HxD' eingesehen. In diesem können Bereiche mit Klartextbereichen extrahiert werden. Eine Durchsicht des Speicherdumps mittels der Softwarelösung 'Notepad++' ergab eine Zeilenübersicht von 1.472.339 Zeilen. Nach Entfernen des nicht lesbaren Speicherbereiches konnten 314.874 Zeilen mit lesbarem Inhalt eingesehen werden. Der Speicherbereich zeigt eine Geräteübersicht aller mit dem Router verbundenen Geräte mit dem letzten Log-out Zeitstempel zu dem jeweils zugehörigen Gerät auf. Es wird, wie unter der Tabelle '4.4 Vodafone Station Arris TG3442DE - Syntax Verbindungsaufbau Teilnehmer - Router' beschrieben, der letzte erfolgte Verbindungsaufbau abgelegt.


```
"Device5":  {
    "InstanceNumber":   5,
    "PhysAddress":  "00:57:4A:15:40:44",
    "HostName": "unknown",
    "FriendlyName": "",
    "DisconnectedTS":   "2023-06-08T13:17:14Z",
    "ClientSteerPreference":    0,
    "DeviceType":   0
},
```


Abbildung 4.10: Vodafone Station Arris TG3442DE - Auszug Geräteübersicht Disconnect

Für die Ermittlung der Log-in History wurde eine Filterung mittels des Begriffes 'MAC xx:xx:xx:00:00:00 associated to SSID Router' und 'MAC xx:xx:xx:00:00:00 authentication with SSID Router' durchgeführt. Die Ergebnisse wurden in ein Tabellen Kalkulationsprogramm geladen und nach dem Datum- und Zeitstempel sortiert. Trotz zwischenzeitlicher Stromentnahme, kann eine nahtlose Historie bis zum Erstkontakt des jeweiligen Gerätes mit dem Router entnommen werden. Die Historie umfasst den Analysezeitraum von insgesamt 15 Tagen.

Eine Datenextraktion der Log-in und Log-out Einträge zu mit dem Router verbundenen Geräten kann dem Speicherdump des Flash Speichers im Klartext entnommen werden.

4.2.6.6 Bootloader, Betriebssystem und Dateisystem

Ein Zugriff auf die Prozessablaufstruktur konnte nicht hergestellt werden. Eine Analyse am laufenden System kann zu dem Bootloader, dem Betriebssystem und dem Dateisystem nicht durchgeführt werden. Andere Zugriffsmöglichkeiten lassen sich nicht erkennen.

4.2.7 USB

Eine USB-Schnittstelle ist auf dem WLAN-Router vorhanden. Bezugnehmend auf das Benutzerhandbuch zu dem Router Vodafone Station Arris TG3442DE wird die USB-Schnittstelle derzeit nicht unterstützt. Ein Bedienen externer Speichermedien unter Verwendung der USB-Schnittstelle sei so nicht möglich. Die Schnittstelle selbst soll zukünftig Verwendung finden. Nähere Angaben hierzu werden nicht getätigt [45].

4.2.8 Ethernet

Der WLAN-Router weist vier GbE-LAN Ethernet-Ports auf. Ein LAN-Anschluss kann zum Transfer von Daten genutzt werden. Ein mögliches Protokoll für die Übertragung von Daten ist TFTP.

4.2.9 Alternative Kommunikationswege - TFTP

Das Vorhandensein des Protokolls kann nicht überprüft werden. Aufgrund der nicht verfügbaren seriellen Schnittstelle ist eine Nutzung des Dienstes nicht möglich.

4.3 TP-Link AC1200 Mesh Wi-Fi Router

Aus der Kombination der Ergebnisse von Statista, den Ergebnissen der mitgeschnittenen lokal begrenzten Örtlichkeiten mit WiGLE und dem Vorkommen an WLAN-Routern, welche im strafrechtlichen Kontext vorgefunden werden konnten, wurde für die anschließende Analyse ein WLAN-Router des Unternehmens 'TP-Link' gewählt. Bei dem Modell handelt es sich um das Gerät 'AC1200 Mesh Wi-Fi Router'. In diesem Router ist wie unter Punkt '2.2.4 Router ohne Modem' beschrieben kein Modem verbaut. Zur Kommunikation mit dem Internetprovider muss folgend noch ein Modem vorgesetzt werden. Der Router selbst kann als Erweiterung des Heimnetzwerkes dienen und als Zwischenknoten wie unter Punkt '2.4.1 Access Point' fungieren. Weiter ist das gewählte Modell Mesh-fähig. Die besonderen Eigenschaften der Mesh-Funktion sind unter Punkt '2.4.3 Mesh-System' benannt. Vermarktet wird der Typ dieses Gerätes seit 2019 [46].

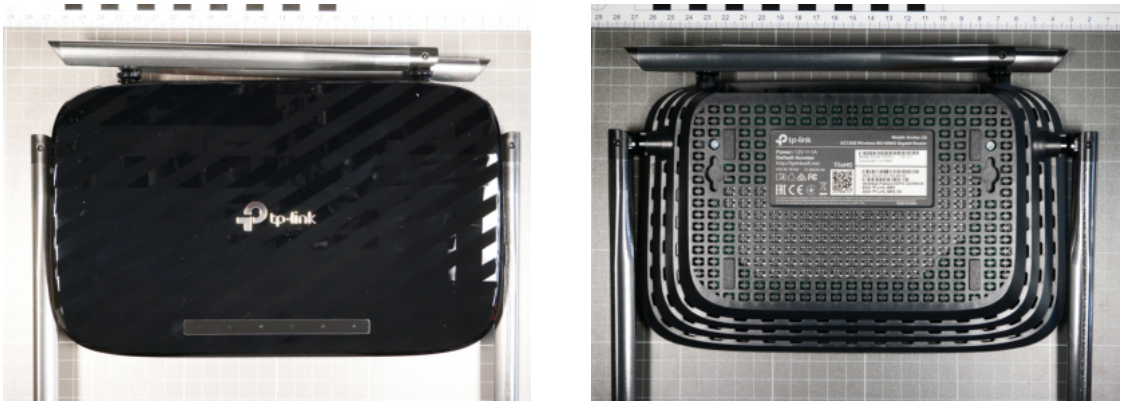

Abbildung 4.11: TP-Link AC1200 Mesh Wi-Fi Router - Vorderseite und Rückseite

Bei dem zu untersuchenden Gerät handelt es sich um eine Neuanschaffung. Daten wurden auf diesem zuvor nicht geschrieben. Eine Datenmanipulation kann zum Analysebeginn ausgeschlossen werden.

Zur Einrichtung des WLAN-Routers wird die grafische Benutzeroberfläche aufgerufen. Dies kann in Form der Default Gateway IP-Adresse '192.168.0.1' oder des Domainnamens 'tplinkwifi.net' erfolgen. Mit dem erstmaligen Aufruf wird der Benutzer zur Eingabe eines freigewählten Passwortes aufgefordert. Ein Standardkennwort wird hierfür nicht vergeben.

Nach der durchgeführten Einrichtung erfolgte noch vor der ersten Nutzung durch Endgeräte das Freilegen der Leiterplatine. Bei dem Gehäuse handelt es sich um zwei mit 11 Haltenasen und zwei Schrauben befestigte Gehäuseteile. Die Schrauben sind auf der Rückseite des Gehäuses klar erkennbar. Die Haltenasen sind schwer unbeschädigt zu öffnen. Für das Öffnen des Gerätes muss die Stromversorgung nicht unterbrochen werden. Da sich das Öffnen der Haltenasen als schwerfällig darstellt, ist im Bereich der Stromversorgung mit äußerster Vorsicht zu arbeiten.

An der Leiterplatine des WLAN-Routers sind vier äußere und eine innere Antenne implementiert. Die Antennen sind nicht abnehmbar.

4.3.1 Technische Eigenschaften

Im Folgenden wird eine Reihe an technischen Eigenschaften aufgeführt, welche das Gerät genauer an seinen Funktionalitäten beschreibt. Zu der Benennung erfolgen die inneren Eigenschaften sowie äußeren Eigenschaften. Äußerlich erkennbar ist das Gerät mit 6x LEDs, 4x 1 GbE-LAN Ethernet-Ports, sowie mit einer Eingangsspannung von 12 VDC und 1 A. Auf der Leiterplatine können diverse Module, wie der RAM, WPS- und WAN-Komponenten, erkannt werden. Diese werden im Folgenden tabellarisch zusammengefasst:

Ausstattung	Beschreibung
LED	6x LEDs: Betrieb, WLAN-2G, WLAN-5G, LAN, WAN, WPS
CPU (SoC)	Qualcomm Atheros QCA9563, 775 MHz
NOR Flash	GigaDevice GD25Q64CSIG, 8 MiB
RAM	Zentel A3R1GE40JBF, 128 MiB DDR2
Ethernet	Qualcomm QCA8337N: 4x 1 Gbps LAN + 1x 1 Gbps WAN
Radio	2,4 GHz, 300 Mbit/s (802.11 b/g/n) Qualcomm Atheros QCA9563 integrated (3x3) 5 GHz, 867 Mbit/s (802.11 a/n/ac) Qualcomm Atheros QCA9886 (2x2)
Schalter	1x An/Aus-Schalter, 1x Zurücksetzen-Schalter, 1x WPS

Tabelle 4.5: TP-Link AC1200 Mesh Wi-Fi Router - Technische Eigenschaften [46] [47]

Mit der Eigenschaft zwei Frequenzbänder gleichzeitig abdecken zu können, handelt es sich bei dem gewählten Modell um ein Gerät, welches die Dualband-Eigenschaft unterstützt. Die kabelgebundene Datenübertragungsrate beläuft sich im Gigabit Bereich und unterstützt damit besonders hohe Geschwindigkeiten. Durch die MU-MIMO Eigenschaft können zudem bis zu zwei mal schnellere Verbindungen realisiert werden. Genauer beschrieben ist eine Kommunikation mit zwei Endgeräten zur selben Zeit möglich. Ein Überschneiden der Bandbreite wird damit ausgeschlossen.

Der WLAN-Router kann neben der grafischen Benutzeroberfläche auf dem Smartphone mit einer App konfiguriert und verwaltet werden. Bei der benötigten App kann die Softwarelösung 'TP-Link Tether' gewählt werden [48]. Schnittstellen wie USB, SATA, Video, Audio oder Telefon sind nicht implementiert.

4.3.1.1 SoC

Auf der Leiterplatine können unter einem Blech zwei Chips vorgefunden werden. Der Chip 'QUALCOMM QCA9563-AL3A' sowie der Chip 'ZENTEL A3R1GE40JBF-8E'. Der Chip 'ZENTEL A3R1GE40JBF-8E' fungiert als DDR2 RAM. Es handelt sich bei diesem Modul um einen Speicher mit doppelter Datenrate.

Bei dem Chip 'QUALCOMM QCA9563-AL3A' handelt es sich um einen WLAN-fähigen LAN Chipsatz 802.11 b/g/n SoC [49]. Dieser wird mit seinen hoch entwickelten Funktionen im Bereich der WLAN-Technologie beschrieben. Die besonderen Eigenschaften können der Tabelle '4.6 TP-Link AC1200 Mesh Wi-Fi Router - SoC Eigenschaften' entnommen werden.

Erwähnenswert bleibt die Pinbelegung mit USB. Hier sei auf das Kapitel '4.3.6 USB' verwiesen.

Ausstattung	Beschreibung
CPU	Taktfrequenz: Bis zu 775 MHz
Wi-Fi	Spitzengeschwindigkeit: Bis zu 300 Mbit/s Generation: Wi-Fi 4 Standards: 802.11b, g, n Kanäle: 40 MHz MU-MIMO Aufbau: 2x2 Räumliche Streams: Bis zu 2
Ethernet	Anzahl Ports: 4+1 (ein Uplink/WAN Port, der nicht als LAN Port genutzt wird) Spitzen-PHY-Rate: 100 Mbit/s Standards: IEEE 802.3
Speicher	Geschwindigkeit: 300 MHz Typ: DDR2
Schnittstellen	Unterstützte Schnittstellen: USB 2.0, UART, PCIe 1.1, SPI, JTAG Allzweck-I/Os: 17
Paket	Typ: DRQFN Größe: 12 × 12 mm

Tabelle 4.6: TP-Link AC1200 Mesh Wi-Fi Router - SoC Eigenschaften [50]

4.3.2 Grafische Benutzeroberfläche

Wie unter Punkt '4.3 TP-Link AC1200 Mesh Wi-Fi-Router' benannt, erfolgt zunächst die Anmeldung auf der grafischen Benutzeroberfläche. Tabellarisch betrachtet kann in der obersten Reihe zwischen den Reitern 'Quick Setup', 'Basic' sowie der 'Advanced' Ansicht navigiert werden. Die Spaltenauswahl der linken Ansicht ändert sich je nach gewähltem Reiter der Reihenansicht. Zu Beginn wird die Basisansicht dargestellt. Für forensische Untersuchungen empfiehlt es sich, in die fortgeschrittene Ansicht 'Advanced' zu navigieren.

Zur Auswahl stehen in der Reihenansicht nun die folgenden Reiter 'Status', 'Network', 'Operation Mode', 'Wireless', 'Guest-Network', 'Parental Controls', 'Quality of Service (QoS)', 'Security', 'NAT-Forwarding', 'IPv6', 'Virtual Private Network (VPN)-Server', 'Smart Life-Assisstent' und 'System Tools'.

Unter dem Reiter 'Status' können auf den ersten Blick wichtige Informationen zu LAN, WLAN sowie der Internetverbindung eingesehen werden. Ebenfalls können die momentan mit dem Router verbundenen Geräte erfasst werden. Bei Anklicken eines Gerätes werden neben der SSID, die IP-Adresse sowie die MAC-Adresse und, falls eine drahtlose Verbindung über WLAN hergestellt wurde, das verwendete Frequenzband dargestellt. Zeitstempel für den Beginn der aktiven Verbindung werden nicht angezeigt.

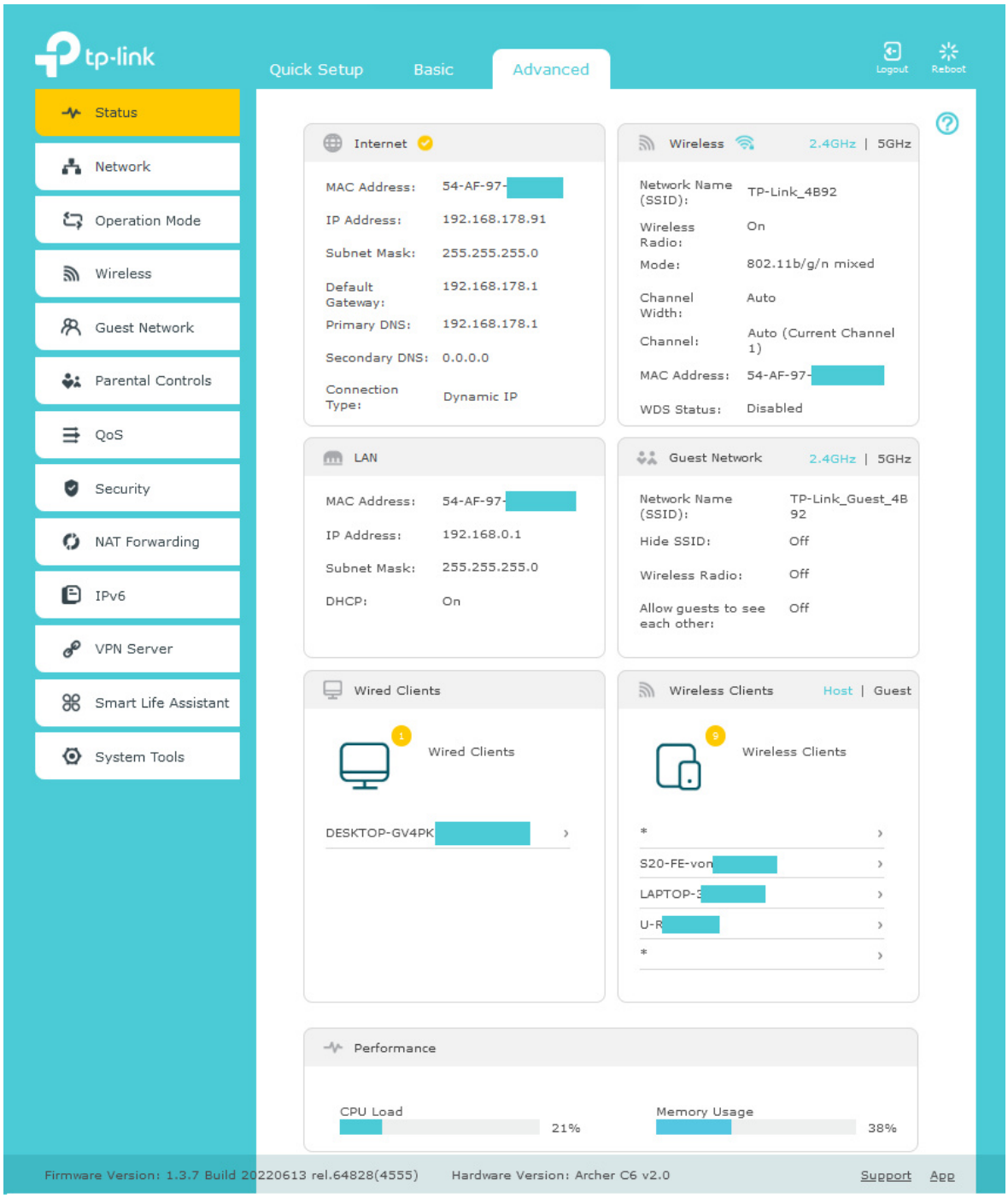

Abbildung 4.12: TP-Link AC1200 Mesh Wi-Fi Router - Grafische Benutzeroberfläche

Unter der waagerechten Reiterauswahl ’Basic’ befindet sich der Button ’TP-Link Cloud’. Für eine Verwendung dieser Funktion ist eine erneute Registrierung notwendig. Nach erfolgter Registrierung werden, neben den für diesen Router registrierten Benutzerkonten, lediglich die Account und Geräteinformationen angezeigt (Abbildung ’4.13 TP-Link AC1200 Mesh Wi-Fi Router - TP-Link Cloud Startseite’).

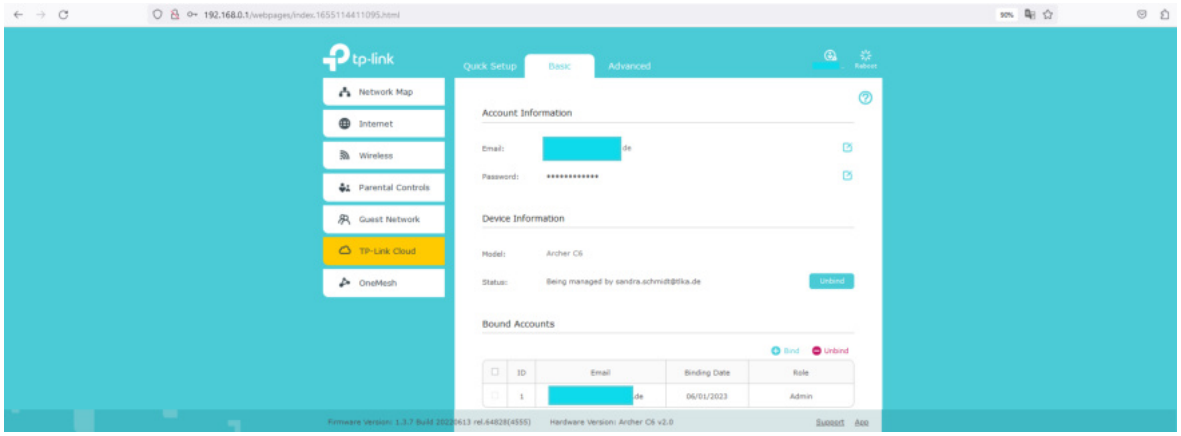

Abbildung 4.13: TP-Link AC1200 Mesh Wi-Fi Router - TP-Link Cloud Startseite

Auf der zugehörigen Weboberfläche kann eruiert werden, dass die Nutzung von TP-Link Cloud Kameras vorbehalten ist. Der Nutzen bezieht sich auf eine zeitgenaue WLAN übertragene Videoüberwachung [51].

Für die Untersuchung der flüchtigen und persistenten Datenbasis werden Datensicherungen von der Erstinbetriebnahme, einer Laufzeit von 7 Tagen sowie der Datenansicht nach Entfernen der Stromzufuhr vorgenommen und miteinander verglichen. Hierzu können nachfolgende Erkenntnisse aus der Ansicht der grafischen Benutzeroberfläche gewonnen werden:

4.3.2.1 Flüchtige Datenbasis

Für die Navigation wird die fortgeschrittene Ansicht 'Advanced' gewählt. Anhand folgender Punkte kann eine flüchtige Datenbasis ermittelt werden:

1. Unter dem Punkt
Network → DHCP Server → DHCP Client List
   kann eine Geräteliste entnommen werden. Diese wird zeitaktuell geführt. Mit der Einwahl eines Gerätes wird dieses in die Liste eingepflegt und mit der Auswahl eines Gerätes aus der Liste entfernt. Ein zeitlicher Ablauf der Verbindungsdaten findet nicht statt. Unter diesem Punkt wird eine 'Lease Time' geführt, welche einen Countdown abwärts zählt. Die Tabelle wird mit den Reitern 'ID, Client Name, MAC-Adresse, IP Adresse' ausgegeben. Die Einstellung der 'Lease Time' wird unter dem Punkt
Network → DHCP Server → Settings
   im Feld 'Adresse Lease Time' vom Administrator eingestellt.
2. Unter dem Punkt
Wireless → Statistics → Wireless Station Online
   kann eine Geräteliste entnommen werden. Diese wird zeitaktuell geführt. Mit der Einwahl eines Gerätes wird dieses in die Liste eingepflegt und mit der Auswahl eines Gerätes aus der Liste entfernt. Ein zeitlicher Ablauf zu den Verbindungsdaten findet nicht statt. Die Tabelle wird mit den Reitern 'ID, MAC-Adresse, Connection Type (2,4 GHz / 5 GHz), Security (Wi-Fi Protected Access [Wi-Fi-geschützter Zugriff] (WPA)2Pre-shared key (PSK)), Received Packets, Sent Packets' geführt. Dabei stimmen die Werte mit denen des folgenden Punktes überein:
Security → Access Control → Online Devices

Diese wird zeitaktuell geführt. Mit der Einwahl eines Gerätes wird dieses in die Liste eingepflegt und mit der Auswahl eines Gerätes aus der Liste entfernt. Ein zeitlicher Ablauf zu den Verbindungsdaten findet nicht statt. Die Tabelle wird mit den Reitern 'ID, Device Name, IP-Adresse, MAC-Adresse, Connection Type (wireless/wired), Modify' geführt.

3. Unter dem Punkt

   Security → IP- & MAC-Binding → Address Resolution Protocol (ARP) List

   kann eine Geräteliste entnommen werden. Diese wird zeitaktuell geführt. Mit der Einwahl eines Gerätes wird dieses in die Liste eingepflegt und mit der Auswahl eines Gerätes aus der Liste entfernt. Ein zeitlicher Ablauf zu den Verbindungsdaten findet nicht statt. Die Tabelle wird mit den Reitern 'ID, MAC-Adresse, IP-Adresse, Bound (unbound), Modify' geführt.
4. Unter dem Punkt

   System Tools → Administration → System Log

   kann eine Logdatei entnommen werden. Das System Log ist als Logdatei downloadbar. Die Logeinträge werden mit den Reitern 'ID, Time, Type (Remote / Local Management, DHCP Server, Access Control), Level (Info, Notice), Log Content (IP und MAC-Adresse)' geführt.
   Aus dem gesicherten Datenbestand des System Logs können die von dem Router an die Endgeräte zugewiesenen IP-Adressen erkannt werden. Ein Zeitstempel wird mit angegeben. Die Anzeige des Zeitstempels erfolgt in der Zeitzone Mitteleuropäische Zeit (MEZ). Bei Vorliegen der mitteleuropäischen Sommerzeit muss diese um eine Stunde addiert werden. Die Zeit für das Einloggen eines Gerätes auf dem Router kann dem System-Log entnommen werden. Eine Grafik wird unter dem Punkt 'N.1 TP-Link AC1200 Mesh Wi-Fi Router - Anmeldevorgang Paketaustausch Syslog' dargestellt. Es kann festgestellt werden, dass es sich bei der Datenablage zu diesem Modell um einen Ringspeicher handelt. In der Datenablage werden die ältesten Einträge zuerst überschrieben. Die Dateigrößen aller gesicherter Ereignissprotokolle befinden sich bei 48 kB. Die Speicherdauer umfasst bis zu sieben Tage.

4.3.2.2 Persistente Datenbasis

Als persistente Datenbasis können sämtliche Konfigurationsdaten erkannt werden. Das betrifft für diesen Router alle Daten bis auf die im Punkt '4.3.2.1 Flüchtige Datenbasis' benannten. Auf der grafischen Benutzeroberfläche stellen Daten mit Bezug zu Geräten durchweg flüchtige Daten dar.

4.3.3 SSH

Für die Überprüfung des Dienstes SSH erfolgt mittels Portscans eine Durchsicht auf offene Ports (Abbildung '4.14 TP-Link AC1200 Mesh Wi-Fi Router - Portscan').

Für den Dienst SSH kann bei der Überprüfung des Dienstes ein offener Port festgestellt werden. Der Dienst ist auf diesem Router freigegeben. Es besteht die Annahme, dass dieser somit ansprechbar ist. Ein Zugriff zu diesem Dienst gestaltet sich als schwierig. Bei Ansprechen des Dienstes unter dem entsprechenden Port wird die Fehlermeldung 'channel 0: open failed: unknown channel type: Connection to 192.168.0.1 closed.' (Abbildung '4.15 TP-Link AC1200 Mesh Wi-Fi Router - SSH') ausgegeben.

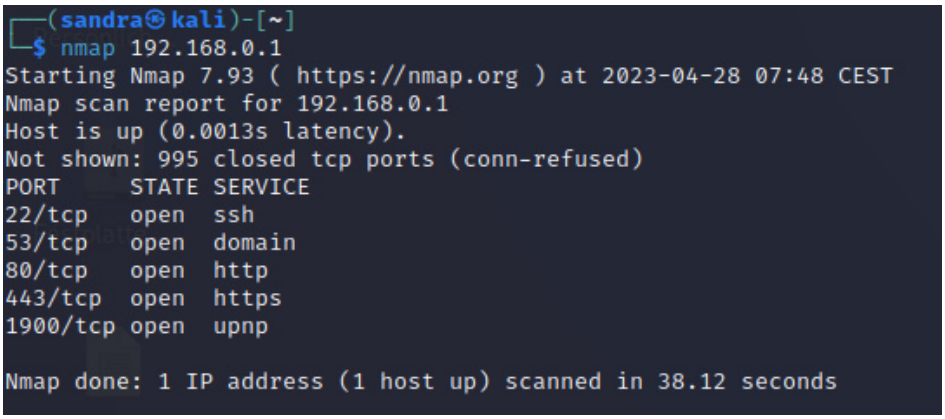

Abbildung 4.14: TP-Link AC1200 Mesh Wi-Fi Router - Portscan

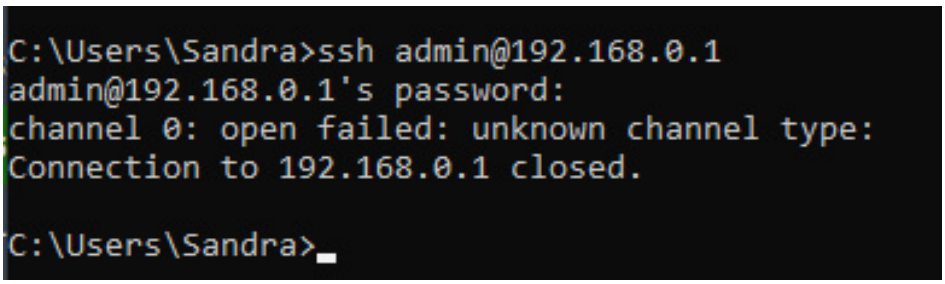

Abbildung 4.15: TP-Link AC1200 Mesh Wi-Fi Router - SSH

Die Fehlermeldungen unterscheiden sich nach Art des gewählten Benutzers. Bei der Eingabe eines falschen Benutzers erscheint die Fehlermeldung 'Connection closed by 192.168.0.1 port 22', Abbildung '4.16 TP-Link AC1200 Mesh Wi-Fi Router - SSH falscher Benutzer':

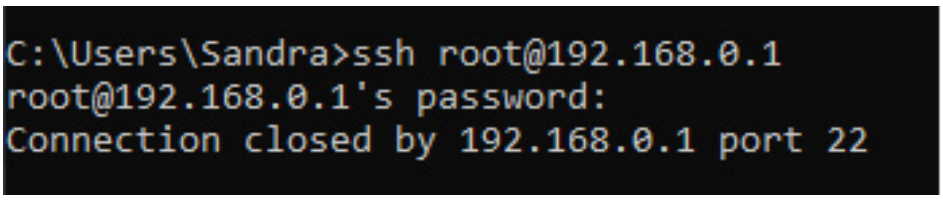

Abbildung 4.16: TP-Link AC1200 Mesh Wi-Fi Router - SSH falscher Benutzer

Bei der Eingabe des richtigen Benutzers mit dem falschen Passwort wird die Meldung 'Permission denied, please try again.' ausgegeben:

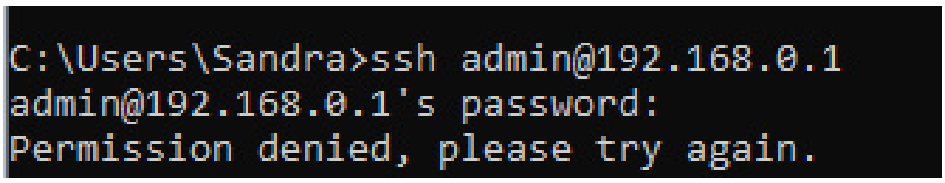

Abbildung 4.17: TP-Link AC1200 Mesh Wi-Fi Router - SSH falsches Passwort

Es kann festgestellt werden, dass der Zugang zum Dienst SSH mit dem Benutzer 'admin' und als Kennwort das Kennwort der grafischen Oberfläche versehen ist. Trotz offenen Ports konnte keine erfolgreiche Verbindung zu dem Dienst hergestellt werden. Bei der anschließend durchgeführten Recherche konnte ermittelt werden, dass der Dienst SSH der Produkte von TP-Link nur für TP-

Link Apps gelte [52]. Die App fungiert für eine bessere Verwaltung und Konfiguration des Gerätes. Beispiele für Apps der TP-Link seien Tether 2.0-, Deco-, Tapo- sowie die tpCamera-App. Ein Zugriff dritter Geräte ist somit ausgeschlossen [53].

4.3.4 Telnet

Für die Überprüfung des Dienstes Telnet erfolgt mittels Portscans eine Durchsicht auf offene Ports. Für den Dienst Telnet kann bei der Überprüfung des Dienstes kein offener Port festgestellt werden. Der Dienst ist auf diesem Router nicht freigegeben und somit nicht ansprechbar.

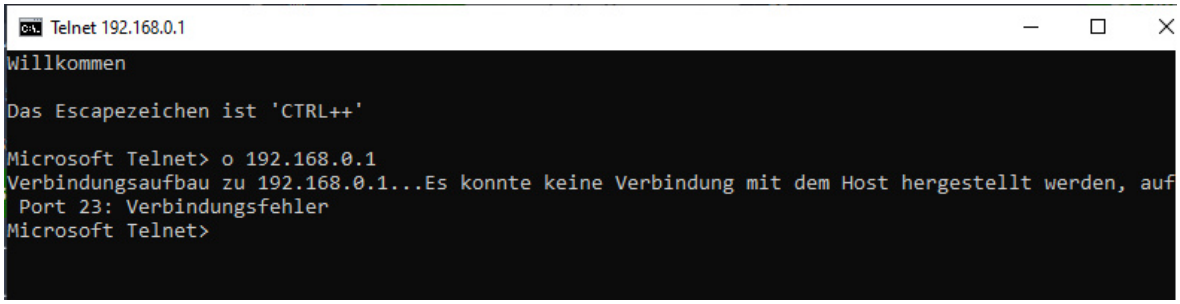

Abbildung 4.18: TP-Link AC1200 Mesh Wi-Fi Router - telnet

4.3.5 UART

Auf der Leiterplatine kann eine integrierte oberflächen-UART-Schnittstelle erkannt werden. Die Kontaktierpunkte liegen nicht nah beieinander und werden an unterschiedlichen Punkten vorgefunden. Eine Benennung der UART-Kontaktierpunkte erfolgt vom Hersteller aus. Die Kontaktierung und Testung der Pinbelegung wie unter Punkt '3.5.3 UART' benannt, ist nicht erforderlich. Aufgrund der Größe der Testpunkte und der auf der Oberfläche der Leiterplatine befindlichen Kontaktierpunkte ist eine Belegung mit den zugehörigen Datenkabel mit einer Kontaktierspinne erforderlich.

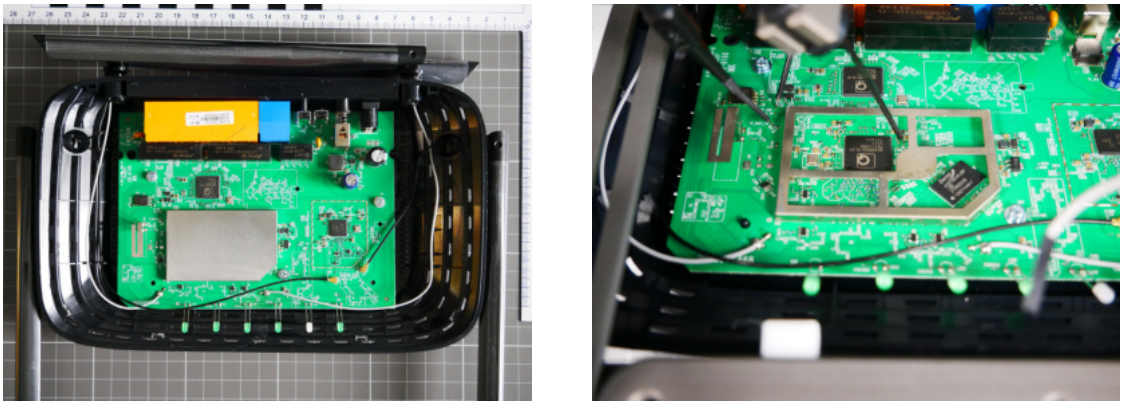

Abbildung 4.19: TP-Link AC1200 Mesh Wi-Fi Router - Leiterplatine und UART-Pinbelegung

Für die Verbindung einer seriellen Kommunikation wird die Softwarelösung 'Putty' gewählt. Der Zugriff auf die Konsole gestaltet sich als herausfordernd. Für verschiedene Baudraten wurden zum Teil klar lesbare und zum Teil nicht lesbare Inhalte ausgegeben. Ein Konsolenzugang mit durchlaufendem Booten des Systems ist nicht möglich. Bei Kontaktierung der Schnittstelle unter laufendem Betrieb kann der Konsolenzugang hergestellt werden. In der Tabelle '4.7 TP-Link AC1200 Mesh Wi-Fi Router - UART-Konsole' können die unterschiedlich ermittelten Werte der Baudraten entnommen werden.

Baudrate	Ausgabe
128000, 8N1	Bootvorgang nur Anfang, danach nicht lesbar, Eingabe verrauscht - nicht möglich [128000-115200=12800 → 128000-6400=121600]
121600, 8N1	Bootvorgang nur Anfang, danach nicht lesbar, Eingabe verrauscht - nicht möglich [121600-3200=118400]
118400, 8N1	Bootvorgang komplett, bestes Ausgabeergebnis, Eingabe verrauscht - nicht möglich [118400-1600=116800]
116800, 8N1	Bootvorgang komplett, bestes Ausgabeergebnis, Eingabe verrauscht - nicht möglich [116800-800=116000]
116000, 8N1	Bootvorgang Anfang nicht lesbar, danach lesbar, Eingabe wird nicht erkannt nicht möglich
115200, 8N1	Bootvorgang Anfang nicht lesbar, danach lesbar, Eingabe wird nicht erkannt nicht möglich
115200, 8N1	laufender Betrieb - Konsole ansprechbar, Eingabe wird erkannt Navigation im Dateisystem möglich, alles einsehbar

Tabelle 4.7: TP-Link AC1200 Mesh Wi-Fi Router - UART-Konsole

Ein problemloser Zugang zur Konsole ist am laufenden Betrieb möglich. Eine Passworteingabe ist nicht vorgesehen. Mit der Betätigung der Tabulator Taste erfolgt automatisch der Zugang zur Konsole. Ein freies navigieren durch die Dateisystemstruktur ist möglich. Eine grafische Darstellung der Startausgabe mittels der Softwarelösung 'Putty' auf der Kommandozeile kann der Grafik aus Anhang 'O TP-Link AC1200 Mesh Wi-Fi Router - Beginn der Konsolenausgabe' entnommen werden. Der Verbindungsaufbau und die damit veränderte Datenbasis in Form der Eintragung des Untersuchungsgerätes in den Speicherinhalten des Routers kann in der RAM Sicherung und der Konsole entnommen werden (Anhang 'P TP-Link AC1200 Mesh Wi-Fi Router - Einwahl Untersuchungsrechner am WLAN-Router').

4.3.5.1 Bootloader, Betriebssystem und Dateisystem

Nach Punkt '4.3.5 TP-Link AC1200 Mesh Wi-Fi Router - UART' kann mit Einschalten des Gerätes der Bootprozess eingesehen werden. Es folgen diverse durchlaufende Prozesse. Benötigte Treiber werden geladen. Die Hard- und Software wird auf ihre Kapazitäten und Verfügbarkeiten hin überprüft. Die Komponenten der Hardware Flash Speicher, RAM, SoC sowie CPU werden im Bootprozess geprüft. Die Angaben entsprechen denen von Punkt '4.3.1 Technische Eigenschaften'. Über die Softwareeigenschaften kann der Bootloader 'U-Boot Version 1.1.4', das Betriebssystem 'Linux 3.3.8' sowie das Dateisystem 'Squashfs Version 4.0' aus dem Bootprozess ermittelt werden.

Weiterhin erfolgt eine Konfiguration der dynamischen Speicherverwaltung, der globalen Daten, des Boot Parameters und des Stapelzeigers. Das Laden der 'Access Control' wird aufgezeigt. Hierzu können Inhalte der Datei '/tmp/client_list.json' dem Bootprozess entnommen werden. Eine Untersuchung dieser erfolgt unter Punkt '4.3.8.5 Client List'.

Es wird ausgegeben, dass der Kernel in seiner Eingabeaufforderung auf der Konsole mit ttyS0 mit einer Baudrate von 115200 kommuniziert. Dabei wird unter ttyS0 ein Gerät verstanden, welches für die Verwendung von seriellen Schnittstellen wie UART seine Anfänge gefunden hat. Hierbei wird der COM-Port 1 als ttyS0 benannt [54]. Der angegebene Wert spiegelt sich mit dem getesteten Wert, welcher einen Zugriff auf das System zulässt, wieder.

Dem Bootprozess kann folgende Partitionstabelle entnommen werden:

Offset	Größe	Partition
0x000000-0x030000	192 kiB	u-boot
0x030000-0x130000	1024 kiB	uImage
0x130000-0x7e0000	6848 kiB	rootfs
0x7f0000-0x800000	64 kiB	ART

Tabelle 4.8: TP-Link AC1200 Mesh Wi-Fi Router - Bootloader [Partitionen]

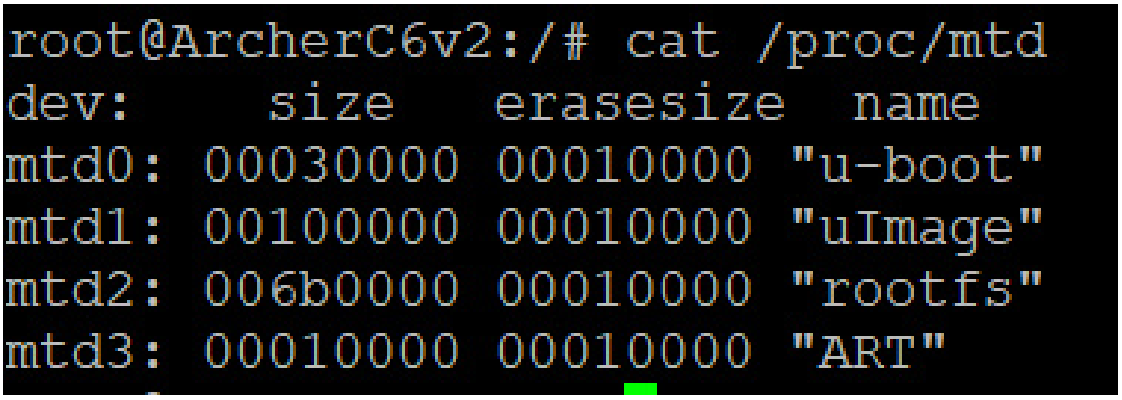

Abbildung 4.20: TP-Link AC1200 Mesh Wi-Fi Router - Dateisystem [Partitionen]

Die Summe der Partitionen ergibt die Datengröße des Flash Speichers und verifiziert dessen angegebene Speichergröße. Eine Datenextraktion der einzelnen Partitionen hat in Analysetools wie 'HxD' oder 'XWays' keinen nachvollziehbaren Kontext ergeben. Das Format ist nicht lesbar. Eine Interpretation der Daten war nicht möglich.

Der durchlaufende Bootprozess kann nach Durchlaufen mit ca. 700-800 Zeilen als Übergabe in eine Textdatei eingesehen werden.

4.3.6 USB

Eine USB-Schnittstelle ist auf dem WLAN-Router nicht vorhanden. Eine Datenextraktion hierüber kann nicht vorgenommen werden.

Bei der Durchsicht des Datenblattes zu dem im Gerät verbauten SoC aus Kapitel '4.3.1 Technische Eigenschaften' kann festgestellt werden, dass an diesem zwei USB 2.0 Host-Controller verbaut sind. Diese weisen eine MAC- und PHY-Adresse auf. Für jeden USB 2.0 Host-Controller sind drei Pins gesetzt [55]. Der Tabelle '4.9 TP-Link AC1200 Mesh Wi-Fi Router - USB-Belegung auf SoC' kann die Pinbelegung des SoCs entnommen werden.

Es ist erkennbar, dass von beiden USB 2.0 Host-Controllern zwei der drei Pins auf der Leiterplatine nicht verbunden sind. Von diesen gehen keine Datenleitungen ab [56]. Der Stiftabstand der Pins beträgt zueinander 0,5 Millimeter (mm).

4.3.7 Ethernet

Der WLAN-Router weist vier LAN-Anschlüsse auf. Ein LAN-Anschluss kann zum Transfer von Daten genutzt werden. Ein mögliches Protokoll für die Übertragung von Daten über Ethernet ist TFTP.

Pin	Belegung	Bedeutung	Status
B43	VDD12_PLL_USB	1,2V Versorgung für USB PLL	verbunden
A55	USB_DP1	Zweites USB D+ Signal; überträgt USB-Daten	zu und vom USB 2.0 PHY nicht verbunden
B42	USB_DM1	Zweites USB-D-Signal; überträgt USB-Daten	zu und vom USB 2.0 PHY nicht verbunden
A53	VDD12_PLL_USB	1,2V Versorgung für USB PLL	verbunden
B40	USB_DP0	USB D+-Signal; überträgt USB-Daten	zu und vom USB 2.0 PHY nicht verbunden
A52	USB_DM0	USB-D-Signal; überträgt USB-Daten	zu und vom USB 2.0 PHY nicht verbunden

Tabelle 4.9: TP-Link AC1200 Mesh Wi-Fi Router - USB-Belegung auf SoC

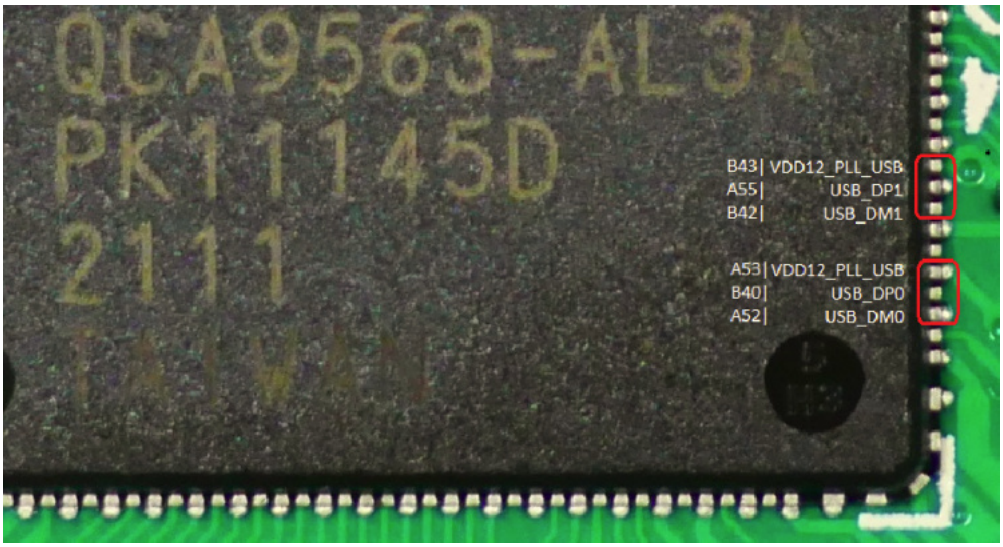

Abbildung 4.21: TP-Link AC1200 Mesh Wi-Fi Router - SoC Überblick USB-Pin Belegung Nahansicht

4.3.8 Alternative Kommunikationswege - TFTP

Mit dem durchgeführten Portscan konnte kein offener Port für 'TFTP' festgestellt werden. Der Standardport für 'TFTP' ist für Port 69 vergeben.

In der Dateiansicht kann das Kommando 'TFTP' unter dem Pfad '/usr/bin/TFTP' aufgefunden werden. Der Aufruf der Hilfe lässt die Syntax darstellen. Für die Verwendung des Protokolls 'TFTP' wird ein TFTP-Server gestartet. Bei der gewählten Softwareapplikation wird das Programm 'TFTPd64' verwendet. Der Untersuchungs-PC agiert als TFTP-Server, der WLAN-Router als TFTP-Client. In die Konsole der UART-Verbindung wird die geforderte Befehlssyntax in seine entsprechenden Parameter überführt. Als Ergebnis kann festgehalten werden, dass eine Ausgabe nicht stattgefunden hat. Eine Fehlermeldung wird nicht ausgegeben. Bei der logischen Durchsicht im Dateisystem kann unter dem Dateipfad '/etc/group' ermittelt werden, dass für den Dienst 'TFTP' der Port 55 vergeben wird (Abbildung '4.22 TP-Link AC1200 Mesh Wi-Fi Router - Port 'TFTP").

Ein darauf erfolgter Datenversand konnte erfolgreich verzeichnet werden. Die Dateigröße des gesicherten Datenbereiches stimmt mit dem des RAM-Moduls überein. Beide betragen, wie in der Tabelle '4.5 TP-Link AC1200 Mesh Wi-Fi Router - Technische Eigenschaften' benannt, 128 MiB.

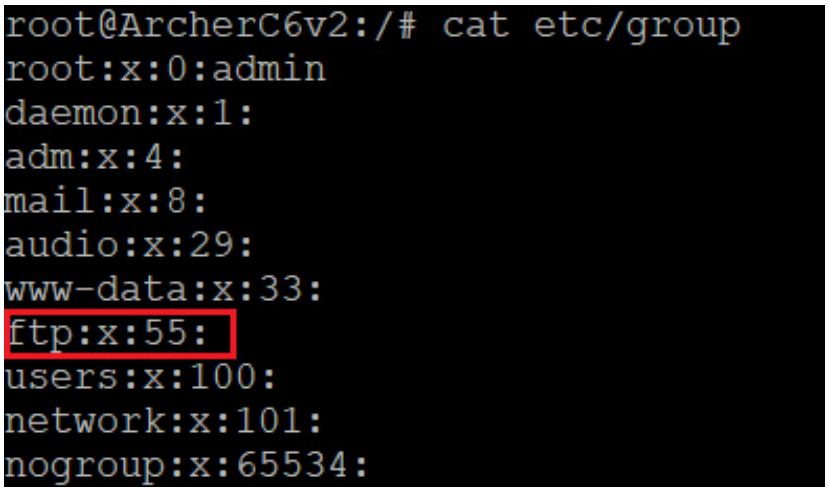

Abbildung 4.22: TP-Link AC1200 Mesh Wi-Fi Router - Port 'TFTP'

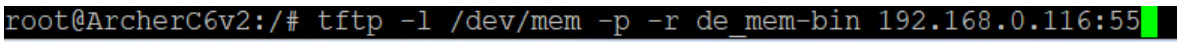

Abbildung 4.23: TP-Link AC1200 Mesh Wi-Fi Router - Datentransfer 'TFTP' Konsole

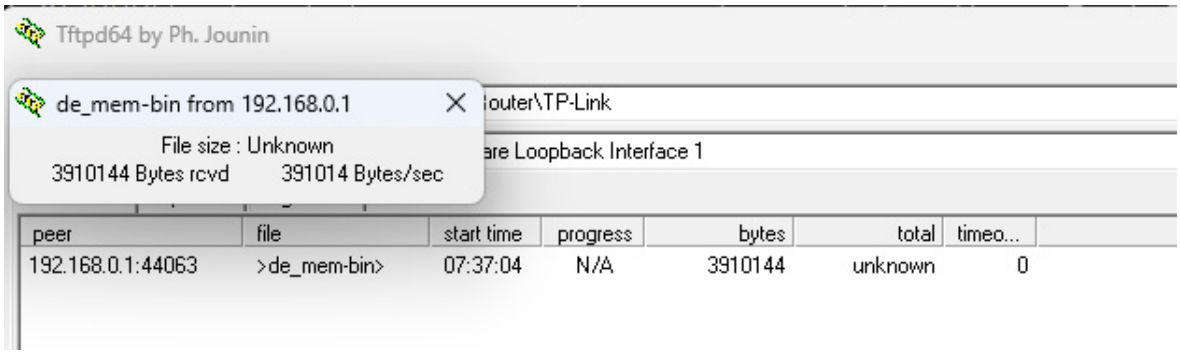

Abbildung 4.24: TP-Link AC1200 Mesh Wi-Fi Router - Datentransfer 'TFTP' TFTPd64

4.3.8.1 Datenbasis

Mit dem Verbinden des Untersuchungsrechners und dem laufenden System an der seriellen Schnittstelle UART können über die Oberfläche der Kommandozeile viele forensisch wertvolle Informationen gewonnen werden. Ein Überblick zu der vorliegenden Dateibaumstruktur kann mittels des Linux Konsolenbefehls 'list (ls)' auf der Konsole aufgezeigt werden.

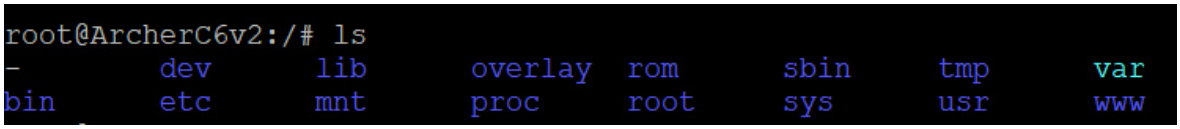

Abbildung 4.25: TP-Link AC1200 Mesh Wi-Fi Router - Dateisystem Rootverzeichnis

Nach Überprüfung des Befehls 'TFTP' ist ein Datenabzug der Datenbasis aus der Dateibaumstruktur, aber auch eine Sicherung des flüchtigen Speicherinhaltes des RAM-Moduls möglich. Die Ablage des flüchtigen RAM Datenbestandes kann unter dem Dateipfad '/dev/mem' aufgefunden werden. Die Übertragung kann über LAN oder WLAN erfolgen. Bei der Eingabe muss auf die IP-Adresse

des Untersuchungs PCs geachtet werden. Diese ist vorher über die Konsole des Untersuchungs PCs mittels 'arp -a' zu überprüfen. Die Durchsicht des gesicherten RAM Speicherinhaltes erfolgte mittels des Linux-Kommandozeilenbefehls 'binwalk'. Diese führte zu keinem Ergebnis, mit welchem eine weiterführende Analyse durchgeführt werden kann. Die Betrachtung des RAM-Speicherinhaltes in seiner Binärform erfolgte für die weiteren Analysen zum einen mittels des Hexeditors 'HxD' und zum anderen mittels dem Texteditor 'Notepad++'. Es erfolgte die Sichtung der Klartextanteile. Neben diversen Konfigurationsprogramminhalten wird der überwiegende Inhalt in einem nicht lesbaren Format ausgegeben.

Um den gewonnenen Datenbestand besser einschätzen zu können, wurden mehrere Datensicherungen zu unterschiedlich durchgeführten Szenarien vorgenommen. So konnte ermittelt werden, welche Daten gespeichert werden und in welcher Form die Datenablage erfolgt.

Die folgenden Punkte sollen einen Überblick über die Datenvielfalt verschaffen.

4.3.8.2 DHCP Datenpakettransfer

Eine durchgeführte Falscheingabe des WLAN Kennwortes bei der Einwahl, lässt einen versuchten Anmeldevorgang in der flüchtigen Datenbasis der RAM-Sicherung erkennen. Nach einer zuvor beginnenden Verbindung erfolgt anschließend die Trennung dieser.

```
69 6E 66 6F 20   06:32:55 <daemon.info> nrd[5649]: triggermon info
72 20 30 30 3A  : triggerMonAssocObserver: Update Threshold for 00:
72 6F 73 73 69  57:4A:15:40:44 due to association, highTxRateCrossi
20 61 70 53 74  ngThreshold_UG:50,highRSSIXingThreshold_UG:40, apSt
58 69 6E 67 54  eerLowRSSIXingThresholds_5g:28, apSteerLowRSSIXingT
69 6E 66 6F 3E  hresholds_24g:28..2023-06-12 06:32:55 <daemon.info>
2E 31 31 3A 20   hostapd: ath1: STA 00:57:4a:15:40:44 IEEE 802.11:
6E 65 6C 3A 20  associated.2023-06-12 06:32:55 <kern.warn> kernel:
45 3A 20 43 68  [123275.390000] [wifi1] FWLOG: [126232860] RATE: Ch
73 20 30 78 30  ainMask 1, peer_mac 40:44, phymode 10, ni_flags 0x0
2C 20 6C 65 67  621b006, vht_mcs_set 0xfffe, ht_mcs_set 0x00ff, leg
6E 2E 69 6E 66  acy_rate_set 0x0ff0.2023-06-12 06:32:56 <daemon.inf
74 73 43 6D 6E  o> nrd[5649]: wlanif     info : wlanifLinkEventsCmn
34 20 64 69 73  GenerateDisassocEvent: Client 00:57:4A:15:40:44 dis
32 33 2D 30 36  associated on APId 255 ChanId 36  ESSId 0  .2023-06
20 20 20 69 6E  -12 06:32:59 <daemon.info> nrd[5649]: stadb      in
20 30 20 77 69  fo : stadbUpdateAssoc: Update associaton state 0 wi
37 3A 34 41 3A  th btm status 2, rrm status 2 for station 00:57:4A:
74 61 70 64 3A  15:40:44.2023-06-12 06:32:59 <daemon.info> hostapd:
73 73 6F 63 69   ath1: STA 00:57:4a:15:40:44 IEEE 802.11: disassoci
                ated.2023-06-12 06:33:01
```

Abbildung 4.26: TP-Link AC1200 Mesh Wi-Fi Router - Versuchter Anmeldevorgang

Dem erfolgreich durchgeführten Anmeldevorgang kann unter der Abbildung '4.27 TP-Link AC1200 Mesh Wi-Fi Router - Erfolgreicher Anmeldevorgang' ein vollständiger WPA Paketaustausch entnommen werden.

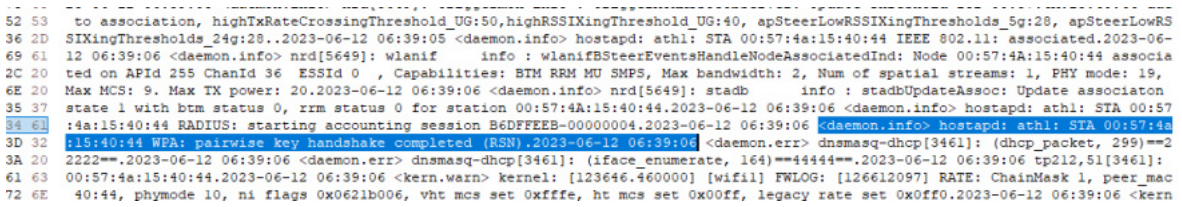

Abbildung 4.27: TP-Link AC1200 Mesh Wi-Fi Router - Erfolgreicher Anmeldevorgang

Bei der Sichtung des RAM-Inhaltes konnten Bereiche des Paketversandes aus dem Verbindungsaufbau zum paarweisen Schlüsselaustausch über WPA von Teilnehmern im lokalen Netzwerk ermittelt werden (Anhang 'R.1 TP-Link AC1200 Mesh Wi-Fi Router - Richtige Passworteingabe _ Anmeldevorgang Paketaustausch'). Die geführten Einträge weisen die MAC-Adresse mit der zugehörigen IP-Adresse des Geräts in Verbindung mit der IP-Adresse des Routers, einen Log-in Zeitstempel, sowie einen Pakettransfer Zeitstempel auf. In der folgenden Tabelle kann der Ablauf eines Paketversandes nachvollzogen werden:

Nr.	Paket	IP	IP	MAC	Zeit	DHCP	DHCP
1	tp212,51			MAC Gerät	Datum & Uhrzeit	DISCOVER	OFFER
2	tp212,52	IP Gerät	IP Router	MAC Gerät	Datum & Uhrzeit		
3	tp212,51			MAC Gerät	Datum & Uhrzeit	DISCOVER	OFFER
4	tp212,52	IP Gerät	IP Router	MAC Gerät	Datum & Uhrzeit	DISCOVER	OFFER
5	tp212,52	IP Gerät	IP Router	MAC Gerät	Datum & Uhrzeit		
6	tp212,53	IP Gerät		MAC Gerät	Datum & Uhrzeit	REQUEST	ACK
7	tp212,54	IP Gerät	IP Router	MAC Gerät	Datum & Uhrzeit		

Tabelle 4.10: TP-Link AC1200 Mesh Wi-Fi Router - Paketversand RAM-Sicherung

Es kann erkannt werden, dass der Verbindungsaufbau über das Protokoll DHCP hergestellt wird. Das Protokoll versieht seine Aufgabe in der Verwaltung von IP-Adressen und der Verteilung in einem Netzwerk [57]. Der DHCP Server ist im Router implementiert. Die folgenden Nummerierungen aus der Tabelle '4.10 TP-Link AC1200 Mesh Wi-Fi Router - Paketversand RAM-Sicherung' bezeichnen dabei folgenden Inhalt: Nr. 1 enthält neben den in Tabelle '4.10 TP-Link AC1200 Mesh Wi-Fi Router - Paketversand RAM-Sicherung' ermittelten Angaben weitere Konfigurationsparameter. Unter anderem wird seitens des Teilnehmers das 'DHCPDISCOVER' Paket an den DHCP Server gesandt. In diesem teilt der Teilnehmer dem DHCP Server seine MAC-Adresse mit dem aktuellen Zeitstempel aus Datum und Uhrzeit mit. Der Teilnehmer erwartet eine ihm zugeteilte IP-Adresse. Die dem Teilnehmer zugeteilte IP-Adresse wird in dem Paket 'DHCPOFFER' von dem DHCP Server an den Teilnehmer mit weiteren Konfigurationsparametern übertragen. Weiter werden in dem Paket die Werte der MAC-Adresse einschließlich dem aktuellen Zeitstempel aus Datum und Uhrzeit übermittelt. In Nr. 6 erfolgt durch den Teilnehmer der Versand des Datenpaketes mit einem 'DHCPREQUEST'. In diesem quittiert der Teilnehmer dem DHCP Server die gewählte IP-Adresse des Teilnehmers. Weiter im 'DHCPREQUEST' des Teilnehmers wird die MAC-Adresse des Gerätes einschließlich dem aktuellen Zeitstempel aus Datum und Uhrzeit übertragen. Der DHCP Server antwortet mit

einem 'DHCPACK' Datenpaket an den Teilnehmer. In dem Datenpaket werden die Werte der IP-Adresse des Teilnehmers, dessen MAC-Adresse sowie dem Zeitstempel aus Datum und Uhrzeit bestätigt. Der Datentransfer wird mit dem ACK Datenpaket des DHCP Servers beendet [58]. Weder die Daten aus dem versuchten Anmeldevorgang, noch der DHCP Datenpakettransfer, konnten in der Dateibaumstruktur aufgefunden werden.

4.3.8.3 'Config List'

Im Bezug auf den Dateninhalt der 'Config List' kann dieser in der RAM-Datensicherung festgestellt werden. Die Datei selbst kann in der Dateibaumstruktur unter dem Dateipfad '/etc/config/history_list' ermittelt werden. Die Schreibweise der MAC-Adresse wird in der Form 'xxxxxxxxxxxx' geführt.

Die 'Config List' enthält alle Geräte, welche sich seit der Inbetriebnahme mit dem Router verbunden haben. Diese Informationen sind persistenter Natur, bleiben folglich über einen Neustart bzw. einer Stromunterbrechung hinweg erhalten. Bei der Führung dieser Informationen werden keine Zeitdaten gespeichert. Die Ablage erfolgt in der Form:

option mac '*'	MAC-Adresse
option hostname '*'	Gerätename
option access_host '*'	Zugriffsberechtigung

Tabelle 4.11: TP-Link AC1200 Mesh Wi-Fi Router - Aufbau 'Config List'

Ein Screenshot zur visuellen Einsicht kann der Anlage 'S TP-Link AC1200 Mesh Wi-Fi Router - Aufbau 'Config List" entnommen werden.

4.3.8.4 'Config White_List'

Im Bezug auf den Dateninhalt der 'Config White_List' kann dieser in der RAM-Datensicherung festgestellt werden. Die Datei selbst kann in der Dateibaumstruktur unter dem Dateipfad '/etc/config/access_control' ermittelt werden. Die Schreibweise der MAC-Adresse wird in der Form 'xx:xx:xx:xx:xx:xx' geführt.

Die 'Config White List' enthält alle Geräte, welche über die Berechtigungsvoraussetzungen, sich mit dem Router verbinden zu dürfen, verfügen. Diese Informationen sind persistenter Natur, bleiben folglich über einen Neustart bzw. einer Stromunterbrechung hinweg erhalten. Bei der Führung dieser Informationen werden keine Zeitdaten gespeichert. Die Ablage erfolgt in der Form:

option real_mac '*'	MAC-Adresse
option mac '*'	MAC-Adresse
option name '*'	Gerätename

Tabelle 4.12: TP-Link AC1200 Mesh Wi-Fi Router - Aufbau 'Config White List'

Ein Unterschied zwischen der 'real-MAC'-Adresse und der 'MAC'-Adresse ist nicht bekannt. Beide Adressen sind stets identisch. Auch randomisierte MAC-Adressen weisen keinen Unterschied auf. Ein Screenshot zur visuellen Einsicht kann der Anlage 'T TP-Link AC1200 Mesh Wi-Fi Router - Aufbau 'Config White List" entnommen werden.

4.3.8.5 'Client List'

Im Bezug auf den Dateninhalt der 'Client List' kann dieser in der RAM-Datensicherung festgestellt werden. Die Datei selbst kann in der Dateibaumstruktur unter dem Dateipfad '/tmp/client_list.json' ermittelt werden. Die Schreibweise der MAC-Adresse wird in der Form 'xx-xx-xx-xx-xx-xx' geführt.

Die 'Client List' enthält alle Geräte, welche sich aktuell mit dem Router verbunden haben. Diese Informationen sind flüchtiger Natur. Sie gehen zum einem über einen Neustart bzw. einer Stromunterbrechung verloren, zum anderen werden die Informationen bereits vom System aktualisiert, sobald ein Endgerät nicht mehr mit dem Router verbunden ist. Bei der Führung dieser Informationen werden die letzten Log-in Zeitdaten gespeichert. Die Ablage erfolgt in der Form:

{"XX-XX-XX-XX-XX-XX":{	Beginn eines Engderätes
"MAC": "XX-XX-XX-XX-XX-XX";	MAC-Adresse
"hostname":"*",	Gerätename
"name":"*",	Gerätename
"config_proxy_MAC":"XX-XX-XX-XX-XX-XX",	MAC-Adresse
access_time":1685617735,	UNIX-Zeitstempel GMT +02:00 letzter Log-in
"guest":"NON_GUEST",	Status im Netzwerk
"wire_type":"5G",	Verwendetes Frequenzband
"IP":"192.168.0.XXX"}	IP-Adresse

Tabelle 4.13: TP-Link AC1200 Mesh Wi-Fi Router - Aufbau 'Client List'

Ein Screenshot zur visuellen Einsicht kann der Anlage 'U TP-Link AC1200 Mesh Wi-Fi Router - Aufbau 'Client List" entnommen werden.

4.3.8.6 'DHCP Leases List'

Im Bezug auf den Dateninhalt der 'DHCP Leases List' kann dieser in der RAM-Datensicherung festgestellt werden. Die Datei selbst kann in der Dateibaumstruktur unter dem Dateipfad '/tmp/dhcp.leases' ermittelt werden. Die Schreibweise der MAC-Adresse wird in der Form 'xx:xx:xx:xx:xx:xx' geführt.

Die 'DHCP Leases List' enthält alle Geräte, welche sich aktuell mit dem Router verbunden haben. Diese Informationen sind flüchtiger Natur. Sie gehen zum einem über einen Neustart bzw. einer Stromunterbrechung verloren, zum anderen werden die Informationen bereits vom System aktualisiert, sobald ein Endgerät nicht mehr mit dem Router verbunden ist. Bei der Führung dieser Informationen werden keine Log-in Zeitdaten gespeichert. Die Ablage erfolgt in der Form:

MAC-Adresse	IP-Adresse	Gerätename	MAC-Adresse

Tabelle 4.14: TP-Link AC1200 Mesh Wi-Fi Router - Aufbau 'DHCP Leases List'

Ein Screenshot zur visuellen Einsicht kann der Anlage 'V TP-Link AC1200 Mesh Wi-Fi Router - Aufbau 'DHCP Leases List" entnommen werden.

4.3.8.7 Auswertung Zeiten

Der Router wurde über einen Zeitraum vom sieben Tagen am Netzbetrieb belassen. Während dieser Zeit herrschte normaler Netzwerkverkehr. Nach Ablauf der sieben Tage erfolgte eine Sicherung des RAM Speicherinhaltes. Die Auswertung der RAM Sicherung unter Bezug auf die dort befindlichen Zeitstempel konnte als ältesten Zeitstempel den des Analysebeginns aufzeigen. Der Zeitpunkt der ersten Anmeldung am Router wird mit 'access_time' benannt. Die Zeit selbst wird in der Form 'time_t 32 (bit)' im Big Endian Format abgelegt. Die Zeitangabe belegt 4 Byte und wird in UTC/GMT hinterlegt. Die Datei selbst konnte in der Dateibaumstruktur nicht ermittelt werden. Die Schreibweise der MAC-Adresse wird in der Form 'xx-xx-xx-xx-xx-xx' geführt. Die Ablage erfolgt in der Form:

Nickname	Gerätename
Hostname	Gerätename
IP	IP-Adresse
MAC	MAC-Adresse
wire_type	verwedetes Frequenzband
guest	Teilnehmerstatus
device_type	Gerätetyp
access_time	Zeitpunkt der Anmeldung

Tabelle 4.15: TP-Link AC1200 Mesh Wi-Fi Router - Auswertung Zeiten [Erstanmeldung]

Eine Ansicht kann der Grafik 'X TP-Link AC1200 Mesh Wi-Fi Router - TFTP-Datensicherung Hexansicht 'access time' entnommen werden.

Zu dem Zeitpunkt der letzten Anmeldung am Router können neben der 'Client List' weiterführende Informationen zum Auf- und Abbau der Verbindung entnommen werden. Diese können sowohl live an der Konsole über Putty als auch aus der RAM Datensicherung entnommen werden. So wird der Verbindungsaufbau mit seinem Paketaustausch zum Router aufgezeigt. Neben diesem können Informationen abgelesen werden, wenn sich das Gerät in Reichweite befunden bzw. wenn ein Frequenzbandwechsel stattgefunden hat. Dieser Verkehr wird als 'is triggered by activity' im RAM-Speicher notiert. Sobald das Gerät sich außer Reichweite befindet, kann dies an der Notation 'become inactivity because 'X' second's idle' entnommen werden. Die Abmeldung vom Router erfolgt unter dem Hinweis 'IEEE 802.11: disassociated'. In der Testumgebung konnte erkannt werden, dass die Informationen bereits bei im Nebenraum befindlichen Endgeräten ausgelöst werden. Dies kann wie unter Punkt '2.3.5 Sendeleistung und Reichweite WLAN' benannt, in der baulichen Beschaffung des Gebäudes seine Gründe finden. Die Datei selbst konnte in der Dateibaumstruktur nicht ermittelt werden. Die Schreibweise der MAC-Adresse wird in der Form 'xx:xx:xx:xx:xx:xx' geführt. Die Ausgabe erfolgt in der Form:

<daemon.info> hostapd:	Informationsbeginn
ath1:	Verbindung
STA MAC	MAC-Adresse
IEEE 802.11:	verwendeter Standard
disassociated	Verbindung getrennt
YYYY-MM-TT HH:MM:SS	Zeitstempel Jahr-Monat-Tag Stunde:Minute:Sekunde

Tabelle 4.16: TP-Link AC1200 Mesh Wi-Fi Router - Auswertung Zeiten [Abmeldung]

5 Ergebnisse

Nachfolgend werden die Ergebnisse der analysierten Router 'Vodafone Station Arris TG3442DE' und 'TP-Link AC1200 Mesh Wi-Fi Router' zusammengefasst. Zunächst erfolgt eine Zusammenfassung zum jeweiligen Modell, danach erfolgt ein Vergleich beider Router und deren Analyseergebnisse. Abschließend wird ein Ausblick betrachtet.

5.1 Vodafone Station Arris TG3442DE

Das Modell 'Station Arris TG3442DE' von Vodafone lässt eine Sichtung von Daten in der grafischen Benutzeroberfläche zu. Der Inhalt der Daten im Bezug zu seinem forensischen Nutzen ist überschaubar. Daten mit zeitlichen Abfolgen, wann sich welche Geräte mit dem Router verbunden und die Verbindung wieder getrennt haben, können der grafischen Benutzeroberfläche nicht entnommen werden. Zeitliche Abfolgen, wann sich Geräte mit dem Router verbunden haben, können jedoch dem Ereignisprotokoll entnommen werden. Dieses steht über die grafische Benutzeroberfläche zum Download zur Verfügung. Für den Zugang zur grafischen Benutzeroberfläche wird ein Passwort benötigt. Daten der grafischen Benutzeroberfläche können in der Regel fast ausschließlich eingesehen werden. Ein Download steht lediglich mit dem Ereignisprotokoll bereit. Diese sind nur begrenzt von forensischem Nutzen.

Final kann die Analyse des Routers 'Vodafone Station Arris TG3442DE' als sehr umfangreich betrachtet werden. Übliche Schnittstellen werden nicht unterstützt. Softwareseitige Schwachstellen wurden behoben [59]. Ein Zugriff auf die flüchtige Datenbasis ist ausgeschlossen. Eine Datenextraktion über die Leiterplatine nicht umsetzbar. Andere Modelle desselben Herstellers weisen in demselben Erscheinungsjahr unterschiedlich implementierte Schnittstellen auf (Arris DG3450 [60], Arris TG3452 [35]). Der Vergleich der Leiterplatine mit einem anderen Modell der Herstellerreihe zu unterschiedlich implementierten Schnittstellen zeigt auf, dass eine Neubegutachtung von Routern untereinander durchgeführt werden sollte. Entscheidende Faktoren können an unterschiedlich vorliegenden Firmwareversionen begründet werden.

Dass die UART Schnittstelle nicht bedient werden kann, kann auf unterschiedlichen Faktoren beruhen. Möglich ist ein Fehlen weiterer benötigter Hardwaremodule. Kondensatoren oder Widerstände stellen nur eine gering benannte Auswahl dar. Aber auch eine softwareseitige Deaktivierung der UART Schnittstelle im BIOS ist möglich [40]. Nicht bekannt sind die transferierenden Signale, welche von dem Prozessor zur UART Schnittstelle führen müssen. Eine Lokalisation der UART-führenden Leiterbahnen konnte bei der Überprüfung zu Punkt '4.2.6.1 Vodafone Station Arris TG3442DE - Versuch Möglichkeit 1' nicht ermittelt werden. Für die definierte Lokalisierung wird ein Datenblatt für die Leiterplatine und den Prozessor benötigt. Diese standen nach durchgeführter Recherche nicht zur Verfügung.

Zusammenfassend können zu den Datensicherungsmöglichkeiten folgende Erkenntnisse benannt werden:

5.1.1 Flüchtige Datenbasis

Auf der grafischen Benutzeroberfläche ist die flüchtige Datenbasis vorrangig bei verbundenen Endgeräten zu finden. Als einzig downloadbare Datei ist das Ereignisprotokoll zu benennen. Wie unter Punkt '4.2.2 Vodafone Station Arris TG3442DE - Grafische Benutzeroberfläche' benannt, werden in diesem die ältesten Einträge von den neuesten überschrieben.

5.1.1.1 Möglichkeiten der Live-Forensik

Eine Auswertung der Datenbasis über die grafische Benutzeroberfläche ist möglich. Bleibt das Gerätepasswort unbekannt sind zerstörungsfreie Möglichkeiten zur Gewinnung von Daten über die Leiterplatine nicht vorhanden. Der Informationsgewinn über die grafische Benutzeroberfläche stellt sich wie folgt dar: auf der Hauptseite ist unter dem Reiter 'Übersicht' ein erster Überblick über die wichtigsten Informationen dargestellt. Diese werden nicht mit einem Zeitstempel versehen. Die Nachvollziehbarkeit von Verbindungen mit Endgeräten ist nicht gegeben.

Die Flüchtige Datenbasis ist unter Punkt '4.2.2.1 Vodafone Station Arris TG3442DE - Flüchtige Datenbasis' benannt. Zusammenfassend befindet sich die Laufzeit des Gerätes, eine tabellarische Übersicht der Geräte aus der DHCP Geräteliste, sowie das Ereignisprotokoll im flüchtigen Datenbestand. Die Geräte aus der DHCP Geräteliste weisen keine Log-in bzw. Log-out Daten auf. Zeitstempel für das Einloggen eines Gerätes werden im Ereignisprotokoll geführt. Die Beständigkeit von Telefoniedaten, einschließlich der Anrufhistorie, kann nicht beurteilt werden. Während des Analysezeitraumes wurden keine Daten zu diesem Bereich generiert und lagen somit für eine folgende Analyse nicht vor.

5.1.2 Persistente Datenbasis

Persistente Datenbasis ist über die grafische Benutzeroberfläche hauptsächlich in den Konfigurationsdaten anzutreffen.

5.1.2.1 Möglichkeit der Post-Mortem-Forensik

Das Ereignisprotokoll speichert über die Stromentnahme hinweg eine kleine Menge an gewonnener Datenbasis. Mit dem Neustart werden neue Events geschrieben. Diese überschreiben die ältesten Einträge. Nach einem Neustart des Gerätes ist mit Datenverlust des Ereignisprotokolls zu rechnen.

Mittels der zerstörungsverursachenden Entfernung des Flash Datenspeichers von der Leiterplatine können die Log-in und Log-out Zeitstempel aller Geräte, auch über die Stromentnahme hinweg, verzeichnet werden. Über den Analysezeitraum können alle Daten als Klartext in der Datensicherung aufgefunden werden. Der Analysezeitraum betrug final 15 Tage.

5.1.3 Präventivmaßnahmen

Für datensichernde Maßnahmen muss unter dem Punkt

Internet → Port-Forwarding

beachtet werden, dass ein Löschen der Datenbasis im Fernzugriff durch setzen der Werkseinstellungen ermöglicht wird. Es sind Präventivmaßnahmen einzuleiten. Dies kann durch Entfernen des WAN-Kabels geschehen.

5.1.4 Zusammenfassung

Nach Beenden der Analyse des Routers können die zu Beginn im Punkt '1 Einleitung' benannten Fragestellungen wie folgt beantwortet werden:

Mögliche Spuren können in einem 'Vodafone Arris TG3442DE' auf der grafischen Benutzeroberfläche, dem Ereignisprotokoll und dem Flash Speicher vorgefunden werden.

Es können Informationen im Bereich der Telefonie aufgefunden werden. Eine Kontaktliste wird gepflegt. Diese ist auf der grafischen Benutzeroberfläche einsehbar. Mediaserver oder diverse USB Geräte können für einen Datentransfer im Netzwerk vorhanden sein. Diese können als Speichergeräte oder NAS-Netzwerkspeicher an den Router angeschlossen werden. Netzwerkdaten können dem Ereignisprotokoll entnommen werden. Dies stellt die einzig downloadbare Logdatei dar. Der Logdatei können Events auch zu verbundenen bzw. registrierten Geräten entnommen werden. Eine Lease-Liste wird auf der grafischen Benutzeroberfläche geführt. Diese beinhaltet die für die jeweiligen Endgeräte zugehörigen IP- und MAC-Adressen. Netzwerkverbindungen, Netzwerkstatus, Prozesse und Umgebungsvariablen können über die grafische Benutzeroberfläche nicht eingesehen werden. Das Ereignisprotokoll führt hierzu keine Datenablage. Eine Portfreigabe für den seriellen Datentransfer ist nicht vorhanden. Daten zu dem Betriebssystem oder dem Dateisystem konnten nicht ermittelt werden. Die Systemzeit kann der grafischen Benutzeroberfläche entnommen werden. Für die Nachvollziehbarkeit der Zeitstempel ist die Gerätezeit mit denen einer vergleichbaren Zeitquelle zu überprüfen.

Endgeräte, welche sich am Tattag mit dem dortigen WLAN-Router verbunden haben, können auch über die grafische Benutzeroberfläche Post-Mortem eingesehen werden. Das Zeitfenster hierzu ist überschaubar und kann mitunter wenige Stunden betragen. Für eine größtmögliche Datenbasis potentiell wichtiger Daten ist ein zeitnaher Abzug der Daten durchzuführen. Eine weitere Möglichkeit stellt den Datenabzug des Flash-Speichers mittels der Chip-Off Methode dar. Hier kann eine Speicherung der Daten über mindestens 15 Tage verzeichnet werden.

Endgeräte, welche sich aus dem Umkreis des WLAN Bereiches von diesem entfernt haben, konnten in den Analysen nicht ermittelt werden. Log-out Daten können der grafischen Benutzeroberfläche nicht entnommen werden. Frequenzbandwechsel der Geräte werden verzeichnet. Hierzu erfolgt ergänzend die Angabe eines Zeitstempels.

Hinweise darüber, dass sich Endgeräte an der Tatörtlichkeit befunden haben ohne eine Registrierung mit dem WLAN-Router beabsichtigt zu haben, werden weder auf der grafischen Benutzeroberfläche noch in dem Ereignisprotokoll oder der Datenextraktion des Flash-Speichers aufgezeigt. Endgeräte, welche sich ohne Erfolg mit dem WLAN-Router verbinden wollten, können nicht entnommen werden.

Für die Herangehensweise der forensischen Datensicherung sind ergänzend folgende Erkenntnisse festzuhalten:

Der WLAN-Router kann für eine forensische Analyse im Labor als Asservat von der Örtlichkeit entnommen werden. Bei dieser Vorgehensweise ist über die grafische Benutzeroberfläche jedoch mit Datenverlusten zu rechnen. Des weiteren wird hierfür das Passwort der grafischen Benutzeroberfläche benötigt. Es kann festgestellt werden, dass ein Stromverlust zu einem Verlust der Datenbasis der Logdatei führt. Die Analyse des physischen Speicherbereiches des Flash-Speichers kann mittels Datenaufbereitung durchgeführt werden. Mittels dieser Methode kann der größte Erkenntnisgewinn zu Verbindungsdaten aller Geräte verzeichnet werden. Es haben sich keine Schnittstellen aufzeigen können, unter welchen eine Datenextraktion flüchtiger Datenbasis durchgeführt werden kann. Eine Ausleitung der Daten über die Leiterplatine kann nicht realisiert werden. Sachverhaltsbezogene Daten können von der grafischen Benutzeroberfläche, dem Ereignisprotokoll oder der Datenextraktion des Flash-Speichers entnommen werden. Der größtmögliche Gewinn von Daten kann über die Chip-Off Methode des Flash-Speichers erzielt werden.

5.2 TP-Link AC1200 Mesh Wi-Fi Router

Das Modell 'AC1200 Mesh Wi-Fi Router' von TP-Link lässt eine Sichtung von Daten in der grafischen Benutzeroberfläche zu. Der Inhalt der Daten im Bezug zu seinem forensischen Nutzen ist überschaubar. Daten mit zeitlichen Abfolgen, wann sich welche Geräte mit dem Router verbunden und die Verbindung wieder getrennt haben, können der grafischen Benutzeroberfläche nicht entnommen werden. Zeitliche Abfolgen, wann sich Geräte mit dem Router verbunden haben, können jedoch dem System-Log entnommen werden. Dieses steht über die grafische Benutzeroberfläche zum Download zur Verfügung. Für den Zugang zur grafischen Benutzeroberfläche wird ein Passwort benötigt. Daten der grafischen Benutzeroberfläche können in der Regel fast ausschließlich eingesehen werden. Ein Download steht lediglich bei den System-Log Daten bereit. Diese sind nur begrenzt von forensischem Nutzen.

Zusammenfassend können zu den Datensicherungsmöglichkeiten folgende Erkenntnisse benannt werden:

5.2.1 Flüchtige Datenbasis

Flüchtige Datenbasis ist vorrangig bei Verbindungsdaten von Endgeräten zu finden. Als einzig downloadbare Datei ist das System-Log zu benennen. Dieses unterliegt einem Ringspeicher. Wie unter Punkt '4.3.2 TP-Link AC1200 Mesh Wi-Fi Router - Grafische Benutzeroberfläche' benannt, werden in diesem die ältesten Einträge von den neuesten überschrieben. Die Datenablage folgt somit dem First-in-first-out Prinzip. Die Ablage kann bei wenig Datenaufkommen über einen Tag hinausgehen, bei hohem Datenaufkommem jedoch auch nur eine kleine Zeitspanne betragen. Die Dateigröße von bis zu 18 kB erlaubt lediglich das Ablegen einer geringen Datenmenge.

5.2.1.1 Möglichkeiten der Live-Forensik

Eine Auswertung der Datenbasis über die grafische Benutzeroberfläche ist möglich. Bleibt das Gerätepasswort unbekannt kann eine Datenextraktion an der Leiterplatine über die serielle Schnittstelle UART anvisiert werden. Die Durchsicht des im Punkt '4.3.8 TFTP' benannten gesicherten Datenbestandes lässt zunächst unter dem Hexeditor 'HxD' erkennen, dass der Datenbereich '/dev/mem' aus einer Mischung von Klartext und Hex-codierten Datenbereichen besteht. Dieser ist mit Abschnitten von Programmcode und mehreren Wiederholungen gekennzeichnet. Im Rahmen der Analyse konnte am Referenzmodell festgestellt werden, dass sich die Eingaben an der grafischen Benutzeroberfläche und am Konsolenzugang der UART Schnittstelle im Speicherabbild des flüchtigen Speichers wiederfinden lassen. Aufgrund der geringen Speichergröße von 128 MiB ist ein Überschreiben von bereits bestehenden Daten wahrscheinlich. Welche Daten überschrieben werden, kann nicht ermittelt werden. Für eine Datensicherung des flüchtigen Speichers der Ordnerstruktur '/dev/mem' ist von vorherigen Eingaben abzusehen. Nach erfolgter Sicherung kann eine freie Navigation und Sicherung weiterer Daten am System vorgenommen werden. So können Informationen mit forensischem Wert den Dateipfaden aus folgender Tabelle entnommen werden:

Dateipfad	Dateiinhalt
tmp/client_list.json	Anzeige aktuell verbundene Geräte mit letzten Zeitstempel
tmp/resolv.conf	vorgeschaltetes Netzwerkgerät
etc/TZ	aktuelle Zeitzone
tmp/cloud_service.cfg	Hinweise zum Videoüberwachungssystem
tmp/dhcp.leases	Auflistung der aktuellen Geräte
etc/config/access_control	Auflistung aller berechtigter Geräte
etc/config/history_list	Auflistung aller bekannter Geräte
ntp_time_set	In Betrieb seit
tmp/productinfo	Geräteinformation

Tabelle 5.1: TP-Link AC1200 Mesh Wi-Fi Router - Dateipfade mit forensischen Inhalten

Das Analysemodell agiert als AP. Da es sich bei diesem um ein Gerät ohne integriertes Modem handelt muss ein weiteres Gerät im Netzwerk existent sein. Dies kann in Form eines eigenständigen Modems, aber auch eines Routers mit integriertem Modem sein. Netzwerksniffingtools wie 'WiGLE' können weiterführende Erkenntnisse über ein möglicherweise angebundenes Gerät im Netzwerk liefern. Mittels Konsolenzugang über die UART Schnittstelle kann wie in der Abbildung '5.1 TP-Link AC1200 Mesh Wi-Fi Router - Verbundene Router' ein vorgeschaltetes Netzwerkgerät in der Datei '/tmp/resolv.conf' ermittelt werden.

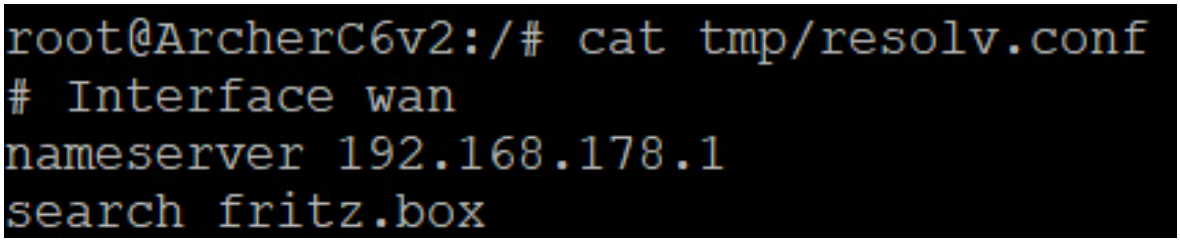

Abbildung 5.1: TP-Link AC1200 Mesh Wi-Fi Router - Verbundene Router

5.2.2 Persistente Datenbasis

Daten mit forensisch wertvollen Inhalten, die im Kontext zu strafrechtlich relevanten Sachverhalten stehen, gehen mit der Stromunterbrechung verloren. Persistente Datenbasis ist hauptsächlich in den Konfigurationsdaten anzutreffen.

5.2.3 Darstellungsformen verschiedener Suchmarker

Während der Analyse konnten zu verschiedenen Suchmarkern verschiedene Darstellungsformen erkannt werden. Die verschiedenen Formen sollten bei einer manuellen Durchschau bedacht werden.

5.2.3.1 Schreibweisen von MAC-Adressen

Bei der Durchsicht der RAM Sicherung mithilfe des Hexeditors 'HxD' konnten mehrere Varianten der Schreibweise zur MAC-Adresse verzeichnet werden. Hierbei erfolgt eine unterschiedliche Trennung der einzelnen Bytewerte. Die folgende Tabelle zeigt die einzelnen Möglichkeiten auf:

Schreibweise	Bezug
'xx-xx-xx-xx-xx-xx'	access_time time_t 32 (bit) Big Endian, 4 Byte Zeitpunkt der ersten Anmeldung am Router
'xxxxxxxxxxxx'	RAM Inhalt, nicht zu interpretieren 'Config List'
'xx:xx:xx:xx:xx:xx'	Zeitpunkt der letzten Anmeldung am Router

Tabelle 5.2: TP-Link AC1200 Mesh Wi-Fi Router - Schreibweisen von MAC-Adressen

5.2.3.2 Schreibweisen von IP-Adressen

Bei der Durchsicht der RAM Sicherung mithilfe des Hexeditors 'HxD' konnten mehrere Varianten der Schreibweise zur IP-Adresse verzeichnet werden. Hierbei erfolgt eine unterschiedliche Trennung der einzelnen Werte. Die Tabelle '5.3 TP-Link AC1200 Mesh Wi-Fi Router - Schreibweisen von IP-Adressen' zeigt die einzelnen Möglichkeiten auf.

Schreibweise	Bezug
'XX XX XX XX'	Hexadezimal, Interpretation byteweise bsp. C0 A8 00 BC → 192.168.0.188 flüchtiger Datenbestand
'XXX.XXX.XXX.XXX'	Binär, bsp. 192.168.0.188
XXXX	UInt8 (unsigned Integer 8 Byte), Übersetzung byteweiße bsp. À¨ ¼ → 192.168.0.188

Tabelle 5.3: TP-Link AC1200 Mesh Wi-Fi Router - Schreibweisen von IP-Adressen

Schreibweise	Bezug
access_time	time_t 32 (bit) Big Endian, Länge: 4 Byte
access_time	Unix Zeitstempel
access_time	Human Time

Tabelle 5.4: TP-Link AC1200 Mesh Wi-Fi Router - Schreibweisen von Zeiten

5.2.3.3 Schreibweisen von Zeiten

Bei der Durchsicht der RAM Sicherung mithilfe des Hexeditors 'HxD' konnten mehrere Varianten der Schreibweise zu den Zeiten verzeichnet werden. Hierbei erfolgt eine unterschiedliche Darstellung der einzelnen Werte. Die Tabelle '5.4 TP-Link AC1200 Mesh Wi-Fi Router - Schreibweisen von Zeiten' zeigt die einzelnen Möglichkeiten auf:

Es kann notiert werden, dass der Punkt 'access_time & time_t 32 (bit) Big Endian' als einziger Datenbestand im Big Endian verzeichnet werden kann. Weitere Datenbasis wird im Little Endian geführt.

5.2.4 Präventivmaßnahmen

Mit der Option der Konfiguration des Remote Zugangs besteht die Möglichkeit, Daten per Fernzugriff vor Datensicherungsmaßnahmen zu löschen. Eine Nachschau unter dem Reiter

System Tools → Administration → Remote Management

sollte durchgeführt werden.

Wie unter Punkt '4.3.2 Grafische Benutzeroberfläche' erwähnt, ist die Möglichkeit, dass ein Videoüberwachungssystem eingebunden wurde, vorhanden. Sollte die Bedienung der grafischen Benutzeroberfläche nicht möglich sein, kann unter dem Dateipfad '/tmp/cloud_service.cfg' erkannt werden, ob hierzu ein Account erstellt und Geräte hinzugefügt wurden. Ein Auszug des Dateiinhaltes ist unter dem Punkt 'W TP-Link AC1200 Mesh Wi-Fi Router - Möglich angebundene Speichergeräte (Cloud)' einsehbar. Weiterführende Informationen konnten aufgrund fehlender Verknüpfungen am Analysemodell nicht ermittelt werden.

Es sind Präventivmaßnahmen einzuleiten. Dies kann durch Entfernen des WAN-Kabels geschehen.

5.2.5 Zusammenfassung

Nach Beenden der Analyse des Routers können die zu Beginn im Punkt '1 Einleitung' benannten Fragestellungen wie folgt beantwortet werden:

Mögliche Spuren können in einem 'TP-Link AC1200 Mesh Wi-Fi Router' auf der grafischen Benutzeroberfläche, dem System-Log und der seriellen Schnittstelle UART vorgefunden werden.

Auf der grafischen Benutzeroberfläche steht der Download eines System-Logs zur Verfügung. Aus diesem können Events zu verbundenen bzw. registrierten Geräten entnommen werden. Lease-Listen werden auf der grafischen Benutzeroberfläche und im Dateisystem geführt. Die Speicherung beinhaltet für die jeweiligen Endgeräte neben den IP-Adressen die zugehörigen MAC-Adressen. Zeitstempel werden nicht geführt. Die Ablage erfolgt aktuell. Hinweise zu Netzwerkverbindungen, dem Netzwerkstatus, Prozessen und den Umgebungsvariablen können über die UART Schnittstelle der Dateisystemstruktur entnommen werden. Über den Bootloader können Erkenntisse zu dem Betriebssystem und dem Dateisystem gewonnen werden. Es empfiehlt sich diesen Prozess als letzten durchzuführen, wenn die Datensicherungsphase abgeschlossen ist. Die Systemzeit kann in der Dateisystemstruktur eingesehen werden.

Eine Datensicherung forensisch relevanter Daten, welche im Kontext zu strafrechtlich relevanten Sachverhalten stehen, können bei dem Modell des TP-Links über die Leiterplatine unter Verwendung der UART-Schnittstelle extrahiert werden. Als Datensicherungsmethode eignet sich das Protokoll 'TFTP'. Der Linuxbefehl 'dd' kann für eine Datensicherungsmethode nicht verwendet werden. Dies beruht auf der Tatsache, dass Speichermedien an das Analysegerät nicht angeschlossen werden können. Eine Datensicherung auf dem laufenden System stellt aufgrund der schreibenden Prozesse am System keine Option dar. Neben diesem sind den Speichergrößen des Analysgerätes Grenzen gesetzt, was eine Sicherung, ungeachtet der ausgeführten Schreibprozesse, eingeschränkt ausführbar lässt. Es kann festgehalten werden, dass an dem Analysemodell endgerätbezogene Zeitstempel lediglich über die RAM Sicherung der seriellen Schnittstelle UART gewonnen und extrahiert werden können. Eine Auflistung aufeianderfolgender Log-in und Log-out Zeiten erfolgen weder in der grafischen Benutzeroberfläche noch in der Ablage des Dateisystems. Mit dem Abzug des RAM Speichers kann eine Chronologie bis zu einem gewissen Zeitrahmen durch Events erstellt werden. Je kleiner das Analysezeitraumfenster ist, desto höher sind die Chancen auf vorliegende Datenbasis. Für den Tattag ist eine Auflistung der verbundenen Geräte mit dem dortigen WLAN-Router möglich. Wann sich Endgeräte aus dem Umkreis des WLAN Bereiches von diesem entfernt haben, kann der RAM Sicherung entnommen werden. Eine Auflistung in der Datenbasis erfolgt nicht. Erkenntnisse darüber, dass sich Endgeräte an der Tatörtlichkeit befunden haben, ohne eine Registrierung mit dem WLAN-Router beabsichtigt zu haben, konnten nicht erlangt werden. Es liesen sich keine Hinweise im RAM Speicher, der Dateisystemstruktur oder der Konsolenmitteilungen erkennen. Endgeräte, welche sich ohne Erfolg mit dem WLAN-Router zu verbinden versuchten, können in der RAM Sicherung festgestellt werden. Eine Einsichtnahme auf der grafischen Benutzeroberfläche oder der Dateisystemstruktur ist nicht möglich.

Zeitstempel für den Beginn der aktuell aktiven Verbindung werden in der grafischen Benutzeroberfläche nicht angezeigt. Diese können der Dateisystemstruktur über die UART Schnittstelle entnommen werden. Daten mit Bezug zu Geräten stellen durchweg flüchtige Daten dar. Neben diesem können Informationen im RAM Speicherabbild abgelesen werden, wenn sich das Gerät in Reichweite befunden bzw. wenn ein Frequenzbandwechsel stattgefunden hat. Weitere Ports für einen Datentransfer sind nicht freigegeben.

Für die Herangehensweise der forensischen Datensicherung wird empfohlen, den WLAN-Router im eingeschalteten Zustand zu belassen. Es besteht die Möglichkeit der forensischen Analyse an der Örtlichkeit durch konnektieren der UART Schnittstelle. Weitere Schnittstellen stehen für ein Ansprechen nicht zur Verfügung. Es können sowohl in den Speicherbereichen des Dateisystems als auch der RAM Datensicherung sachverhaltsbezogene Daten vorgefunden werden. Einige Informationen

der RAM Sicherung konnten in der Dateisystemstruktur nicht aufgefunden werden. Umso wichtiger erscheint ein zügiges Abbild des RAM Speichers. Sollte der WLAN-Router für eine forensische Analyse im Labor als Asservat von der Örtlichkeit entnommen worden sein, ist lediglich eine Sicherung der Konfigurationsdaten möglich.

5.3 Fazit

Die gewählten Geräte zeigen deutlich welche Hürden die Analyse von WLAN Routern aufweisen können. Eine UART Schnittstelle kann eine serielle Verbindung mit dem Gerät herstellen, wodurch das Ausleiten von Daten möglich ist. Ist mit der Analyse des Routers 'TP-Link AC1200 Mesh Wi-Fi Router' eine Analyse der Datenbasis auf dem Gerät und des flüchtigen Speicherinhaltes im RAM gut durchführbar, so gestaltet sich die Untersuchung des 'Vodafone Station Arris TG3442DE' schwieriger. Innerhalb dieser Arbeit sind Ansatzpunkte untersucht worden, unter welchen ein Zugriff auf die Datenbasis möglich erscheinen kann. Diese stellen hier verstärkt die seriellen Schnittstellen dar. Für die Extraktion relevanter Daten muss zunächst festgelegt werden, welche Daten im konkreten Sachverhalt von Interesse sind und in welchem Bereich der Verfügbarkeit sich diese befinden. Es ist die methodische Vorgehensweise zu strukturieren, um systematisch eine Datensicherung durchführen zu können.

Zu den anfangs geführten Fragestellungen der forensischen Analyse lässt sich die Gegensätzlichkeit beider gewählter WLAN Router erkennen. Kann zu dem 'TP-Link AC1200 Mesh Wi-Fi Router' die Fragestellung, welche Endgeräte sich am Tattag mit dem dortigen WLAN-Router verbunden haben, wann sich diese aus dem Umkreis des WLAN Bereiches von diesem entfernt haben und ob es Endgeräte gibt, welche sich ohne Erfolg mit dem WLAN-Router zu verbinden versuchten, über die Datensicherung durch konnektieren der UART Schnittstelle mit einem positiven Ergebnis im Bereich der flüchtigen Datenbasis verzeichnet werden, kann diese zu dem 'Vodafone Station Arris TG3442DE' durch das Auslesen des Flash Speichers mittels der Chip-Off Methode im persistenten Speicher beantwortet werden. Beiden gemein ist die Tatsache des Auffindens der gesuchten Datenbasis. Hinweise zu den Fragestellungen, ob Aussagen darüber getroffen werden können, dass sich Endgeräte an der Tatörtlichkeit befunden haben ohne eine Registrierung mit dem WLAN-Router beabsichtigt zu haben, konnten bei beiden Geräten nicht aufgefunden werden.

Gerade im Bezug zu den Routern befinden sich die für die strafverfolgenden Ermittlungsbehörden straftatrelevanten Daten überwiegend im flüchtigen Speicher. Eine Datensicherung vor dem Trennen der elektrischen Spannungszufuhr stellt sich somit als notwendig heraus. Für die Herangehensweise der gewählten Router kann für die forensische Datensicherung folgende Empfehlung notiert werden:

Eine Sicherung der flüchtigen Datenbasis kann nur an der Örtlichkeit durchgeführt werden. Die Stromzufuhr darf nicht unterbrochen werden. Der WLAN-Router muss im eingeschalteten Zustand verbleiben. Bei beiden Routern kann über die grafische Benutzeroberfläche jeweils eine Logdatei gedownloaded werden. Bei Fehlen des Gerätekennwortes ist eine weitere Vorgehensweise zu dem 'Vodafone Station Arris TG3442DE' durch Auslesen des Flash Speichers mittels der Chip-Off Methode im Labor möglich. Der 'TP-Link AC1200 Mesh Wi-Fi Router' kann an der Örtlichkeit über die serielle Schnittstelle UART kontaktiert werden. Hier können sowohl in der RAM Sicherung als auch in der Dateisystemstruktur sachverhaltsbezogene Daten vorgefunden werden. Weitere Schnittstellen lassen einen Datenabzug nicht zu.

Mögliche Spuren in beiden Routern können im Bereich der Netzwerkdaten die downloadbaren Logdateien sein. Diese beinhalten Events zu verbundenen Geräten mit dem Router. Ein Zeitstempel wird geführt. Auf der grafischen Benutzeroberfläche kann die Lease-Liste entnommen werden. Diese beinhaltet für die jeweiligen Endgeräte, neben den IP-Adressen, die zugehörigen MAC-Adressen. Andere Ports für einen Datentransfer sind nicht freigegeben.

Die Zugänglichkeit der Modelle zu den jeweiligen Herstellern kann variieren. So kann den Anlagen 'Y Arris - Standard Benutzername und Standard Passwort (nach Gerät)' und 'Z TP-Link - Standard Benutzername und Standard Passwort (nach Gerät)' Standard Benutzernamen und Standard Passwörter entnommen werden, welche einen Zugriff auf die grafische Benutzeroberfläche bzw. der UART Schnittstelle ermöglichen. Es kann eine Ähnlichkeit bzw. Übereinstimmung der Standardeingaben zu den Modellen der Hersteller erkannt werden.

5.4 Ausblick

Diese Arbeit lässt einen kurzen Einblick in das Abgreifen von Daten an WLAN Routern zu. Bei den genutzten seriellen Schnittstellen handelt es sich um Debug-Schnittstellen, welche ihren Ursprung in der Fehlersuche und Überprüfung des Systems beim Hersteller haben. Diese können durch Anwender zweckentfremdet genutzt werden. Es ist möglich, dass die Hersteller bei der Implementation dieser bei zukünftigen Geräten verzichten, auch um einen Zugriff auf die Firmware durch Dritte unterbinden zu können. Der Router 'Vodafone Station Arris TG3442DE' stellt dabei einen modernen Vertreter mit nicht mehr implementierten seriellen Schnittstellen dar.

Für aktuelle Analysen wird ohne vorliegendes Gerätekennwort das Vorhandensein serieller Schnittstellen zur Ausleitung der Daten genutzt. Diese Vorgehensweise ist bei dem Vertreter des 'Vodafone Station Arris TG3442DE' nicht mehr möglich. Für weitere Untersuchungen könnte ein Angriff auf das Gerätepasswort anvisiert werden. Aufgrund des netzartigen Verbundes und der untereinander erfolgten Kommunikation ist für das Mesh-System kennzeichnend, dass dieses für den Nutzer mit einer einzigen SSID und einem Sicherheitskennwort ausgestattet ist. Für folgende Untersuchungen könnte der interne Kommunikationsaustausch und das Vorhandensein von Datenbasis analysiert werden.

Für das Modell 'TP-Link AC1200 Mesh Wi-Fi Router' wurde keine USB Schnittstelle implementiert. Der SoC lässt eine solche Implementation jedoch zu. Das Datenblatt des SoCs steht zur Verfügung und kann eingesehen werden. Möglich ist es einen Adapter mittels eines 3D-Druckes zu erstellen und in diesem die fehlenden Verbindungen fest anzubringen. Dies würde eine weitere Möglichkeit für die Extraktion der Daten bieten, auch im Bezug auf den Linux Konsolenbefehl 'dd'.

Die ständig fortführende Entwicklung der Geräte im Hinblick auf deren Hard- und Software stellt für die IT-Forensik eine kontinuierliche Herausforderung dar. Erkenntnisse, welche bereits gewonnen werden konnten, können mit der nächsten Version bereits nicht mehr übereinstimmen. Final betrachtet unterscheiden sich die Router zu den jeweiligen Herstellern sowie zu den jeweiligen Modellen und Versionen voneinander. Die Verfügbarkeit der Daten ist von Router zu Router erneut zu überprüfen. Ein Überblick über die verschiedenen Zugriffsmöglichkeiten zu Modellen einer Herstellerreihe im Vergleich zu anderen, würde sich für die forensische Herangehensweise bei polizeilich relevanten Sachverhalten von Vorteil erweisen.

Anhang A: UART Einstellungen - Putty Standardeingabe

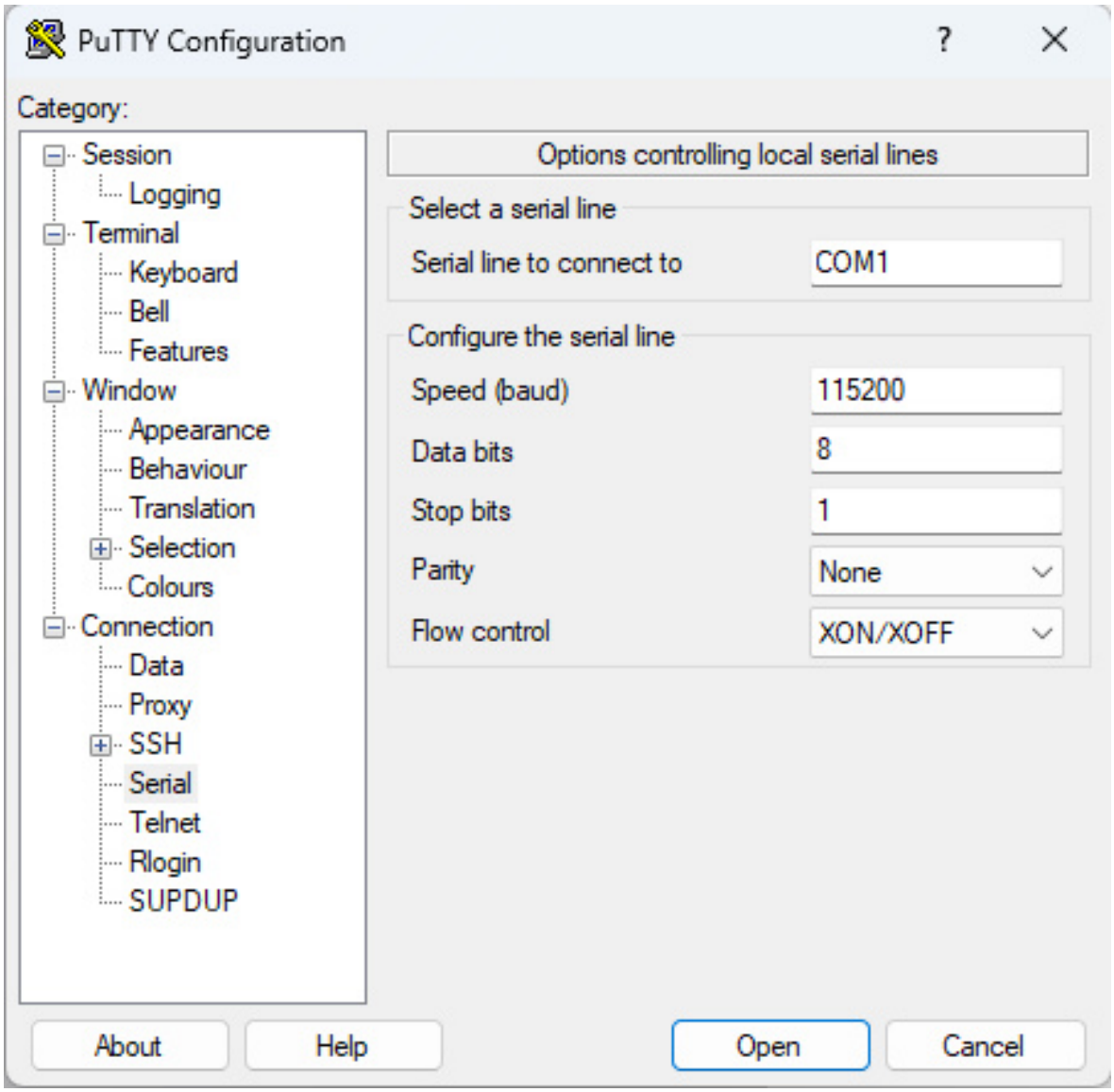

Abbildung A.1: UART Schnittstelle - Softwarelösung 'Putty' Standardeingabe

Anhang B: Marktrecherche: 'WiGLE'

Hersteller	Anzahl
Cannot find MAC address Anzahl	2104
Avm Audiovisuelles Marketing und Computersysteme Gmbh Anzahl	1018
Arcadyan Corporation Anzahl	356
Huawei Technologies Co.,ltd Anzahl	276
Ruckus Wireless Anzahl	192
Aruba, a Hewlett Packard Enterprise Company Anzahl	181
Cisco Meraki Anzahl	95
Ubiquiti Networks Inc. Anzahl	95
TP-Link Technologies Co.,ltd. Anzahl	86
Askey Computer Corp Anzahl	79
Compal Broadband Networks, Inc. Anzahl	74
Extreme Networks, Inc. Anzahl	73
Sercomm Corporation. Anzahl	57
Technicolor Ch Usa Inc. Anzahl	57
Hewlett Packard Enterprise Anzahl	55
Arris Group, Inc. Anzahl	54
Zyxel Communications Corporation Anzahl	47
Netgear Anzahl	34
devolo Ag Anzahl	31
Cambium Networks Limited Anzahl	21
Sophos Ltd Anzahl	21
Wistron Neweb Corporation Anzahl	15
Lancom Systems Gmbh Anzahl	14
eero inc. Anzahl	13
Tatung Technology Inc. Anzahl	12
Apple, Inc. Anzahl	11
D-Link International Anzahl	11
Murata Manufacturing Co., Ltd. Anzahl	11

Tabelle B.1: Auswertung: WiGLE

Anhang C: Vodafone Station Arris TG3442DE - Analyse Ereignisprotokoll

1. Datensicherung 30.05.2023	Analysebeginn
WAN Status Systemzeit Eventlog	0 Tage, 0 Stunden, 8 Minuten, 9 Sekunden 0 Tage, 0 Stunden, 0 Minuten 30.05.2023 14:12 Uhr 30.05.2023 11:52 Uhr - 30.05.2023 14:05 Uhr Dateigröße: 16 kB Dauer: 02:13 Stunden
2. Datensicherung 08.06.2023	Analyseende
WAN Status Eventlog	8 Tage, 21 Stunden, 31 Minuten, 5 Sekunden 0 Tage, 8 Stunden, 21 Minuten 08.06.2023 06:45 Uhr - 08.06.2023 11:16 Uhr Dateigröße: 17 kB Dauer: 3:31 Stunden
3. Datensicherung 08.06.2023	Neustart
WAN Status Systemzeit Eventlog	0 Tage, 0 Stunden, 16 Minuten, 11 Sekunden 0 Tage, 0 Stunden, 0 Minuten 08.06.2023 12:33 Uhr 08.06.2023 11:08 Uhr - 08.06.2023 12:38 Uhr Dateigröße: 18 kB Dauer: 02:53 Stunden
	Stromstecker gezogen
Eventlog	08.06.2023 12:18 Uhr - 08.06.2023 12:52 Uhr Dateigröße: 16 kB Dauer: 00:44 Stunden
4. Datensicherung 12.06.2023	
WAN Status Systemzeit Eventlog Eventlog	4 Tage, 3 Stunden, 57 Minuten, 5 Sekunden 0 Tage, 4 Stunden, 4 Minuten 12.06.2023 16:48 Uhr 11.06.2023 07:18 Uhr - 11.06.2023 19:35 Uhr Dateigröße: 18 kB Dauer: 12:17 Stunden 11.06.2023 15:27 Uhr - 12.06.2023 05:28 Uhr Dateigröße: 17 kB Dauer: 10:01 Stunden
5. Datensicherung 14.06.2023	
WAN Status Eventlog WAN Status Eventlog	5 Tage, 16 Stunden, 37 Minuten, 29 Sekunden 0 Tage, 5 Stunden, 16 Minuten 13.06.2023 21:30 Uhr - 14.06.2023 05:20 Uhr Dateigröße: 12 kB Dauer: 08:50 Stunden 6 Tage, 7 Stunden, 31 Minuten, 46 Sekunden 0 Tage, 6 Stunden, 7 Minuten 14.06.2023 08:42 Uhr - 14.06.2023 20:15 Uhr Dateigröße: 12 kB Dauer: 11:33 Stunden
6. Datensicherung 15.06.2023	
WAN Status Systemzeit Eventlog	6 Tage, 15 Stunden, 45 Minuten, 12 Sekunden 0 Tage, 6 Stunden, 15 Minuten 15.06.2023 04:33 Uhr 15.06.2023 04:05 Uhr - 15.06.2023 04:29 Uhr Dateigröße: 23 kB Dauer: 00:24 Stunden

Tabelle C.1: Vodafone Station Arris TG3442DE - Analyse Ereignisprotokoll

Anhang D: Übersicht Leiterplatine Arris TG3452

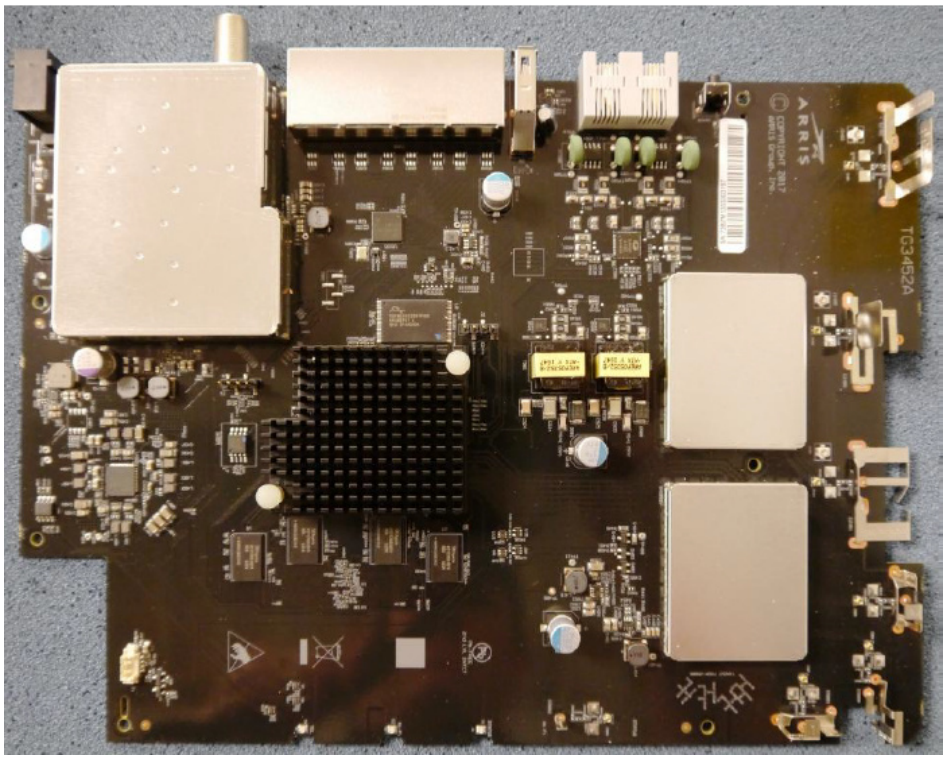

Abbildung D.1: Arris TG3452 - Leiterplatine Vorderseite | Original [61]

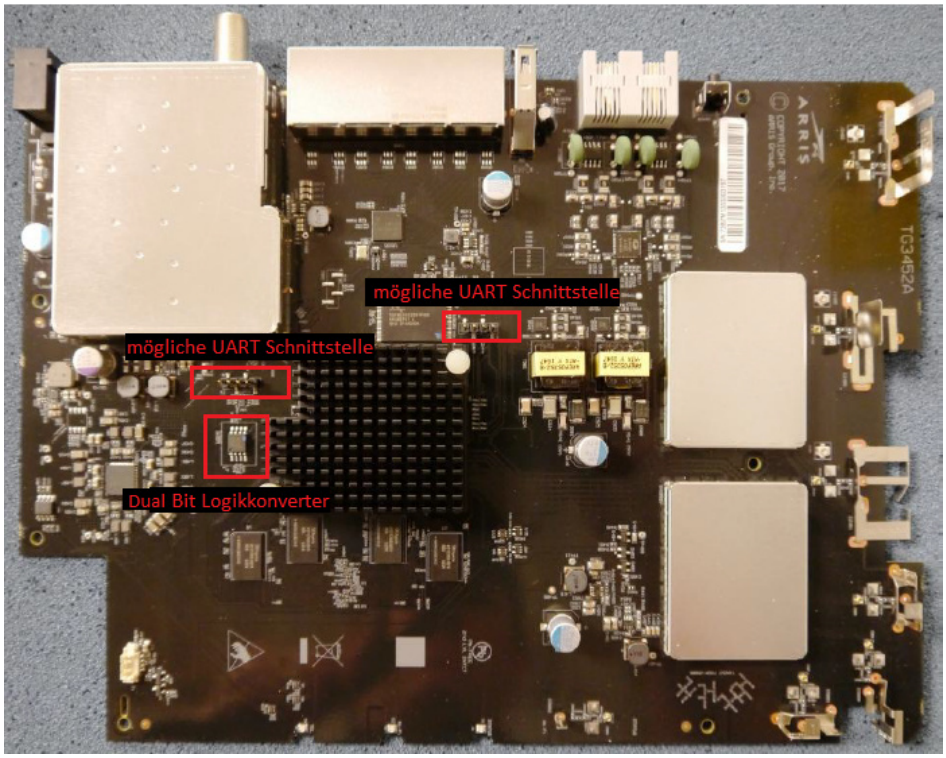

Abbildung D.2: Arris TG3452 - Leiterplatine Vorderseite | bearbeitet [61]

Anhang E: Übersicht Leiterplatine Arris TG3442

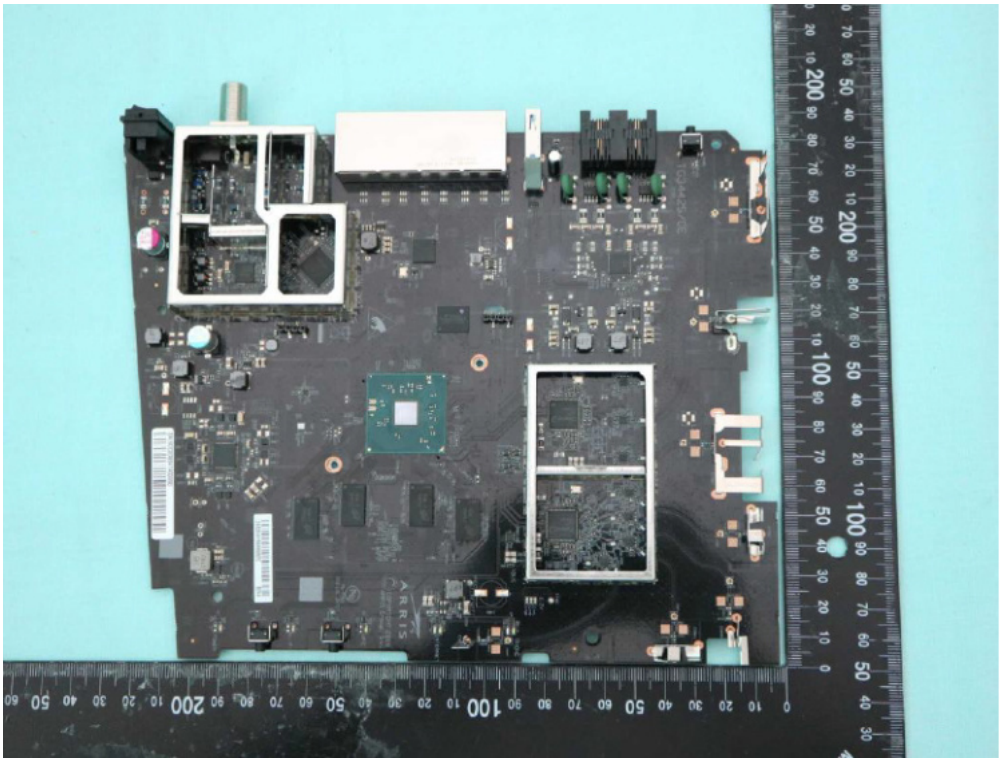

Abbildung E.1: Arris TG3442 - Leiterplatine Vorderseite | Original [62]

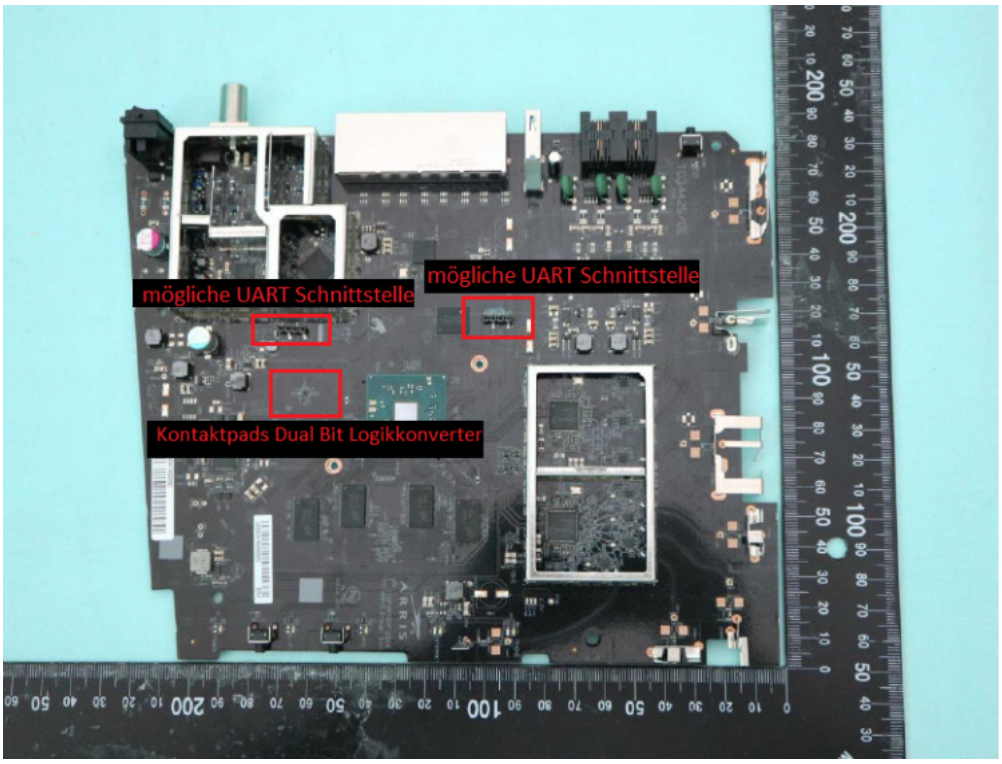

Abbildung E.2: Arris TG3442 - Leiterplatine Vorderseite | bearbeitet [62]

Anhang F: Übersicht Leiterplatine Vodafone Station Arris TG3442DE

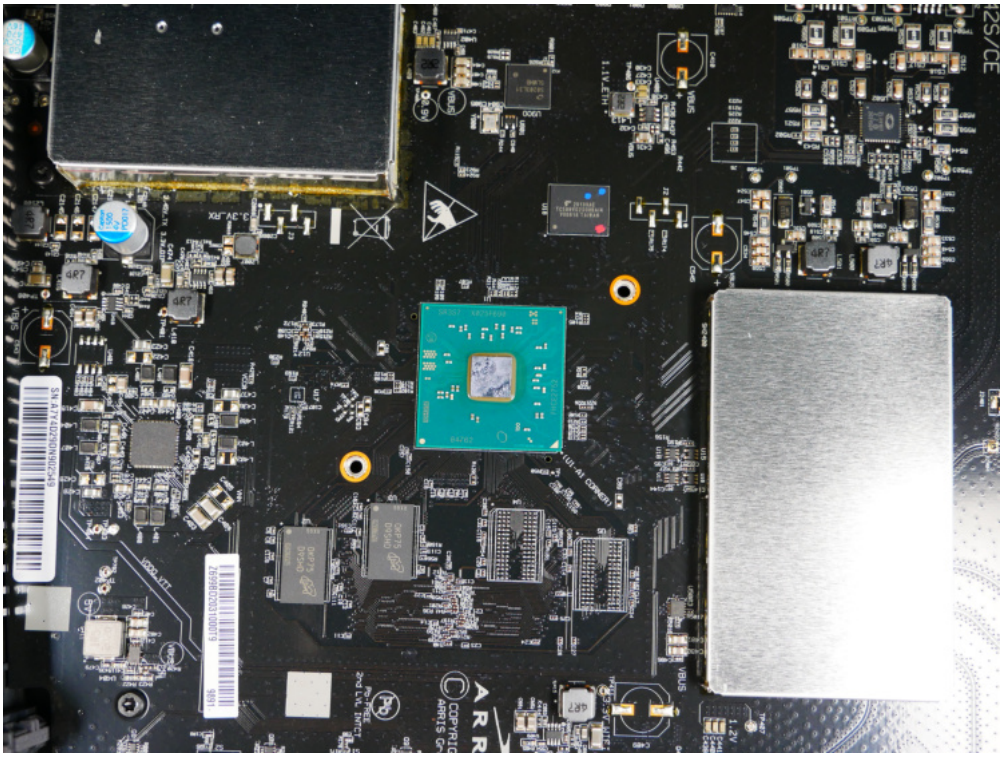

Abbildung F.1: Vodafone Station Arris TG3442DE - Leiterplatine Vorderseite | Original

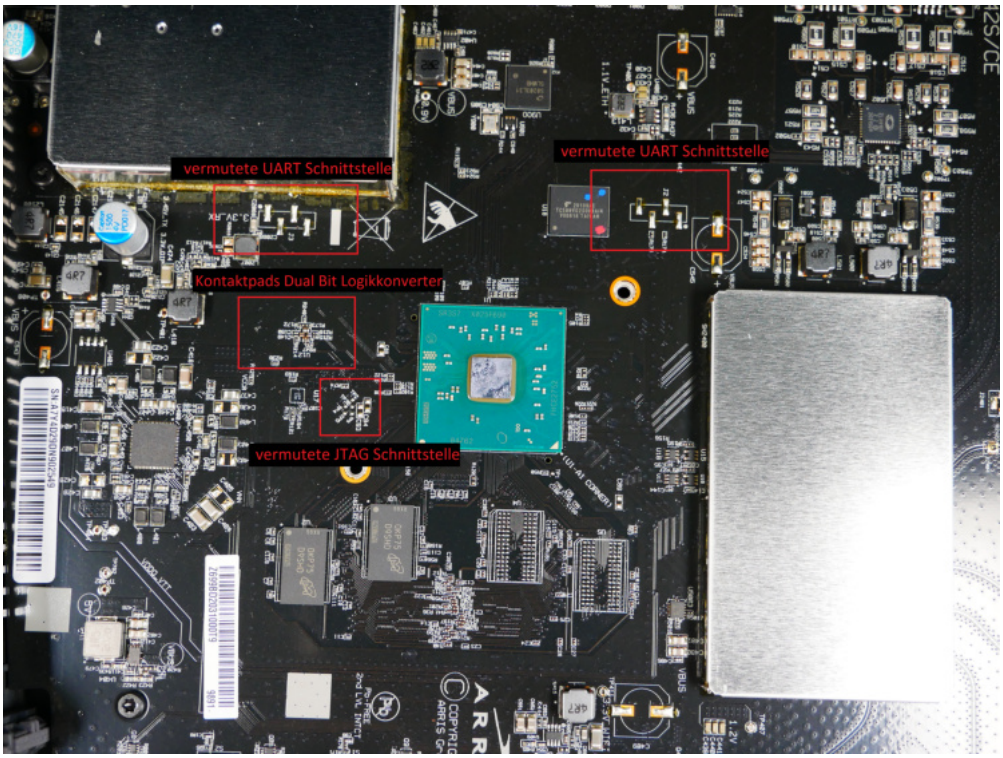

Abbildung F.2: Vodafone Station Arris TG3442DE - Leiterplatine Vorderseite | bearbeitet

Anhang G: Vodafone Station Arris TG3442DE - Röntgenansicht

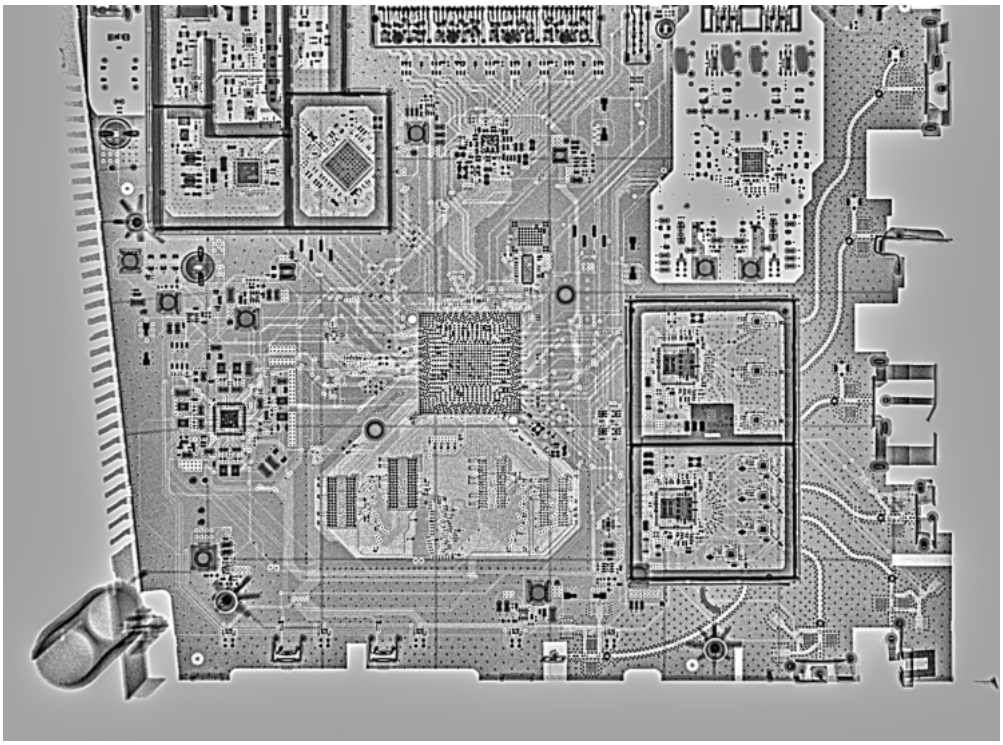

Abbildung G.1: Vodafone Station Arris TG3442DE - Röntgenansicht | Vorderansicht

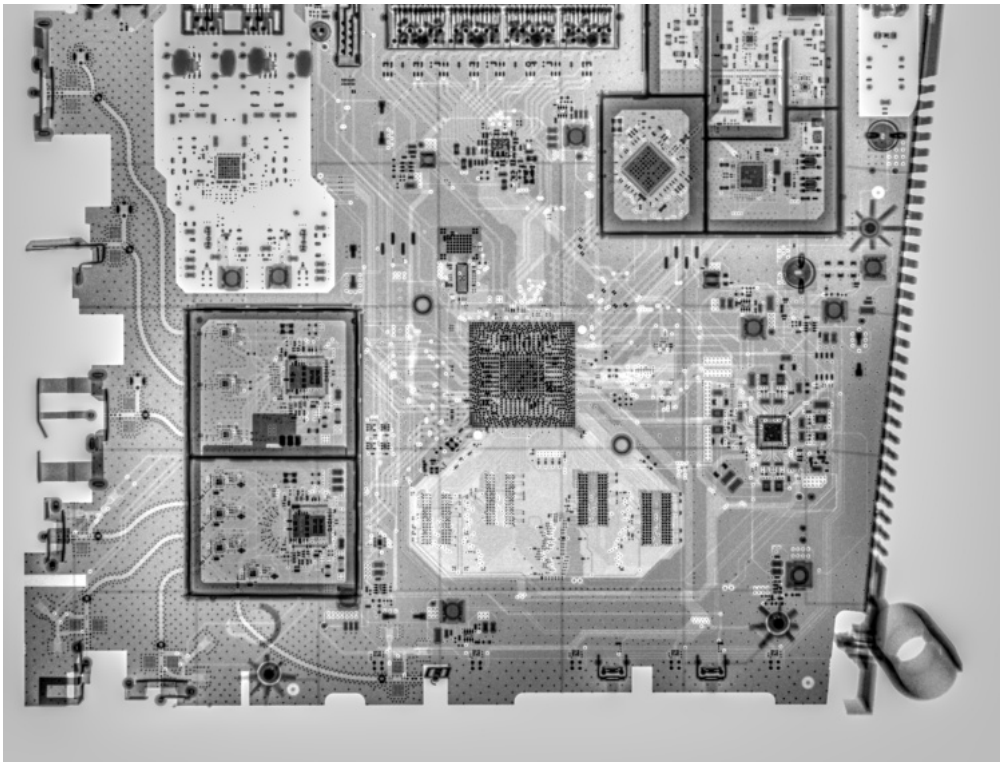

Abbildung G.2: Vodafone Station Arris TG3442DE - Röntgenansicht | Rückansicht

Anhang H: Vodafone Station Arris TG3442DE - UART-Schnittstellenanalyse

H.1 Schnittstellenanalyse

Bei der Lokalisation der Schnittstellen können die vermuteten Schnittstellen aufgezeigt werden. Die der Grafik links zu entnehmende Schnittstelle wird als Schnittstelle 1 [Kontaktpadstelle J3] und die der rechts aus der Grafik zu entnehmende Schnittstelle als Schnittstelle 2 [Kontaktpadstelle J2] bezeichnet.

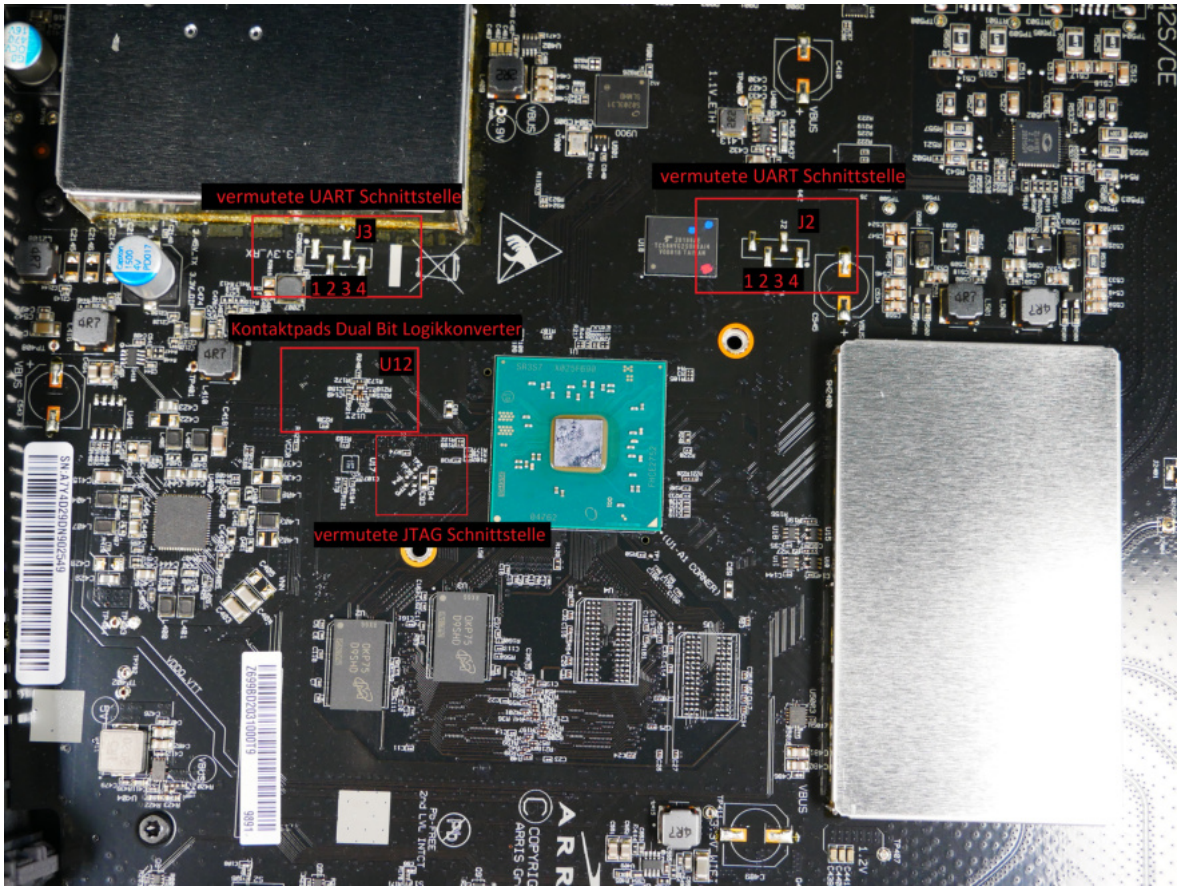

Abbildung H.1: Vodafone Station Arris TG3442DE - UART Schnittstellenanalyse

H.2 Schnittstelle 1 [Kontaktpadstelle J3]

Kontaktierpunkt	Messergebnis unter Stromzufuhr	Messergebnis Werkzeug	Belegung
1	3,3 V	Multimeter & Oszilloskop	Spannung
2	0 V	Multimeter & Logik Analysator	RX
3	3,3 V	Multimeter & Logik Analysator	TX
4	0 V	Multimeter (Durchgangsleitung | Gleichstrom)	Erdung

Tabelle H.1: Vodafone Station Arris TG3442DE - Schnittstelle 1 [Kontaktpadstelle J3]

H.3 Schnittstelle 2 [Kontaktpadstelle J2]

Kontaktierpunkt	Messergebnis unter Stromzufuhr	Messergebnis ohne Stromzufuhr	Messergebnis Werkzeug	Belegung
1	0 V	0 K	Multimeter	Erdung
2	3,3 V	1 Megaohm	Logik Analysator	kein Datenverkehr
3	3,3 V	1 Megaohm	Logik Analysator	kein Datenverkehr
4	3,3 V	0,5 K	Multimeter & Oszilloskop	Spannung

Tabelle H.2: Vodafone Station Arris TG3442DE - Schnittstelle 2 [Kontaktpadstelle J2]

Anhang I: Vodafone Station Arris TG3442DE - Versuchsaufbau Lokalisation der UART Schnittstelle

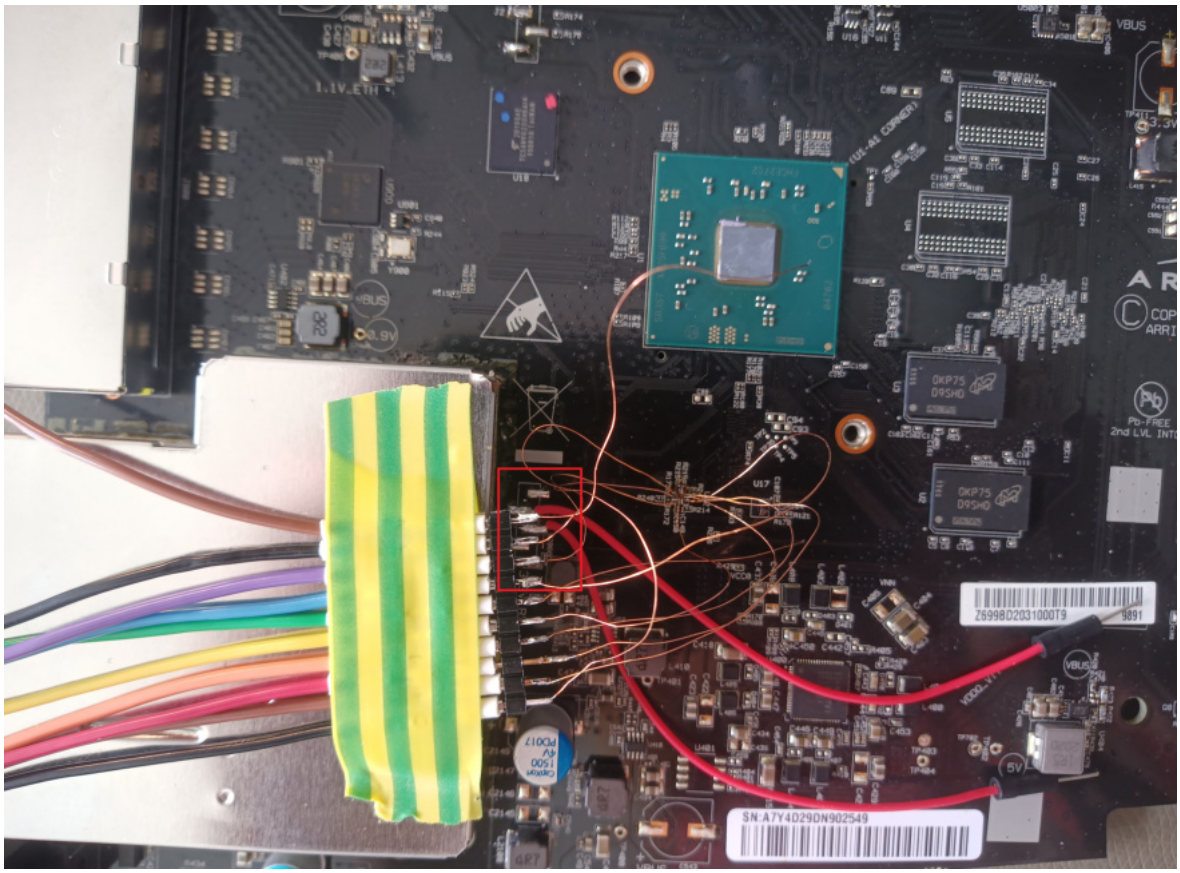

Abbildung I.1: Vodafone Station Arris TG3442DE - Lokalisierte UART Schnittstelle 1

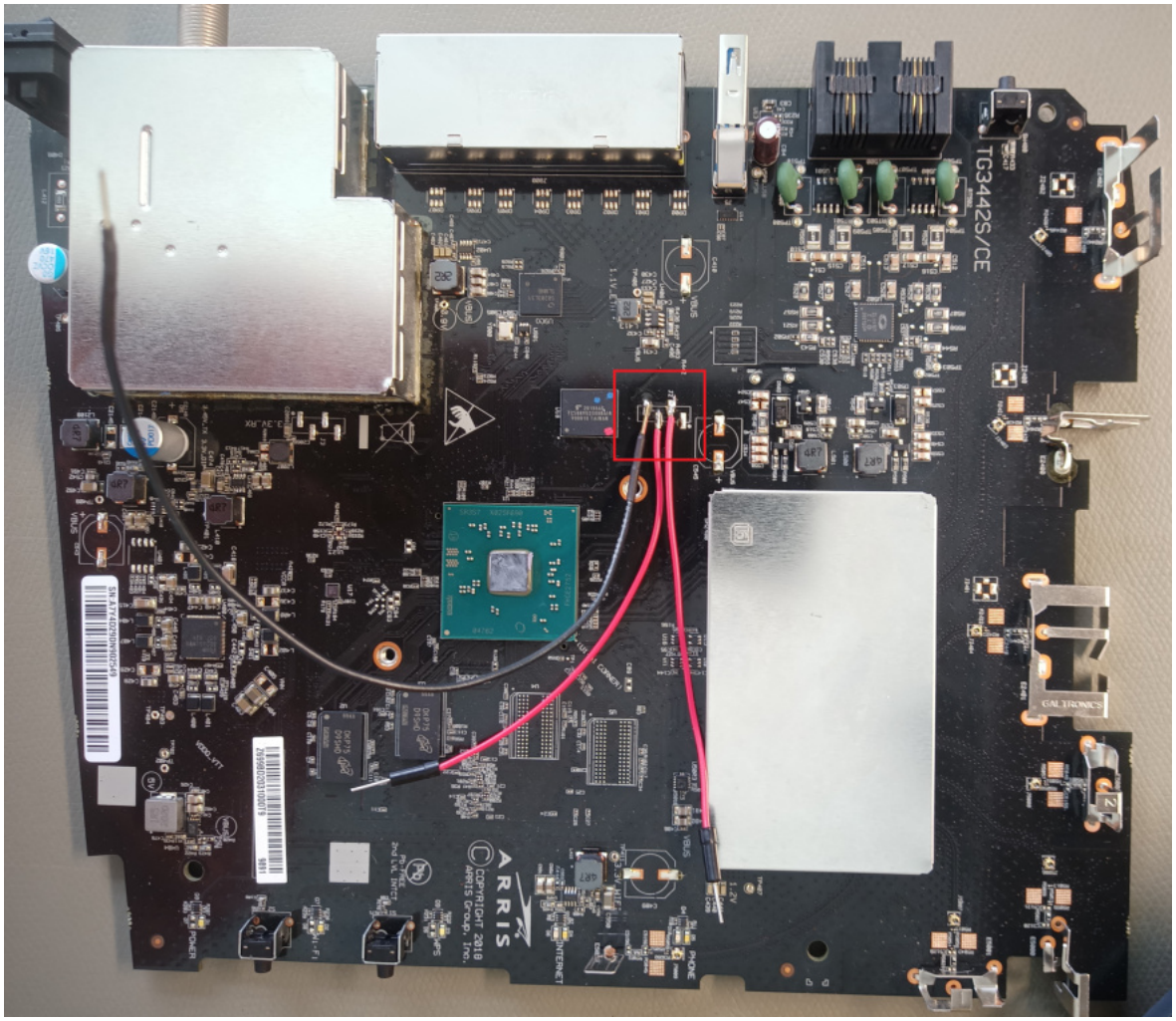

Abbildung I.2: Vodafone Station Arris TG3442DE - Lokalisierte UART Schnittstelle 2

Anhang J: Vodafone Station Arris TG3442DE - Logik Analysator

J.1 Vodafone Station Arris TG3442DE - Softwareausgabe Logik Analysator 'saneae'

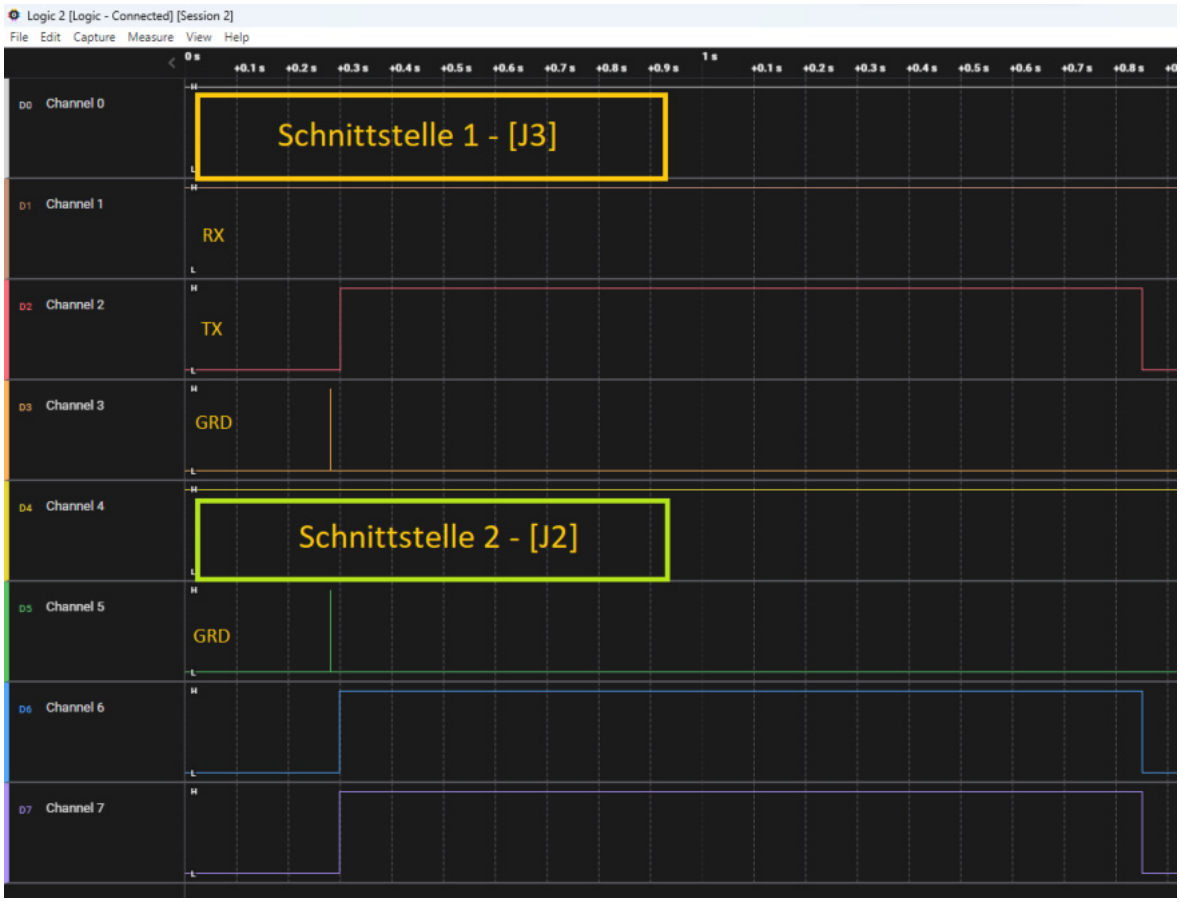

Abbildung J.1: Vodafone Station Arris TG3442DE - Softwareausgabe Logik Analysator 'saneae'

Der Grafik kann kein Datenstrom entnommen werden. Bei der Datenübertragung werden Spannungspegel übertragen. Datenleitungen im Ruhezustand können je nach Konfiguration einen High-Pegel oder Low-Pegel aufweisen. RX und TX werden entweder durch ein Pull-Up auf einen High-Pegel von 3,3 V oder durch ein Pull-Down auf einen Low-Pegel von 0 V gezogen.

J.2 Vodafone Station Arris TG3442DE - Hardwareverbund Logik Analysator 'saneae'

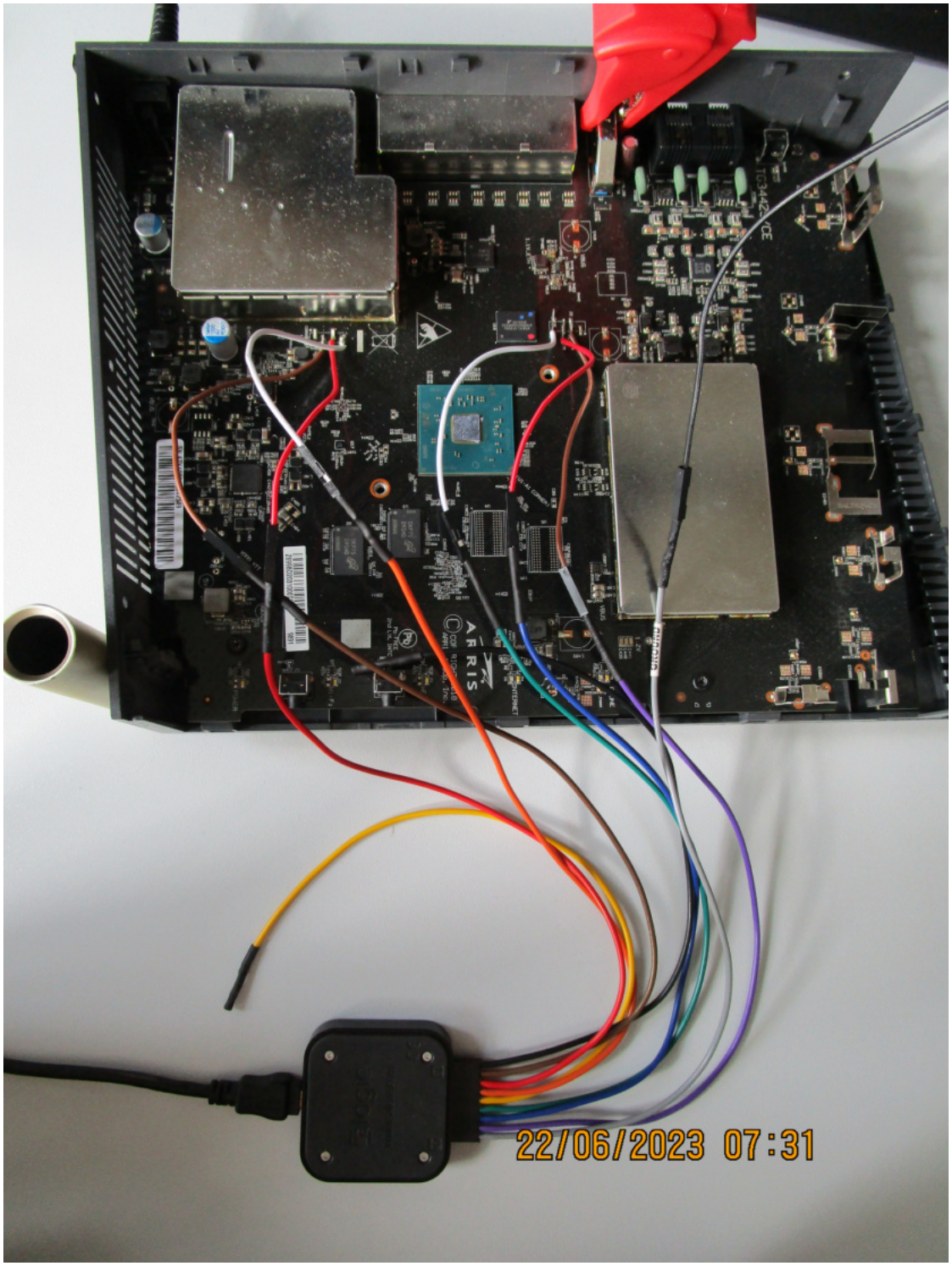

Abbildung J.2: Vodafone Station Arris TG3442DE - Hardwareverbund Logik Analysator 'saneae'

J.3 Vodafone Station Arris TG3442DE - Lokalisierter Logikkonverter

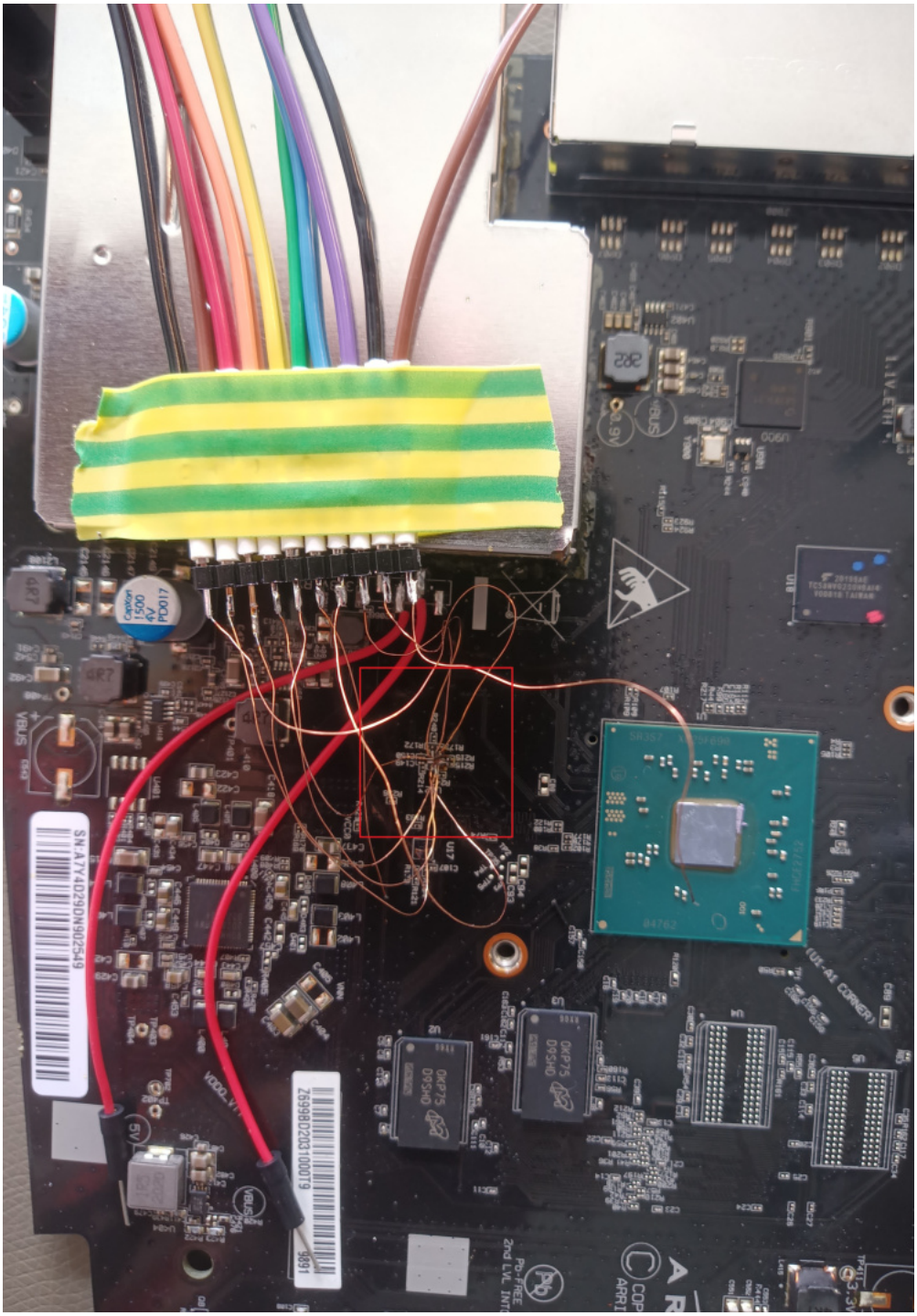

Abbildung J.3: Vodafone Station Arris TG3442DE - Lokalisierter Logikkonverter

J.4 Vodafone Station Arris TG3442DE - Lokalisierte JTAG Schnittstelle

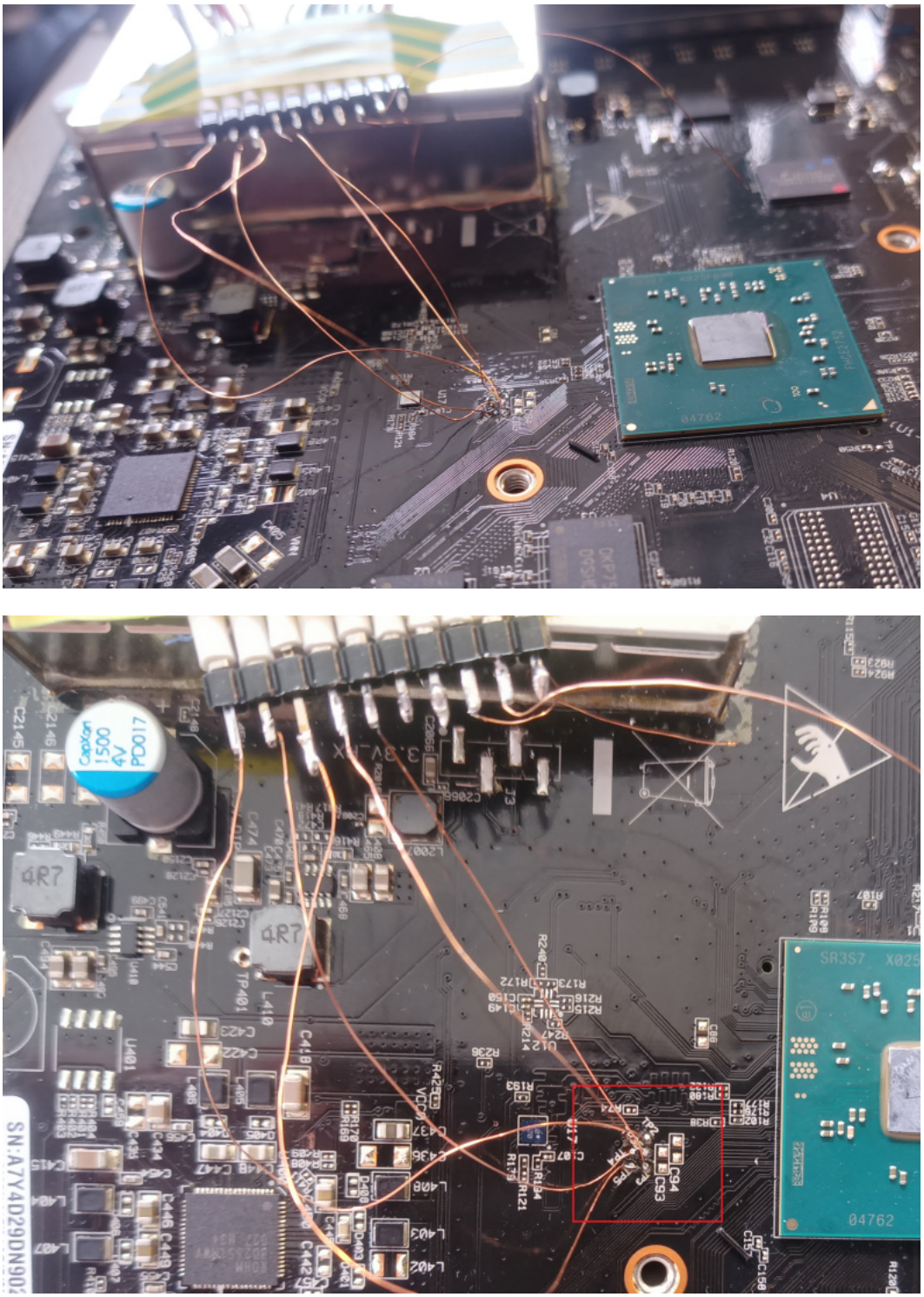

Abbildung J.4: Vodafone Station Arris TG3442DE - Lokalisierte JTAG Schnittstelle

Anhang K: Vodafone Station Arris TG3442DE - Versuchsaufbau Möglichkeit 2

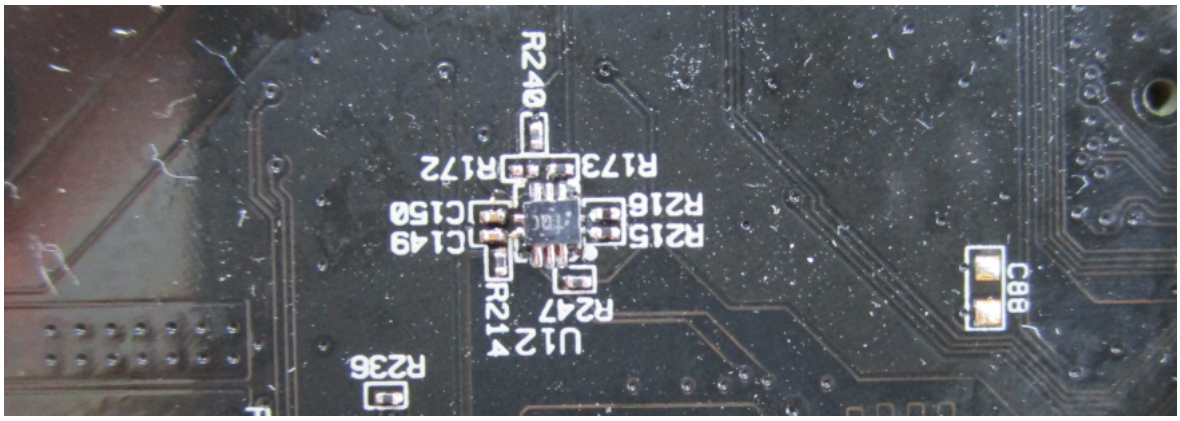

Abbildung K.1: Vodafone Station Arris TG3442DE - Versuchsaufbau Möglichkeit 2 | Anlöten des Dual-Bit Logikkonverters

Anhang L: Vodafone Station Arris TG3442DE - Versuchsaufbau Möglichkeit 4

L.1 Anlöten von Kupferlackdrähten an eMMC Modul

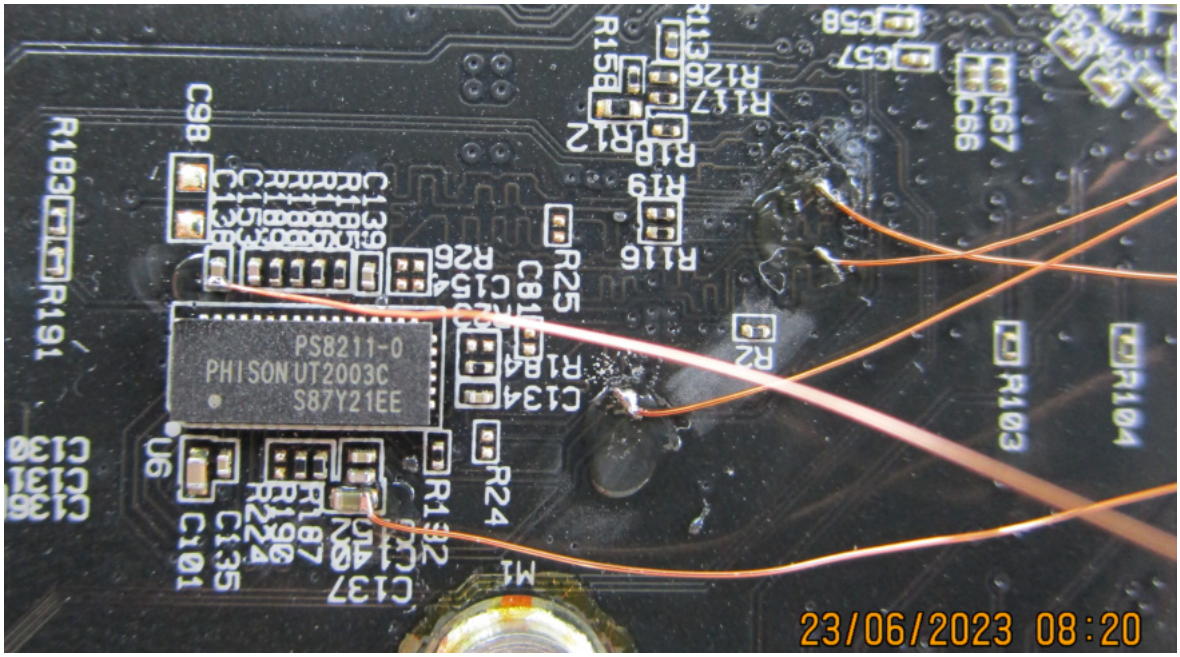

Abbildung L.1: Vodafone Station Arris TG3442DE - Versuchsaufbau Möglichkeit 4 | Anlöten von Kupferlackdrähten an eMMC Modul

L.2 Freigelegter SD Card Kartenadapter

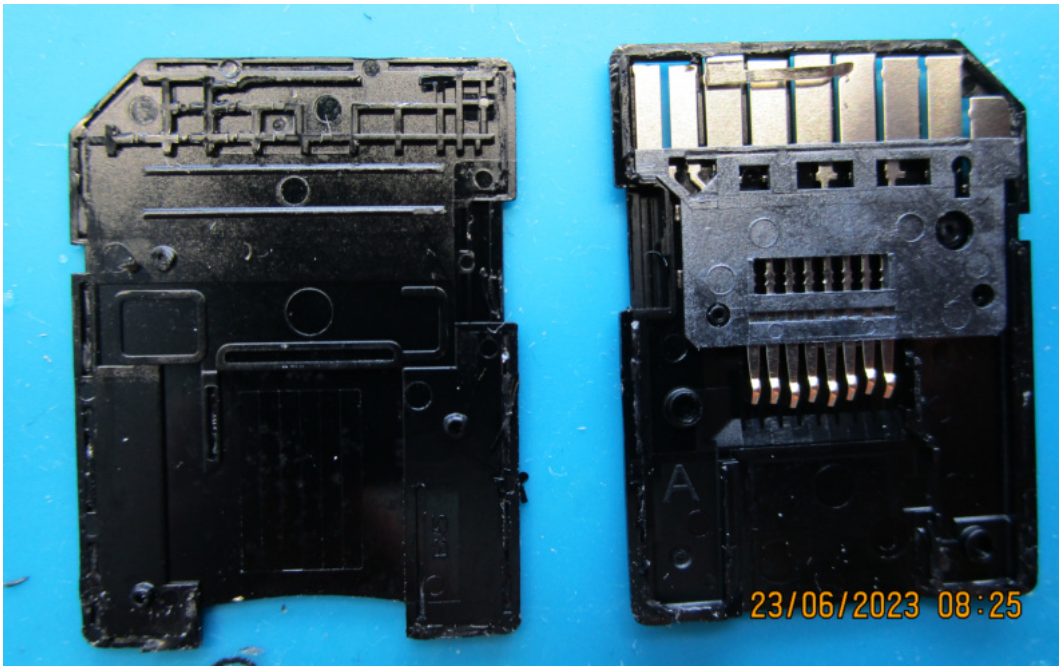

Abbildung L.2: Vodafone Station Arris TG3442DE - Versuchsaufbau Möglichkeit 4 | geöffneter SD Card Kartendapter

L.3 Verbinden des SD Card Kartenadapters mit eMMC Modul

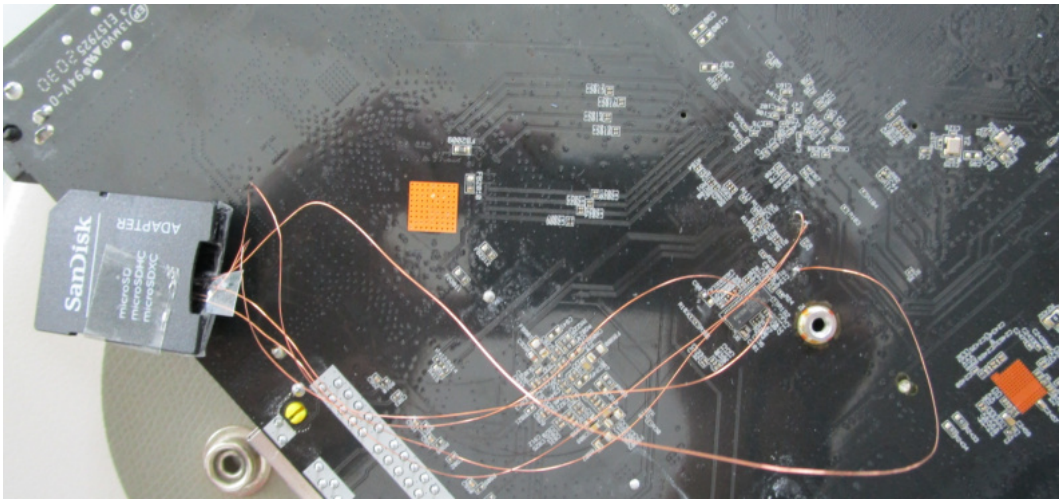

Abbildung L.3: Vodafone Station Arris TG3442DE - Versuchsaufbau Möglichkeit 4 | verbundener SD Card Kartendapter mit Lödpadstelle U6, eMMC Modul Phison PS8211-0

Anhang M: Vodafone Station Arris TG3442DE - Versuchsaufbau Möglichkeit 5

M.1 Chip-Off Flash Speicher

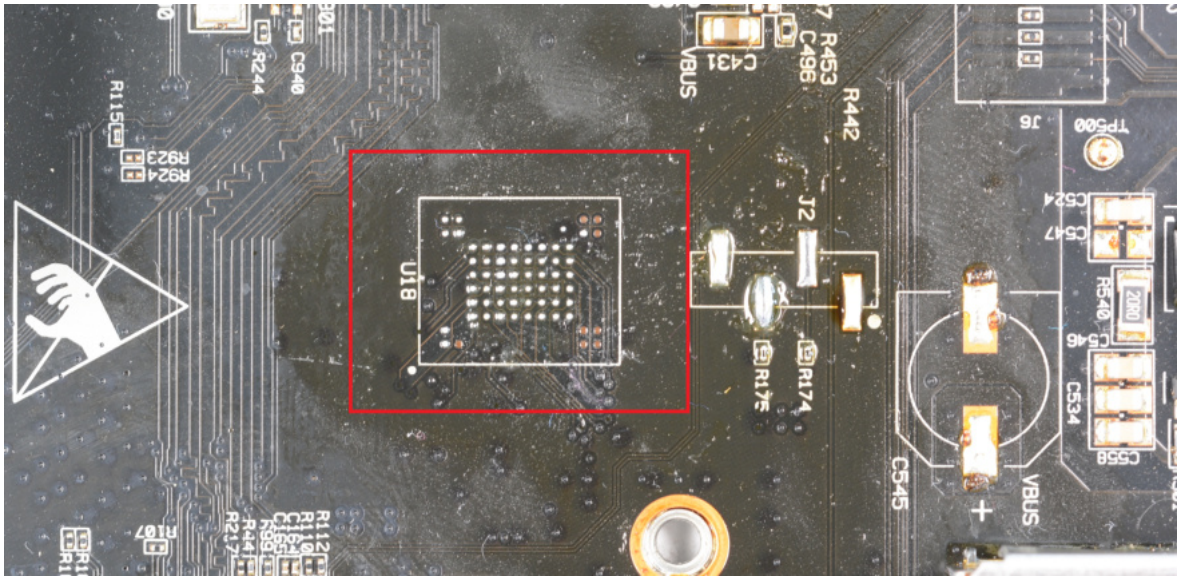

Abbildung M.1: Vodafone Station Arris TG3442DE - Versuchsaufbau Möglichkeit 5 | Chip-Off Flash Speicher

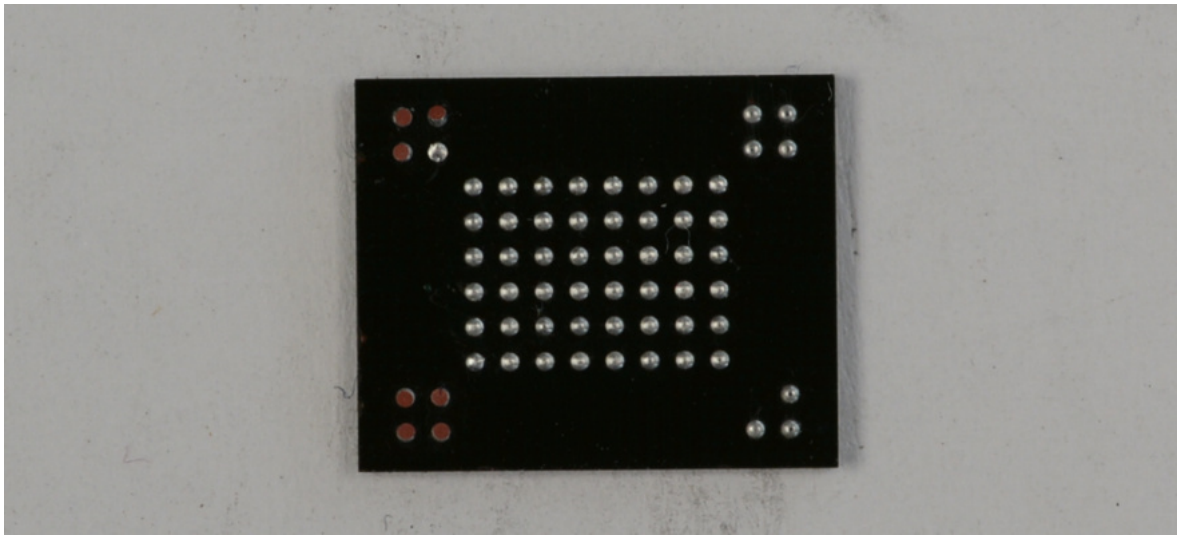

Abbildung M.2: Vodafone Station Arris TG3442DE - Versuchsaufbau Möglichkeit 5 | Chip-Off Flash Speicher - BGA Chip

Anhang N: TP-Link AC1200 Mesh Wi-Fi Router - Anmeldevorgang Paketaustausch [Syslog]

```
2023-06-06 17:57:58 dhcps[4049]: <6> 212054 send ack ip 192.168.0.188 and dns 192.168.0.106 to 00:57:4a:15:40:44
2023-06-06 17:57:58 dhcps[4049]: <6> 212053 receive request ip 192.168.0.188 from 00:57:4a:15:40:44
2023-06-06 17:57:58 dhcps[4049]: <6> 212052 send offer ip 192.168.0.188 and dns 0.0.0.0 to 00:57:4a:15:40:44
2023-06-06 17:57:58 dhcps[4049]: <6> 212051 receive discover from 00:57:4a:15:40:44
```

Abbildung N.1: TP-Link AC1200 Mesh Wi-Fi Router - Paketaustausch Anmeldevorgang Endgerät [Grafische Benutzeroberfläche: Syslog]

Anhang O: TP-Link AC1200 Mesh Wi-Fi Router - Beginn der Konsolenausgabe

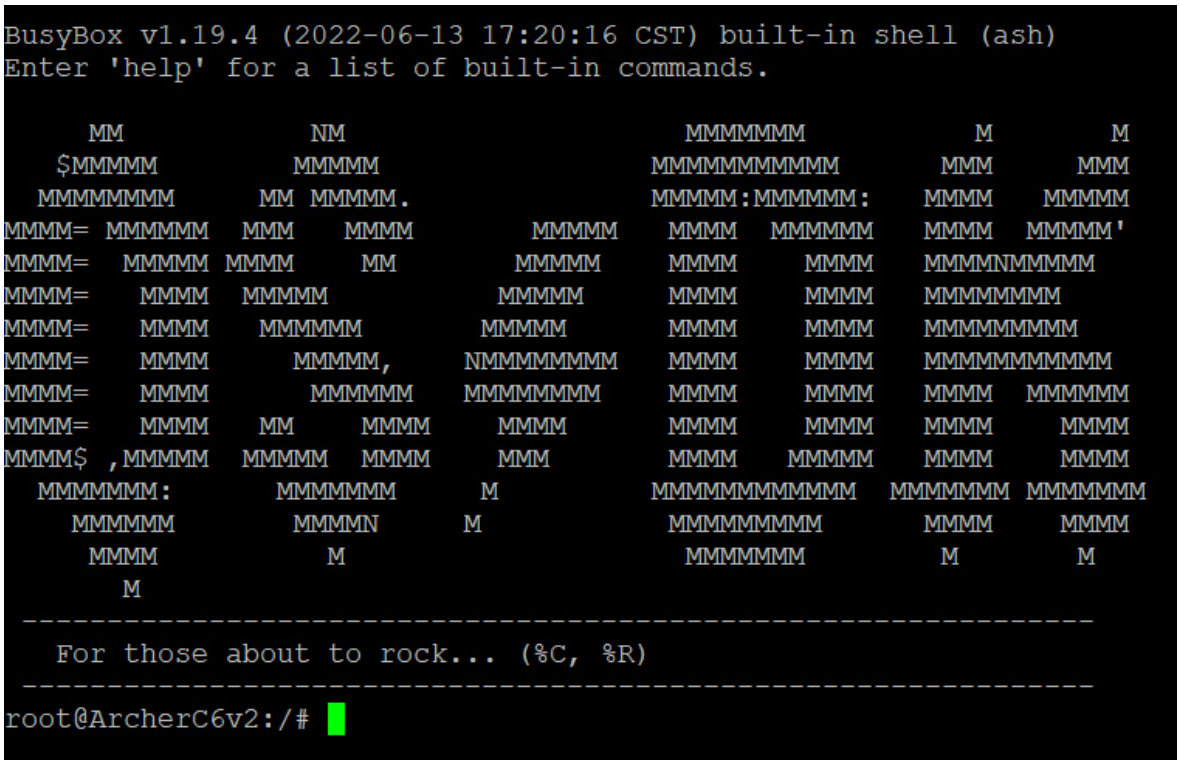

Abbildung O.1: TP-Link AC1200 Mesh Wi-Fi Router - Beginn der Konsolenausgabe über die Softwarelösung 'Putty'

Anhang P: TP-Link AC1200 Mesh Wi-Fi Router - Einwahl Untersuchungsrechner am WLAN Router

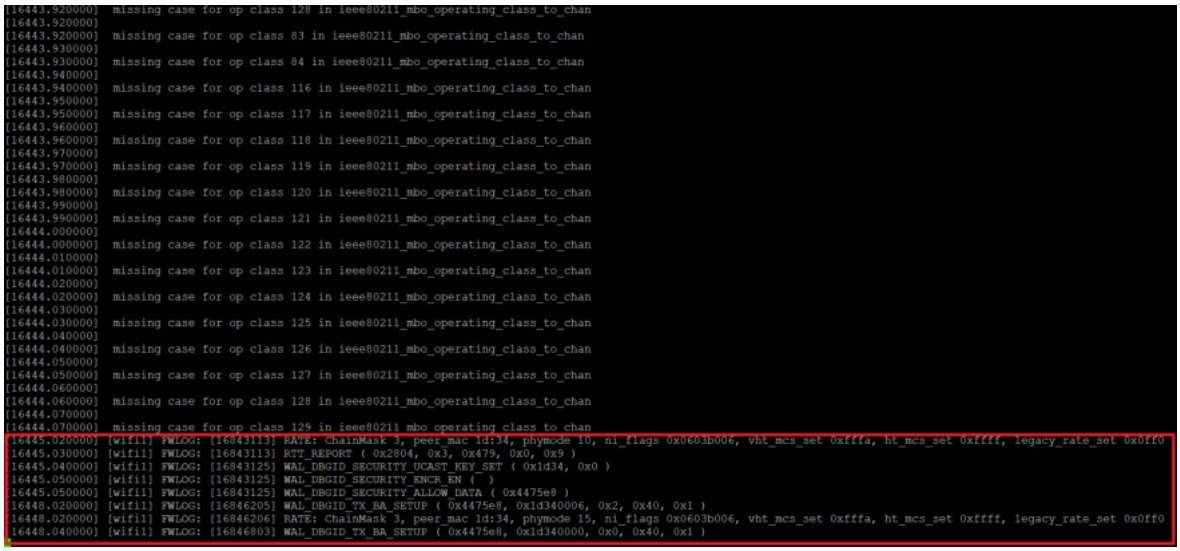

Abbildung P.1: TP-Link AC1200 Mesh Wi-Fi Router - Einwahl Untersuchungsrechner am WLAN Router'

Anhang Q: TP-Link AC1200 Mesh Wi-Fi Router - SoC

Figure 2-1 shows the QCA9563 pinout

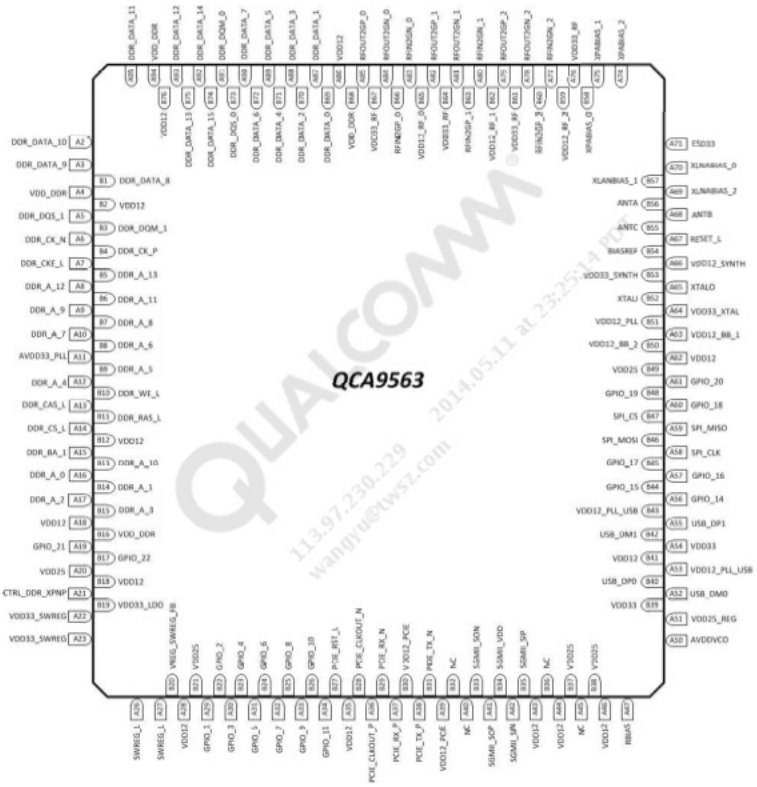

Figure 2-1 Package Pinout (See-Through Top View)

Abbildung Q.1: TP-Link AC1200 Mesh Wi-Fi Router - Pin Out SoC [63]

Anhang R: TP-Link AC1200 Mesh Wi-Fi Router - Richtige Passworteingabe Anmeldevorgang Paketaustausch

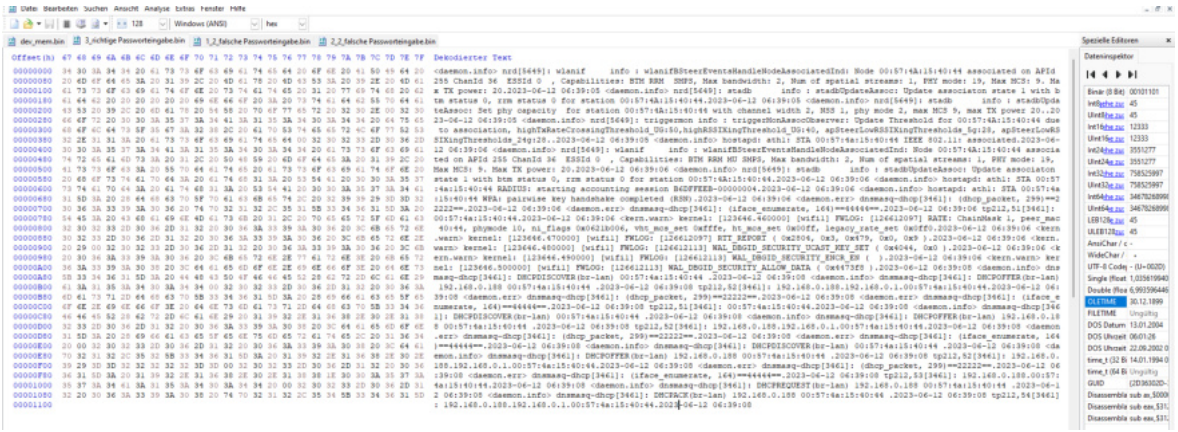

Abbildung R.1: TP-Link AC1200 Mesh Wi-Fi Router - Richtige Passworteingabe _ Anmeldevorgang Paketaustausch

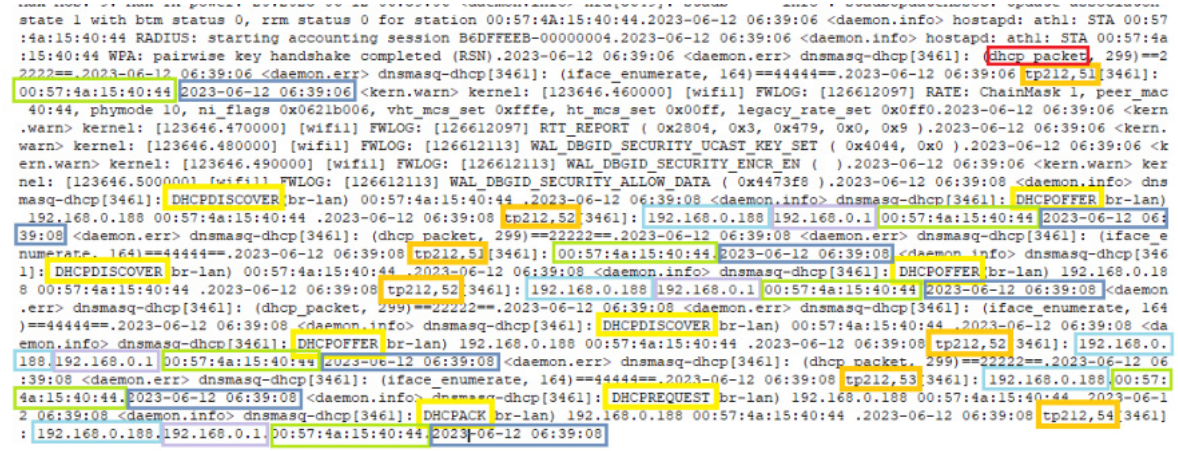

Abbildung R.2: TP-Link AC1200 Mesh Wi-Fi Router - Richtige Passworteingabe _ Anmeldevorgang Paketaustausch [markiert]

Anhang S: TP-Link AC1200 Mesh Wi-Fi Router - Aufbau 'Config List'

```
config list
    option mac '9E49AD[redacted]'
    option hostname 'Samsung'
    option access_host '1'

config list
    option mac '36B76A[redacted]'
    option hostname '*'
    option access_host '1'

config list
    option mac '80FA5B[redacted]'
    option hostname 'DESKTOP-[redacted]'
    option access_host '1'

config list
    option mac '788972[redacted]'
    option hostname 'LAPTOP-[redacted]'
    option access_host '1'
```

Abbildung S.1: TP-Link AC1200 Mesh Wi-Fi Router - RAM Dateninhalt 'Config List'

Anhang T: TP-Link AC1200 Mesh Wi-Fi Router - Aufbau 'Config White List'

```
config white_list
    option real_mac '00:57:4A:15:40:44'
    option mac '00:57:4A:15:40:44'
    option name '*'
```

Abbildung T.1: TP-Link AC1200 Mesh Wi-Fi Router - RAM Dateninhalt 'Config White List'

Anhang U: TP-Link AC1200 Mesh Wi-Fi Router - Aufbau 'Client List'

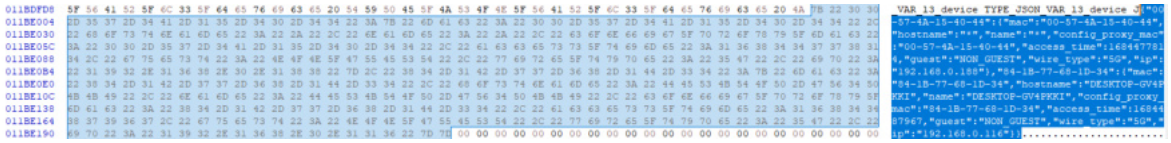

Abbildung U.1: TP-Link AC1200 Mesh Wi-Fi Router - RAM Dateninhalt 'Client List'

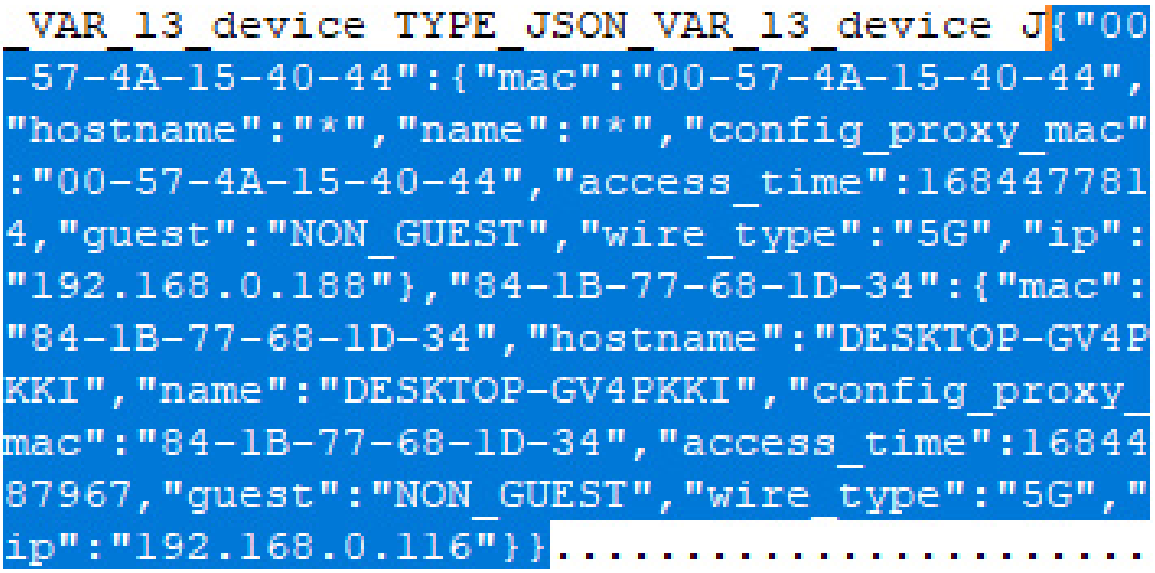

Abbildung U.2: TP-Link AC1200 Mesh Wi-Fi Router - RAM Dateninhalt 'Client List' [Nahansicht]

Anhang V: TP-Link AC1200 Mesh Wi-Fi Router - Aufbau ’DHCP Leases List”

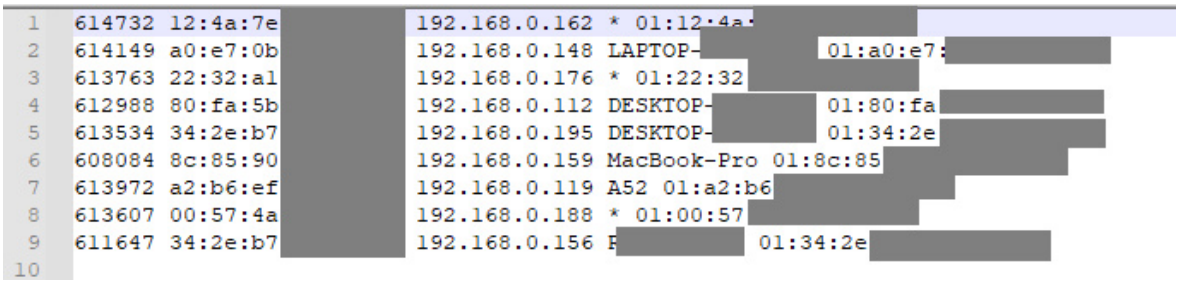

Abbildung V.1: TP-Link AC1200 Mesh Wi-Fi Router - TFTP-Datensicherung ’DHCP Leases List’

Anhang W: TP-Link AC1200 Mesh Wi-Fi Router - Möglich angebundene Speichergeräte (Cloud)

```
root@ArcherC6v2:/# cat tmp/cloud_service.cfg
{
  "global":{
    "sysmode":"ROUTER",
    "account_bind":0
  },
  "service":{
    "account_manage":0,
    "tp_ddns":0,
    "remote_manage":0,
    "private_cloud":0,
    "ifttt":0,
    "alexa":0
  }
}
```

Abbildung W.1: TP-Link AC1200 Mesh Wi-Fi Router - Möglich angebundene Speichergeräte - Cloud

Anhang X: TP-Link AC1200 Mesh Wi-Fi Router - TFTP-Datensicherung Hexansicht access time

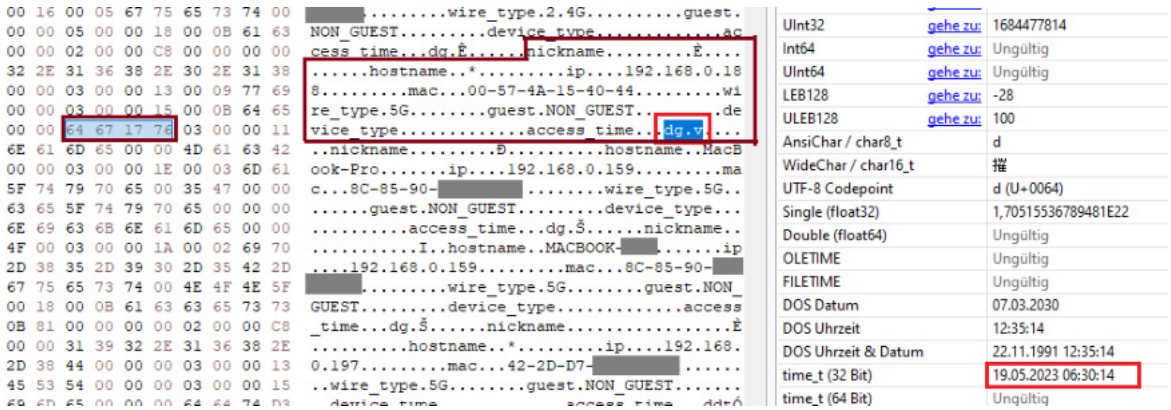

Abbildung X.1: TP-Link AC1200 Mesh Wi-Fi Router - TFTP-Datensicherung _ Hexansicht 'access time'

Anhang Y: Arris - Standard Benutzername und Standard Passwort (nach Gerät)

Model	Benutzername [Standard]	Password [Standard]
Arris WR2100	admin	Password
Arris TG1682G	admin	Password
Arris TG1672G	admin	Password
Arris SBR-AC3200P	admin	Password
Arris SBR-AC1900P	admin	Password
Arris SBG8300	admin	Password
Arris SBG6900-AC	admin	Password
Arris SBG6700-AC	admin	Password
Arris SBG10	admin	Password
Arris SB8200	admin	Password
Arris DG3450	admin	Password
Arris DG950A	admin	Password
Arris DG860P2	admin	Password

Tabelle Y.1: Benutzername [Standart] und Password [Standart] für Arris [64]

Anhang Z: TP-Link - Standard Benutzername und Standard Passwort (nach Gerät)

Model	Benutzername [Standard]	Passwort [Standard]
AC1750	admin	admin
Archer C2	admin	admin
Archer C7	admin	admin
Archer D5	admin	admin
TD-854W	admin	ttnet
TD-8616	admin	admin
TD-8800		admin
TD-8810	admin	admin
TD-8816	admin	admin
TD-8817	admin	admin
TD-8840	admin	admin
TD-8961ND	admin	admin
TD-W8151N	admin	admin
TD-W8901G	admin	admin
TD-W890iG	admin	admin
TD-W8910G	admin	admin
TD-W8920G	admin	admin
TD-W8950ND	admin	admin
TD-W8951ND	admin	admin
TD-W8960N	admin	admin
TD-W8960N	admin	admin
TD-W8960NB	admin	admin
TD-W8961N	admin	admin
TD-W8961NT	admin	admin
TD-W8970	admin	admin
TD-W8980	admin	admin
TD-W8980	admin	admin
TD-W9810G	admin	admin
TL-ER5120		
TL-MR3220	admin	admin
TL-MR3240	admin	admin

Tabelle Z.1: Benutzername [Standart] und Passwort [Standart] für TP-Link [65]

Model	Benutzername [Standard]	Passwort [Standard]
TL-MR3420	admin	admin
TL-R402M	admin	admin
TL-R402M	admin	admin
TL-R460	admin	admin
TL-R460	admin	admin
TL-R470T Plus	admin	admin
TL-R600VPN	admin	admin
TL-WA7210N	admin	admin
TL-WDR4300	admin	admin
TL-WR1043N	admin	admin
TL-WR1043N	admin	admin
TL-WR1043ND	root	admin
TL-WR1043ND	admin	admin
TL-WR1043ND	admin	admin
TL-WR2543ND	admin	admin
TL-WR340G	admin	admin
TL-WR340G	admin	admin
TL-WR340GD	admin	admin
TL-WR541G	admin	admin
TL-WR541G	admin	admin
TL-WR541G	admin	admin
TL-WR542G	admin	admin
TL-WR542G	admin	admin
TL-WR542G	admin	admin
TL-WR641G	admin	admin
TL-WR642G	admin	admin
TL-WR642G	admin	admin
TL-WR720N	admin	admin
TL-WR740N	admin	admin
TL-WR740ND	admin	admin
TL-WR741N	admin	admin
TL-WR741ND	admin	admin
TL-WR743ND	admin	admin
TL-WR841N	admin	admin
TL-WR841ND	admin	admin
TL-WR842N	admin	admin
TL-WR842ND	admin	admin
TL-WR940N	admin	admin
TL-WR941ND	admin	admin
TP	root	sohoadmin

Tabelle Z.2: Benutzername [Standart] und Passwort [Standart] für TP-Link [65]

Anhang : Nützliche Windows Kommandozeilenbefehle

Kommando	Bedeutung
ipconfig	IP Konfiguration IP Adressen des Rechners worunter dieses im Netzwerk aufgerufen werden kann
arp -a	Adress Resolution Protocoll Zeigt ARP Tabelle, Schnittstelle, Internetadresse, Physische Adresse, Typ
nmap -A IP	Portscan mit Portnummer, Status (offen / geschlossen), Service, Version, MAC Adresse und SSID -A: Betriebssystem, Version, Script scanning, Traceroute
SSH root@server	SSH Verbindungsaufbau
Telnet o IP	Telnet Verbindungsaufbau

Tabelle .1: Verwendete Windows Kommandozeilenbefehle

Literaturverzeichnis

[1] I. D21. „Anteil der Onliner, mobilen Internetnutzer und Nutzungsplaner in Deutschland im Jahr 2021“. deutsch, Initiative D21. (), Adresse: https://de.statista.com/statistik/daten/studie/13077/umfrage/internetnutzung-in-deutschland-im-jahr-2009/ (besucht am 29. 04. 2023).

[2] F. Tenzer. „Durchschnittliche tägliche Nutzungsdauer von Smartphones in Deutschland im Jahr 2023 nach Altersgruppe (in Minuten)“. deutsh, Bitkom Research. (), Adresse: https://de.statista.com/statistik/daten/studie/714974/umfrage/taegliche-nutzungsdauer-von-smartphones-in-deutschland/ (besucht am 25. 04. 2023).

[3] I. D21. „Anteil der mobilen Internetnutzer in Deutschland in den Jahren 2015 bis 2022“. deutsch, Initiative D21. (), Adresse: https://de.statista.com/statistik/daten/studie/633698/umfrage/anteil-der-mobilen-internetnutzer-in-deutschland/ (besucht am 29. 04. 2023).

[4] Murmuras. „Durchschnittliche tägliche Smartphone-Nutzung nach App Kategorien in Deutschland 2020, (in Minuten)“. deutsch, murmuras.com. (), Adresse: https://de.statista.com/statistik/daten/studie/1186676/umfrage/durchschnittliche-taegliche-smartphone-nutzung-nach-apps/ (besucht am 27. 06. 2023).

[5] Eurostat. „Anteil der Personen in Deutschland, die das Internet zum Telefonieren oder Videoanrufe nutzen, in den Jahren 2008 bis 2022“. deutsch, Eurostat. (), Adresse: https://de.statista.com/statistik/daten/studie/457978/umfrage/nutzung-von-internettelefonie-oder-videotelefonie-in-deutschland/ (besucht am 29. 04. 2023).

[6] CNKIONLINE und (. SYED ZAIN UL HASSAN et al, „Wireless router forensics: Finding artifacts of suspect traces with a raspberry pi and Kali Linux“, S. 502–525, Dez. 2022. DOI: 10.17605/OSF.IO/RK4YF.

[7] D. Blackman und P. Szewczyk, „The challenges of seizing and searching the contents of Wi-Fi devices for the modern investigator“, Jg. 41, S. 37–48, 2015. DOI: 10.4225/75/57b3f385fb887.

[8] kurthelectronic.de. „Wie funktioniert ein IT-Netzwerk?“ deutsch, Kurth Electronic GmbH. (2022), Adresse: https://www.kurthelectronic.de/fachwissen/wie-funktioniert-ein-it-netzwerk/?cn-reloaded=1 (besucht am 27. 06. 2023).

[9] heimnetzwerke.net. „Router - Was ist das? Einfach erklärt“. deutsch, heimnetzwerke.net. (), Adresse: https://www.heimnetzwerke.net/router-einfach-erklaert/#:~:text=Im%20Heimnetzwerk%20ist%20der%20Router,WLAN%20und%20dem%20%C3%B6ffentlichen%20Internet.&text=Im%20Heimnetzwerk%20ist%20der%20Router%20f%C3%BCr%20den%20Internetzugang%20zust%C3%A4ndig.,-Das%20bedeutet,%20er (besucht am 27. 06. 2023).

[10] Wikipedia, *Wireless Local Area Network — Wikipedia, die freie Enzyklopädie*, [Online; Stand 24. April 2023; 21:00 Uhr], 2022. Adresse: https://de.wikipedia.org/w/index.php?title=Wireless_Local_Area_Network&oldid=228062963.

[11] Wikipedia, *IEEE 802.11 — Wikipedia, die freie Enzyklopädie*, [Online; Stand 24. April 2023; 21:20 Uhr], 2022. Adresse: https://de.wikipedia.org/w/index.php?title=IEEE_802.11&oldid=227349293.

[12] Wikipedia, *OSI-Modell — Wikipedia, die freie Enzyklopädie*, [Online; Stand 24. April 2023; 21:54 Uhr], 2022. Adresse: https://de.wikipedia.org/w/index.php?title=OSI-Modell&oldid=227339064.

[13] Wikipedia, *Wireless Access Point — Wikipedia, die freie Enzyklopädie*, [Online; Stand 25. April 2023], 2022. Adresse: https://de.wikipedia.org/w/index.php?title=Wireless_Access_Point&oldid=224998722.

[14] „Telnet“. deutsch, TechTarget. (), Adresse: https://www.computerweekly.com/de/definition/Telnet (besucht am 27. 04. 2023).

[15] I. SE. „Was Telnet ist und wie man es aktiviert“. deutsch. (), Adresse: https://www.ionos.de/digitalguide/server/tools/telnet-das-systemuebergreifende-remote-protokoll/ (besucht am 28. 04. 2023).

[16] R. S. G. C. KG. „UART verstehen, Grundlagen von Oszilloskopen und Tastköpfen“. deutsch, Rohde Schwarz GmbH Co. KG. (2023), Adresse: https://www.rohde-schwarz.com/de/produkte/messtechnik/essentials-test-equipment/digital-oscilloscopes/uart-verstehen_254524.html (besucht am 22. 04. 2023).

[17] J. Weissgärber. „Die UART Schnittstelle“. deutsch, Jirka Weissgärber. (2. März 2019), Adresse: http://www.mathe-mit-methode.com/schlaufuchs_web/elektrotechnik/mikrocontroller_lernmaterial/microcontroller_allgemein/mikrocontroller_ext_hardware/mikrocontroller_uart.html (besucht am 23. 04. 2023).

[18] Conrad. „USB » Wie funktioniert es was bedeutet es?“ deutsch. (26. Okt. 2022), Adresse: https://www.conrad.de/de/ratgeber/technik-einfach-erklaert/usb.html (besucht am 12. 02. 2023).

[19] reichelt elektronik GmbH Co. KG. „USB Stick“. deutsch, reichelt elektronik GmbH Co. KG. (12. Apr. 2023), Adresse: https://www.reichelt.de/de/de/usb-sticks-c4798.html?r=1 (besucht am 22. 04. 2023).

[20] I. T. M. GmbH. „Was ist Ethernet?, Ohne Ethernet-Protokoll kein globales Kommunikationsnetzwerk. Das sollten Sie wissen.“ deutsch, IDG Tech Media GmbH. (14. März 2023), Adresse: https://www.computerwoche.de/a/was-ist-ethernet,3553178 (besucht am 23. 04. 2023).

[21] R. Schanze. „Was ist Ethernet? – einfach erklärt“. deutsch, GIGA. (), Adresse: https://www.giga.de/artikel/was-ist-ethernet-einfach-erklaert/ (besucht am 23. 04. 2023).

[22] Elektronik-Kompendium.de. „IEEE 802.3 / Ethernet-Grundlagen“. deutsch, Elektronik-Kompendium.de. (), Adresse: https://www.elektronik-kompendium.de/sites/net/0603201.htm (besucht am 23. 04. 2023).

[23] smallnetbuilder.com. „Marktanteile von Router-Herstellern an den Verkäufen auf Amazon.com* im 1. Quartal 2015“. deutsch, smallnetbuilder.com. (), Adresse: https://de.statista.com/statistik/daten/studie/552509/umfrage/marktanteile-von-router-herstellern-am-absatz-auf-amazoncom/ (besucht am 28. 04. 2023).

[24] Amazon.com. „Bestseller in Wireless Access Points“. deutsch, Amazon.com. (), Adresse: https://www.amazon.de/gp/bestsellers/computers/430155031 (besucht am 27. 06. 2023).

[25] Amazon.com. „Bestseller in Router“, Amazon.com. (), Adresse: https://www.amazon.de/gp/bestsellers/computers/430154031 (besucht am 02. 05. 2023).

[26] T.-L. Corporation. „Konzernprofil, Über TP-Link“. englisch, TP-Link Corporation. (7. Juni 2021), Adresse: https://www.tp-link.com/de/about-us/corporate-profile/ (besucht am 27. 04. 2023).

[27] T.-L. C. Limited. „Im 12. Jahr in Folge: TP-Link ist weltweite Nummer 1 der WiFi-Produktanbieter“. deutsch, TP-Link Corporation Limited. (13. Apr. 2023), Adresse: https://www.tp-link.com/de/press/news/20563/ (besucht am 27. 04. 2023).

[28] I. Hassa. „Breitband Report Deutschland, Der deutsche Breitbandmarkt im Profil“. deutsch, DSLWEB. (5. Sep. 2022), Adresse: https://www.dslweb.de/breitband-report-deutschland.php (besucht am 27. 04. 2023).

[29] I. Hassa. „Breitbandmarkt 2020: Wachstum im Krisenjahr, DSLWEB Breitband Report Deutschland 2020“, DSLWEB. (), Adresse: https://www.dslweb.de/breitband-report-deutschland-2020.php (besucht am 27. 04. 2023).

[30] TechInfoDepot. „Arris TG3442“. deutsch, TechInfoDepot. (), Adresse: http://en.techinfodepot.shoutwiki.com/wiki/Arris_TG3442 (besucht am 17. 05. 2023).

[31] A. Sawall. „Kabelnetzausrüster Arris für 7,4 Milliarden Dollar verkauft, COMMSCOPE“. deutsch, Golem.de. (), Adresse: https://www.golem.de/news/commscope-kabelnetzausruester-arris-fuer-7-4-milliarden-dollar-verkauft-1811-137625.html (besucht am 19. 05. 2023).

[32] WikiDevi.Wi-Cat.RU. „Arris TG3442“. englisch, WikiDevi.Wi-Cat.RU. (), Adresse: https://wikidevi.wi-cat.ru/Arris_TG3442 (besucht am 17. 05. 2023).

[33] I. Micron Technology. „Orderable parts, MT41K256M16TW-107:P“. englisch, Micron Technology, Inc. (), Adresse: https://www.micron.com/products/dram/ddr3-sdram/part-catalog/mt41k256m16tw-107 (besucht am 16. 05. 2023).

[34] TechInfoDepot. „Arris“. deutsch, TechInfoDepot. (), Adresse: http://en.techinfodepot.shoutwiki.com/wiki/Arris (besucht am 17. 05. 2023).

[35] TechInfoDepot. „Arris TG3452“. englisch, TechInfoDepot. (), Adresse: http://en.techinfodepot.shoutwiki.com/wiki/Arris_TG3452 (besucht am 20. 05. 2023).

[36] I. Mouser Electronics. „FHCE2752-R3S7“. deutsch, Mouser Electronics, Inc. (), Adresse: https://www.mouser.de/ProductDetail/MaxLinear/FHCE2752-R3S7?qs=aP1CjGhiNiGfKlHc2jI4qA== (besucht am 20. 05. 2023).

[37] TechInfoDepot. „Intel/Intel Puma“. deutsch, TechInfoDepot. (), Adresse: http://en.techinfodepot.shoutwiki.com/wiki/Intel/Intel_Puma (besucht am 20. 05. 2023).

[38] TechInfoDepot. „Arris DG3450“. englisch, TechInfoDepot. (), Adresse: http://en.techinfodepot.shoutwiki.com/wiki/Arris_DG3450 (besucht am 20. 05. 2023).

[39] TechInfoDepot. „Arris SBG8300“. englisch, TechInfoDepot. (), Adresse: http://en.techinfodepot.shoutwiki.com/wiki/Arris_SBG8300 (besucht am 21. 05. 2023).

[40] nox-x. „TG3442DE-Teardown, Were you able to dump the firmware?“ englisch, nox-x. (), Adresse: https://github.com/nox-x/TG3442DE-Teardown/issues/3 (besucht am 17. 05. 2023).

[41] nox-x. „Were you able to dump the firmware? 3“. englisch, GitHub, Inc. (), Adresse: https://github.com/nox-x/TG3442DE-Teardown/issues/3 (besucht am 02. 07. 2023).

[42] T. Instruments. „SN74AVC2T245, Dual-Bit Dual-Supply Bus Transceiver with Configurable Level-Shifting /Voltage Translation and Tri-State Outputs“. englisch, Texas Instruments. (), Adresse: https://www.ti.com/lit/ds/symlink/sn74avc2t245.pdf?ts=1691737300981&ref_url=https%253A%252F%252Fwww.google.com%252F (besucht am 22. 05. 2023).

[43] nox-x. „TG3442DE-Teardown/Hardware“. englisch, GitHub, Inc. (), Adresse: https://github.com/nox-x/TG3442DE-Teardown/blob/main/Hardware.md (besucht am 01. 07. 2023).

[44] M. C. R. Quick. „VM Super Hub 3 Teardown | Arris TG2492 Teardown“. englisch, Mobile Computer Repairs Quick. (), Adresse: https://www.mobile-computer-repairs.co.uk/arris-tg2492.html (besucht am 01. 07. 2023).

[45] A. E. LLC., „Touchstone TG3442DE Telefonie-Gateway, Über Ihr neues Telefonie-Gateway“, deutsch, S. 11, Adresse: https://kabel.vodafone.de/static/media/Arris_VodafoneStation_TG344DE.pdf (besucht am 23. 05. 2023).

[46] tmomas. „Techdata: TP-Link Archer C6 v2 (EU, RU)“. Englisch, OpenWrt. (2. Mai 2023), Adresse: https://openwrt.org/toh/hwdata/tp-link/tp-link_archer_c6_v2_eu (besucht am 05. 05. 2023).

[47] G. Vlaev. „ath79: add support for TP-Link Archer C6 v2“. Englisch, OpenWrt. (28. Dez. 2018), Adresse: https://git.openwrt.org/?p=openwrt/openwrt.git;a=commit;h=d03aae1a09fce5a5d5747855bc07ee1f54388e03 (besucht am 05. 05. 2023).

[48] T.-L. C. Limited. „AC1200 MU-MIMO Dualband-Gigabit-WLAN-Router“. deutsch, TP-Link Corporation Limited. (), Adresse: https://www.tp-link.com/de/home-networking/wifi-router/archer-c6/v2/ (besucht am 16. 05. 2023).

[49] Arrow. „QCA9561-AL3A, 802.11 Wireless LAN“. englisch, Arrow. (), Adresse: https://www.arrow.com/en/products/qca9561-al3a/qualcomm (besucht am 06. 05. 2023).

[50] I. Qualcomm Technologies. „QCA9531“. englisch, Qualcomm Technologies, Inc. (), Adresse: https://www.qualcomm.com/products/technology/wi-fi/qca9531 (besucht am 06. 05. 2023).

[51] T.-L. C. Limited. „Introduction“. englisch, TP-Link Corporation Limited. (), Adresse: https://www.tplinkcloud.com/ (besucht am 02. 06. 2023).

[52] D. Skowroński. „Hacking into TP-Link Archer C6 – shell access without physical disassembly“. englisch. (21. Feb. 2021), Adresse: https://skowronski.tech/2021/02/hacking-into-tp-link-archer-c6-shell-access-without-physical-disassembly/ (besucht am 06. 05. 2023).

[53] T.-L. C. Limited. „Why SSH TCP port 22 is tested as open?, QA of functional explanation or specification parameters“. Englisch, TP-Link Corporation Limited. (1. Feb. 2020), Adresse: https://www.tp-link.com/us/support/faq/2462/ (besucht am 06. 05. 2023).

[54] V. Gite. „So überprüfen und verwenden Sie serielle Ports unter Linux“. englisch, nixCraft. (), Adresse: https://www.cyberciti.biz/faq/find-out-linux-serial-ports-with-setserial/ (besucht am 29. 05. 2023).

[55] SiliconExpert. „QCA8337N-AL3C, Ethernet Switch 7-Port 1000Mbps 148-Pin QFN EP Tray“. englisch, SiliconExpert. (), Adresse: https://www.datasheets.com/en/part-details/qca8337n-al3c-qualcomm-73536426#datasheet (besucht am 06. 05. 2023).

[56] odon-noda. „TP-Link Archer C6 v2“. Englisch, OpenWrt. (22. Dez. 2022), Adresse: https://openwrt.org/toh/tp-link/archer_c6_v2?s[]=tp&s[]=link&s[]=archer&s[]=c6 (besucht am 05. 05. 2023).

[57] E. Kompendium. „DHCP - Dynamic Host Configuration Protocol“. deutsch, Elektronik-Kompendium.de. (), Adresse: https://www.elektronik-kompendium.de/sites/net/0812221.htm (besucht am 01. 07. 2023).

[58] v.-k. Deland-Han eross-msft. „DHCP (Dynamic Host Configuration Protocol) – Grundlagen“. deutsch, Microsoft 2023. (14. Apr. 2023), Adresse: https://learn.microsoft.com/de-de/windows-server/troubleshoot/dynamic-host-configuration-protocol-basics (besucht am 21. 06. 2023).

[59] techinfodepot. „Arris DG3450“. englisch, techinfodepot. (), Adresse: http://en.techinfodepot.shoutwiki.com/wiki/Arris_DG3450 (besucht am 02. 07. 2023).

[60] B. Rodrigues. „ARRIS Cable Modem has a Backdoor in the Backdoor“. englisch, w00tsec. (), Adresse: https://w00tsec.blogspot.com/2015/11/arris-cable-modem-has-backdoor-in.html (besucht am 02. 07. 2023).

[61] FCC.report. „Interne Fotos, FCC-ID: UIDTG3452“. englisch, FCC.report. (28. Nov. 2017), Adresse: https://fcc.report/FCC-ID/UIDTG3452/3411096 (besucht am 21. 05. 2023).

[62] FCC.report. „Interne Fotos, FCC-ID:“ englisch, FCC.report. (9. Jan. 2021), Adresse: https://fcc.report/FCC-ID/UIDTG3442/4802873 (besucht am 21. 05. 2023).

[63] I. Qualcomm Atheros, „QCA9563 802.11n 3x3 2.4 GHzPremium SOC for WLAN Platforms, Data Sheet“, Englisch, S. 22, Adresse: https://www.datasheets.com/en/part-details/qca8337n-al3c-qualcomm-73536426#datasheet (besucht am 06. 05. 2023).

[64] „Semantische Suche“. englisch, TechInfoDepot. (), Adresse: http://en.techinfodepot.shoutwiki.com/w/index.php?title=Special:Ask&q=[[Global+type::~embedded+system*]]+[[Default+login+user::admin]]+[[Default+login+pass::password]]+[[Brand::Arris]]&po=?Embedded+system+type=Type%20?Manuf%20?Manuf+product+model%20?Supported+802dot11+protocols=PHY+modes%20?Default+IP+address=Default+IP%20?Default+login+user=User%20?Default+login+pass=Pass%20?Default+SSID%20?OUI%20?OUI+(ethernet)=OUI+(Eth)%20?Estimated+year+of+release=Est.+year&eq=yes&p[format]=broadtable&order[0]=ASC&sort_num=&order_num=ASC&p[limit]=3500&p[offset]=&p[link]=all&p[sort]=&p[headers]=show&p[mainlabel]=&p[intro]=&p[outro]=&p[searchlabel]=%E2%80%A6+further+results&p[default]=&p[class]=sortable+wikitable+smwtable (besucht am 20. 05. 2023).

[65] H. N. Admin. „TP-Link Default Passwords“. englisch, Home Network Admin. (2023), Adresse: https://homenetworkadmin.com/default-router-passwords/TP-Link/ (besucht am 11. 05. 2023).

Eidesstattliche Erklärung

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

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

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

Mittweida, 11. August 2023	
Ort, Datum	Sandra Schmidt