

Projektarbeit im Fernstudiengang „IT-Forensik“

Analyse und Auswertung von Überwachungs-Tools für Kinder

Eingereicht am: 08.06.2022
von: Lennart Bigalsky

I. Inhaltsverzeichnis

1. Einleitung und Problemstellung	4
2. Auswahl der zu untersuchenden Soft- und Hardware	5
2.1 Software	5
2.1.1 Einleitung	5
2.1.2 Auswahlkriterien	6
2.1.2.1 Funktionsumfang	6
2.1.2.2 Betrachtung der Hersteller	8
2.1.2.3 Preis	9
2.1.2.4 Betriebssysteme	11
2.1.3 Entscheidung	11
2.2 Hardware	11
2.2.1 Einleitung, Auswahlkriterien und Entscheidung	11
3. Analyse der Kommunikation	13
3.1 Versuchsaufbau	13
3.1.1 Versuchsaufbau Software-Tracker	13
3.1.2 Testgeräte	13
3.1.3 Tools	13
3.1.3.1 Wireshark	14
3.1.3.2 Burp Suite	14
3.1.3.3 Einrichtung	14
3.1.4 Bestimmung Parameter	16
3.1.4.1 Messzeitraum	16
3.1.4.2 Testszenarien	16
3.1.4.3 Wiederholbarkeit	16
3.1.4.4 Durchführung der Messung	16
3.1.5 Messungen	17
3.1.5.1 Messung ohne Tracking-App – Grundzustand	17
3.1.5.2 Messung nach Installation der Tracking-App	19
3.1.5.3 Messung mit konfigurierter, im Hintergrund laufenden App	21
3.1.5.4 geöffnete App mit Interaktion	25
3.2 Versuchsaufbau Hardware-Tracker	28
3.2.2 Testgeräte	28
3.2.3 Tools	28
3.2.4 Bestimmung Parameter	29

3.2.4.1 Messzeitraum.....	29
3.2.4.2 Testszenarien.....	29
3.2.4.3 Wiederholbarkeit.....	29
3.2.4.4 Durchführung der Messung	29
3.2.5 Messungen	30
3.2.5.1 Messung nach Installation der Tracking-App.....	30
3.2.5.2 Messung mit konfigurierter, im Hintergrund laufenden App	31
3.2.5.3 geöffnete App mit Interaktion.....	33
4. Rechtliches und moralisches.....	35
5. Fazit.....	37
II. Literaturverzeichnis	38
III. Abbildungsverzeichnis.....	41
IV. Tabellenverzeichnis.....	42

1. Einleitung und Problemstellung

„Fast 200 Kinder unter 14 gelten als vermisst“¹. Mit dieser Headline eröffnen die Stuttgarter Nachrichten ihren Artikel zur Erinnerung an den Tag der vermissten Kinder, welcher seit 2002 als offizieller Gedenktag am 25. Mai praktiziert wird.

Deutschlandweit sind 2021 um die 84.000 Kinder und Jugendliche als vermisst gemeldet worden². Die Aufklärungsquote beträgt hier aber auch ca. 97%, da die meisten Fälle zwischen weniger Stunden bis einer Woche abgeschlossen werden können³.

Für viele Eltern ist das Verschwinden ihrer Kinder ein Horrorszenario. Um jederzeit Gewissheit über den Standort oder die Vorgänge im Leben ihrer Kinder zu erhalten, greifen diese auf die heutige Möglichkeit der technischen Überwachung zurück. In Form von GPS-Trackern als Anhänger, Smart Watches mit Trackern oder Apps, die im Rahmen von Geräteüberwachungen auf den Smartphones der Sprösslinge installiert und online verwaltet werden.

Ziel dieser Hausarbeit soll es sein, den Netzwerk-Traffic eines Hardware-Trackers mit Verwaltungs-App, als auch einer reinen Kontroll-App, mit einer Netzwerk-Traffic Anwendung aufzunehmen, zu analysieren und auszuwerten. Weiterhin werden rechtlichen Aspekte der Überwachung von Kindern und Jugendlichen betrachtet.

¹ StN.de

² vgl. BKA Vermisstenfälle

³ vgl. StN.de

2. Auswahl der zu untersuchenden Soft- und Hardware

2.1 Software

2.1.1 Einleitung

Die Nutzung eines Software-Trackers setzt voraus, dass das zu überwachende Individuum über ein kompatibles Gerät verfügt. Bei einer Umfrage im Jahr 2020 besaßen bereits fast die Hälfte der Kinder ab 6 Jahren ein eigenes Handy oder Smartphone⁴ (s. Abbildung 1).

Welche Geräte besitzt Ihr Kind?

Persönlicher Gerätebesitz von Kindern in Deutschland 2020 (nach Geschlecht)

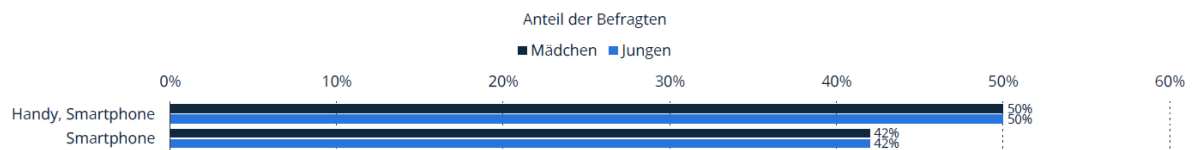


Abbildung 1: Ausschnitt der Statistik zur Anzahl der Kinder mit eigenem Smartphone / Handy; Quelle mpfs / statista.de

Ab einem Alter ab 12 Jahren waren es bereits ca. 90%⁵ (s. Abbildung 2). Diese Voraussetzung kann daher im Test als erfüllt betrachtet werden.

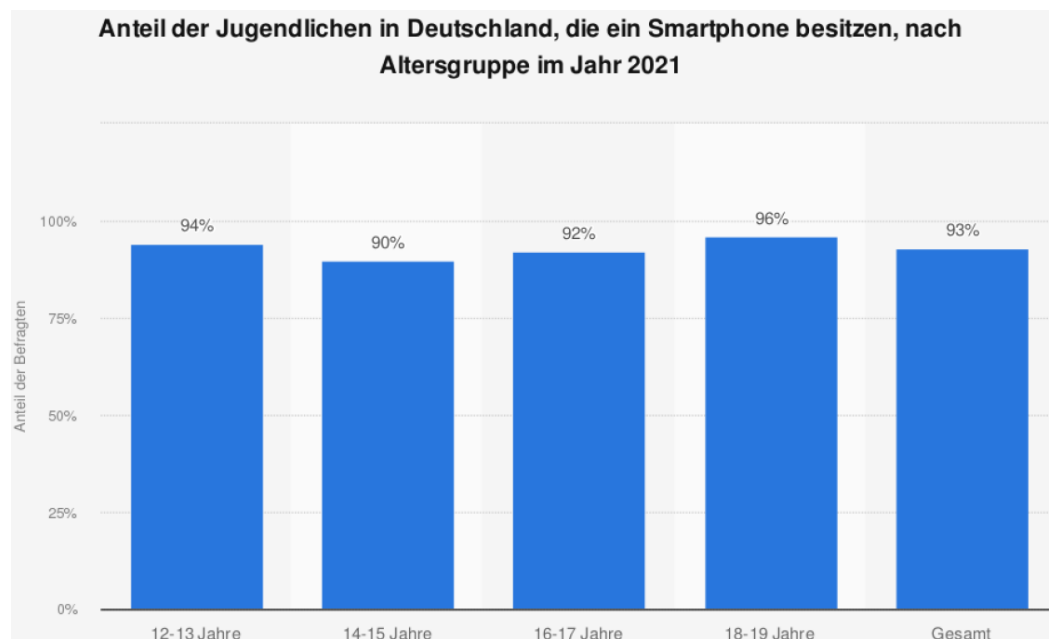


Abbildung 2: Statistik zum Anteil der Jugendlichen mit eigenem Smartphone nach Altersgruppen im Jahr 2021; Quelle: mpfs / statista.de

⁴ Mediennutzung Kinder, S. 7, s. Beschreibung [KIM-Studie 2020]

⁵ Smartphone-Besitz Jugendliche [JIM-Studie 2021]

Im ersten Schritt müssen die in Betracht zu ziehenden Apps ausgewählt werden. Aufgrund der Tatsache, dass es eine große Anzahl an Anwendungen und Apps zur Kontrolle von Kindern auf dem Markt gibt, wurden ein paar Anwendungen aus dieser Menge herausgesucht, die in den weiteren Schritten untereinander verglichen werden. Folgende Apps wurden vorselektiert:

- Mein iPhone suchen,
- FamiSafe Kinder,
- Norton Family Parental Control,
- ESET Parental Control,
- Family Locator,
- Find my Kids,
- Kaspersky Safe Kids und
- MMGuardian Kindersicherung.

2.1.2 Auswahlkriterien

2.1.2.1 Funktionsumfang

Der Funktionsumfang einer App ist ein Kriterium, welches bei der Auswahl in Betracht gezogen werden muss. Mehr Funktionen können mehr Netzwerk-Traffic bedeuten, lassen dann aber eventuell keinen Rückschluss auf die spezifische Funktion ziehen, die den Traffic auslöst. Dem entgegen stehen Apps mit weniger Funktionsumfang, die jedoch weniger Traffic generieren, dieser jedoch einer bestimmten Funktion zugeordnet werden könnte.

Bei den genannten Anwendungen wurden die vorhandenen Features von den jeweiligen Websites der Hersteller entnommen. Ein Ausschnitt der Tabelle, in der verschiedenen Auswahlkriterien aufgeführt wurden, kann in folgender Abbildung erkannt werden.

App	OS	Kosten	Funktionen	Besonderheiten
Mein iPhone suchen	iOS	free, integrierte Funktion in Apple-Produkten	<ul style="list-style-type: none"> + Ton wiedergeben + Modus "verloren" + iPhone löschen + Positionsüberwachung 	+ Ortungsdienst muss an Gerät eingeschaltet sein, außer Modus "verloren" wird aktiviert
FamiSafe Kinder	Android, iOS, Windows, Mac	3d Trial; Abopläne: - 9.99€/M bis 5 Geräte - 59.99€/12M bis 10/30 Geräte - 19.99€/4M bis 10 Geräte	<ul style="list-style-type: none"> + Berichte + Nutzungs-Zeit Kontrolle + Youtube App Control + TikTok History + Browser History + Safe Search + Webüberwachung nach Kategorien und URLs + Standortverlauf + Geofencing + App Block + Social Network / Message Kontrolle + Galerie Kontrolle auf Pornografische Inhalte 	<ul style="list-style-type: none"> + 3 Awards in 2020 + Account bei Nutzung benötigt (wg. Abo-Plan) + technischer Support i.d.R. innerhalb 24Std + Deinstallationsschutz + Keine Berichte (Aktivität, Browser, App-Nutzung) auf iOS, nur auf Android möglich + RSA-Verschlüsselung bei Datenübertragung
Norton Family Parental Control	Android, iOS	30d Trial; 39.99€/Jahr	<ul style="list-style-type: none"> + Webüberwachung (W, I, A) + Online-Zeit (W, I, A) + Safe Search (W, I, A) + Überwachung YouTube (W, I, A) + Überwachung inst. Apps (A) + Berichte (W, I, A) + Elternportal (W, I, A) + Zugriffsanfrage (I, A) + Gerätesperrung (W, I, A) + Meldung bei Aufruf geblockter Inhalte (W, I, A) + School Time (W, I, A) - Positionsüberwachung 	<ul style="list-style-type: none"> - Die Kindersicherung kann nur auf dem Windows-PC oder dem iOS- und Android-Gerät eines Kindes installiert und verwendet werden. Es sind nicht alle Funktionen auf allen Plattformen verfügbar. Eltern können die Aktivitäten ihres Kindes von jedem Gerät aus – Windows PC (mit Ausnahme von Windows 10 im S-Modus), Mac, iOS und Android – über unsere mobile App überwachen und verwalten oder sich zu diesem Zweck mit einem beliebigen Browser (außer Internet Explorer) bei ihrem Konto unter my.Norton.com einloggen und "Kindersicherung" auswählen. - Die Videoüberwachung überwacht Videos, die sich Ihre Kinder auf YouTube.com ansehen. Der Service überwacht oder verfolgt keine YouTube-Videos, die in anderen Websites oder Blogs eingebettet sind. - Die mobile App muss separat heruntergeladen werden. + unbegrenzte Anzahl Geräte

Tabelle 1: Ausschnitt Aufstellung Apps

Um nun die Anwendungen vergleichen zu können, werden diese anhand der gefundenen Funktionen gegenübergestellt. Dies kann in dem folgenden Ausschnitt der Tabelle erkannt werden.

App	Ton wiedergebe n	Postions- überwachung	Berichte	Nutzungs- zeit- Kontrolle	Youtube Kontrolle	TikTok History	Browser History	Safe Search
Mein iPhone suchen	x	x						
FamiSafe Kinder		x	x	x	x	x	x	x
Norton Family Parental Control		-	x		x			x
ESET Parental Control		x	x	x				x
Family Locator		x						
Find my Kids		x		x				
Kaspersky Safekids		x	x	x	x			
MMGuardian Kindersicherung		x		x				

Tabelle 2: Ausschnitt Vergleich der App-Funktionen

Hier nun das zusammenfassende Ergebnis der Aufstellung aus der Tabelle 2:

App	Funktionsanzahl
Mein iPhone suchen	2
FamiSafe Kinder	14
Norton Family Parental Control	9
ESET Parental Control	10
Family Locator	5
Find my Kids	5
Kaspersky Safe Kids	12
MMGuardian Kindersicherung	8

Tabelle 3: Anzahl der App-Funktionen

Wie bereits einleitend zum Funktionsumfang als Auswahlkriterium erläutert, könnte ein hoher Funktionsumfang mehr Netzwerk- und Daten-Traffic bedeuten, was eventuell ein Auslesen dessen erleichtert. Daher wird für diese Ausarbeitung nun entschieden, dass die zu untersuchende App einen hohen Funktionsumfang enthalten soll, der daraufhin analysiert werden kann. Dadurch entfallen 5 von 8 vorselektierten Apps und es verbleibe „FamiSafe Kinder“, „Kaspersky Safe Kids“ und „ESET Parental Control“.

2.1.2.2 Betrachtung der Hersteller

Eine Betrachtung der Hersteller kann ein weiteres Auswahlkriterium darstellen. Der Grund hierfür ist, dass man einen ersten Eindruck über deren Seriosität und eventuell auch Sicherheitsverständnis erhalten kann. Von Entwicklern, die Anwendungen und Apps in der Sicherheitsbranche programmieren, wird durch ihre Erfahrung ein höheres Verständnis für z.B. die verschlüsselte Übertragung von Daten, erwartet als von denen, die Programme im Unterhaltungsbereich, wie z.B. Spiele, entwickeln.

ESET und Kaspersky sind bekannte Marken im Bereich der Antiviren-Programme und befinden sich unter den Top Ten der „besten Schutzprogramme gegen Trojaner, Ransomware, Spyware und [anderen] Internet-Bedrohungen“⁶.

ESET, eine Firma, die seit ihrer Gründung 1992 in der Slowakei Sicherheitssoftware entwickelt, bietet eine Produktpalette für den Heimanwender bis zu Großunternehmen. Mit

⁶ Computer Bild AV-Vergleich

über 110 Millionen Nutzern und über 400.000 Unternehmen in über 200 Länder und Regionen wirbt ESET für ihre Kompetenzen in der Branche für Anwendungen im IT-Sicherheitsbereich⁷.

Kaspersky Lab, die ebenfalls Sicherheitssoftware für Heimanwender und Unternehmen jeglicher Größen entwickeln, kann aufgrund ihrer Gründung 1997 auf 25 Jahre Erfahrung im Bereich der IT-Sicherheit, und über 400 Millionen Nutzern in ebenfalls mehr als 200 Länder und Regionen, zurückgreifen⁸. Wegen der ursprünglichen Gründung in Russland und der russischen Nationalität des Gründers von Kaspersky Lab, Jewgeni Walentinowitsch Kasperski, und der aktuell anhaltenden Kriegssituation zwischen Russland und der Ukraine, wurde vom BSI am 15.03.2022 eine Pressemeldung veröffentlicht, die vor einem weiteren Einsatz der Softwarelösungen des Unternehmens Kaspersky warnt. Da in der heutigen Zeit Kriege nicht mehr nur in der realen Welt, sondern auch durch Cyber-Operationen geführt werden (z.B. Hackerangriffe auf die nationale Stromversorgung der Ukraine⁹), könne nicht ausgeschlossen werden, dass durch „verbundene echtzeitfähigen Clouddienste“¹⁰ und den staatlichen Zwang die verbundenen Ressourcen missbraucht werden könnten¹¹. Kasperski hat als Reaktion in einem offenen Brief sämtliche Anschuldigungen von sich bzw. seiner Firma abgewiesen und auf die langjährige Transparenz seiner „[Quellcodes, [...] Updates, [...] [Architekturen] und [...] Prozesse in den Transparenzzentren Kasperskys in Europa“¹² verwiesen.

FamiSafe dagegen ist ein Produkt der Wondershare Technology Co., Ltd, die mit Hauptsitz in Shenzhen, China, im Unterschied zu ESET und Kaspersky, verschiedenste Produkte im Bereich Konsumenten-Software entwickeln und anbieten¹³. Dennoch wirbt Wondershare bei ihrer App FamiSafe Kinder damit, RSA-verschlüsselte Datenübertragung implementiert zu haben und kann mit 3 Awards aufwarten.

2.1.2.3 Preis

„Zahlst du nichts für ein Produkt oder für eine Dienstleistung, bist du selbst das Produkt – und du bezahlst mit deinen Daten.“ So ungefähr lautet die Weisheit, die es seit bereits Anfang der 1970er Jahre aus dem Bereich der Fernsehwerbung gibt¹⁴.

⁷ vgl. Über ESET

⁸ vgl. Über Kaspersky

⁹ vgl. FR – russ. Cyberangriff

¹⁰ Pressemeldung BSI

¹¹ Pressemeldung BSI

¹² Reaktion Kasperski, offener Brief

¹³ vgl. Bloomberg

¹⁴ vgl. Quora – Daten als Produkt

Doch auch in dem Fall, dass man für etwas bezahlt, bedeutet das nicht, dass der Betreiber einer App nicht dennoch so viele Daten von einem sammeln möchte, wie möglich. Cisco Systems hatte in ihrem White Paper „Cisco Global Cloud Index“ von 2018 Daten aus den Jahren 2016 und 2017 erhoben und bis 2021 eine Prognose zur weltweiten Speicherauslastung in Rechenzentren abgegeben. Wie in Abbildung 3 zu sehen, sind 2016 global bereits 286 Exabytes ($\equiv 307090161664$ Gigabytes) in den Rechenzentren gespeichert worden, 2021 sollte es nach Ciscos Hochrechnung mehr als das 4.5-fache der Datenmenge sein¹⁵.

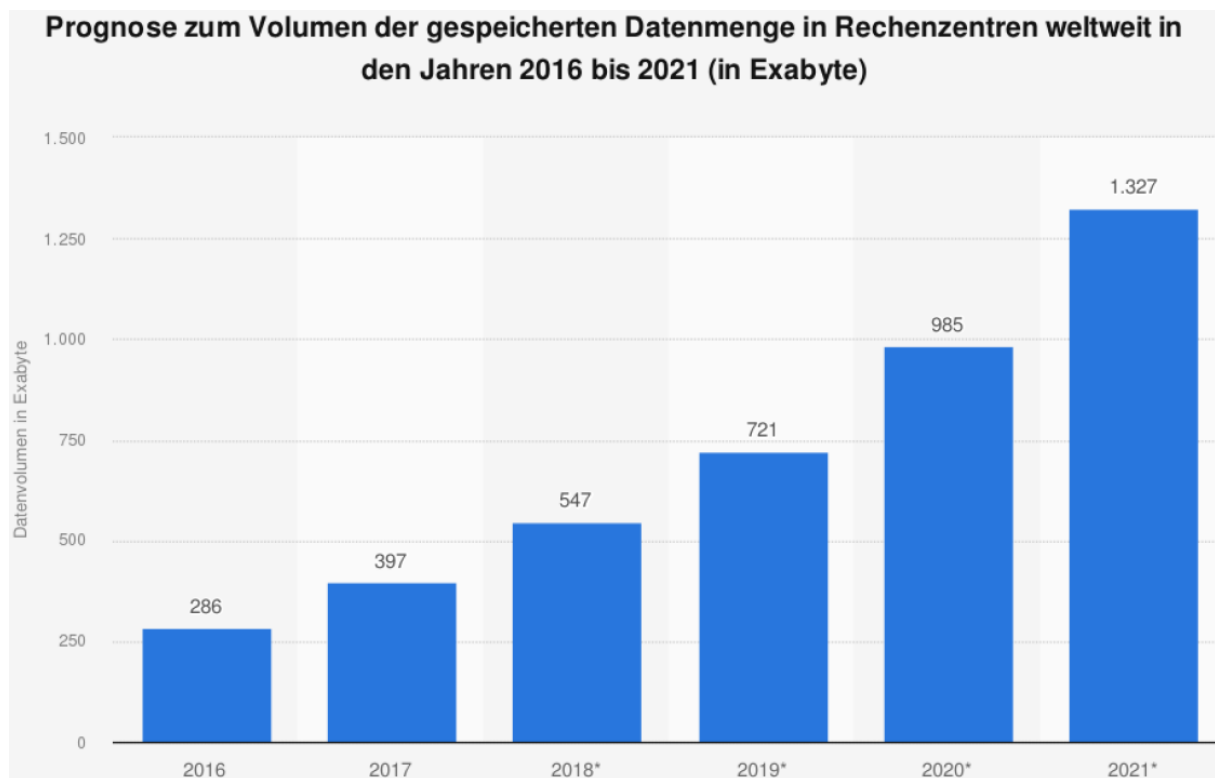


Abbildung 3: Statistik Prognose globaler Datenmengen; Quelle: Cisco Systems / statista.de

Betrachtet man nun die Preismodelle der 3 verbleibenden Anwendungen, so lässt sich erkennen, Kaspersky eine dauerhaft kostenlose Version anbietet, welche jedoch mit der Einschränkung des Funktionsumfangs einhergeht. Möchte man alle Funktionen verwenden, so zahlt man eine Lizenzgebühr von ca. 15€/Jahr. ESET bietet sein App Parental Control 30 Tage kostenlos zum Testen an. Danach kann man die Anwendung für 19,96€/Jahr und Gerät weiterverwenden. Wondershare bietet dagegen nur eine 3-tägige kostenlose Trial-Version an und danach in 3 verschiedenen Abo-Plänen, von 10.99\$/Monat (10.23€) bis zu 60.99\$/Jahr (57.79€).

¹⁵ Cisco Global Cloud Index

2.1.2.4 Betriebssysteme

Alle 3 Apps sind für Android Systeme ausgelegt. Hier erhalten die Anwendungen auch mehr Berechtigungen, die die verschiedensten Systemfunktionen verwenden. Kasperskys Safe Kids und Wondershares FamiSafe Kinder sind zusätzlich auch noch für iOS, Windows und MacOS vorhanden, hier jedoch aufgrund der Begrenzung der Berechtigungen durch das Betriebssystem mit eingeschränkten Funktionen. So wird bei Safe Kids mit angegeben, dass „[aufgrund] von Beschränkungen des Betriebssystems können in iOS nur Altersbeschränkungen eingerichtet werden“¹⁶, wenn es um die „Kontrolle der App-Nutzung“¹⁷ geht. Bei FamiSafe können dagegen keine Berichte für iOS-Geräte erstellt werden.

2.1.3 Entscheidung

Aufgrund der verschiedenen Informationen, die über die Anwendungen gesammelt wurden, in Kombination mit den Entscheidungskriterien, wird in der folgenden Ausarbeitung dieser Hausarbeit die App „FamiSafe Kinder“ von Wondershare begutachtet. FamiSafe ist für verschiedene OS verfügbar und wirbt mit einer RSA-Verschlüsselung, die überprüft werden soll. Der Preis der Anwendung ist zwar verglichen mit den anderen deutlich höher, doch auch der Ursprung des Entwicklers weckt das Interesse, diese App genauer betrachten zu wollen.

2.2 Hardware

2.2.1 Einleitung, Auswahlkriterien und Entscheidung

Bei der Einleitung zu den Software-Trackern wurde auf die Menge an Kindern (bis zu 50%) eingegangen, die bereits ab einem frühen Alter ein eigenes Smartphone besitzen. Dagegen stehen die ca. 50% der Kinder, die ein solches Gerät erst später erhalten. Die Gründe hierfür sind genauso vielseitig, wie die, dem eigenen Kind ein eigenes Gerät zur Verfügung zu stellen. In einer Umfrage des Forum Mobilkommunikation FMK im Jahr 2021, bei der Lehrer*innen befragt wurden, welches Alter das geeignete sei für ein Smartphone, gaben 46% der Befragten das Alter ab 10 Jahren an¹⁸. Dieses Ergebnis deckt sich mit einer weiteren Erhebung einer digitalen Markt- und Meinungsforschungsagentur, bei der Eltern zu verschiedenen Bereichen des Familienlebens befragt wurden, unter anderem ebenfalls das geeignete Alter für den Besitz eines Smartphones bei Kindern¹⁹.

¹⁶ Kaspersky Safe Kids

¹⁷ Kaspersky Safe Kids

¹⁸ vgl. FMK Umfrage

¹⁹ vgl. Marketagent – Familienreport 2015

Daher muss es auch eine Möglichkeit geben, dem Kind einen Tracker zu geben, ohne ihm oder ihr direkt ein Smartphone in die Hand zu drücken.

Hardware-Tracker gibt es in verschiedensten Ausführungen, Preiskategorien und von allerlei Herstellern. Die Auswahlmöglichkeit besteht zwischen reinen GPS-Trackern und Smartwatches für Kinder, die unter anderem z.B. für Notfälle eine Telefon-Funktion enthalten.

Die Auswahl des Hardware-Trackers verläuft daher in einem vereinfachten Prozess, da die meisten über eine ähnliche Ausstattung verfügen. Die ausschlaggebenden Kriterien waren hier unter anderem der Anschaffungspreis. Da das Gerät nur im Rahmen der Hausarbeit verwendet wird, sollte der Preis sich im niedrigsten Preissegment bis max. 30€ befinden. Wichtige, entscheidende Ausstattungsmerkmale waren das Vorhandensein einer Nachrichten-, Telefonie- und Tracking-Funktion. Weiterhin wurde als Entscheidungskriterium ein Artikel der Website dr-datenschutz.de²⁰ und ein darin verlinkter Artikel der Website AV-Test²¹ herangezogen. Darin wurden Kinder-Smartwatches, die in China produziert wurden, getestet und als potenziell gefährlich bewertet, da von diesen Geräten Daten abgegriffen werden konnten, und zwar nicht nur von dem einen Gerät, welches die Forscher untersuchten.

Daraufhin wurde über ebay.de eine markenlose Kinder-Smartwatch erworben, die die geforderten Funktionen enthielt. Die rechtlichen Informationen des Verkäufers zeigen auch einen Sitz in Shenzhen, China, an, was die Möglichkeit auf eine, wie in den Artikeln erwähnte, potenzielle unverschlüsselte Datenübertragung erhöht.



Abbildung 4: Anzeigen-Foto der Kinder-Smartwach von ebay.de

²⁰ Dr. Datenschutz

²¹ AV-Test Internet of Things Blog

3. Analyse der Kommunikation

3.1 Versuchsaufbau

Der Versuchsaufbau variiert für den Test des Software-Trackers mit dem des Hardware-Trackers geringfügig.

3.1.1 Versuchsaufbau Software-Tracker



Abbildung 5: Versuchsaufbau Software-Tracker

Beim Versuchsaufbau des Software-Trackers soll der generierte Traffic, der durch Eingaben und die App selbst entsteht, abgegriffen werden. Dazu wird ein Laptop, welcher über WLAN mit dem Smartphone, und per Ethernet mit Netzwerk verbunden ist, als Proxy Server für das Smartphone verwendet. Auf dem Laptop wird das Netzwerk-Analyze-Tool Wireshark und Burp Suite verwendet, welche den gesamten Netzwerk-Traffic aufnehmen, der im Nachhinein daraufhin analysiert werden kann.

3.1.2 Testgeräte

Das verwendete Testgerät ist ein Samsung Galaxy S7 mit Android 8 und Android-Sicherheitspatch-Ebene mit Datum vom 1. September 2020. Weiterhin verfügt das Gerät über eine Prepaid-SIM-Karte und wird in einem, vom sonstigen Produktivnetzwerk des Autors getrennten WLAN, verwendet. Das Gerät befindet sich in einem originalen, nicht gerooteten Zustand. Ebenfalls wurden bis auf die Apps, die sich nicht deinstallieren lassen, sämtliche Anwendungen, bis auf den Chrome-Browser, entfernt.

Das Gerät, welches zum Aufnehmen und Analyse des Netzwerk-Traffics verwendet wird, ist ein Laptop mit Kali Linux OS, welches ebenfalls in dem separierten Netz eingebunden ist.

3.1.3 Tools

Die Kombination von Wireshark und Burp Suite ist notwendig, da bei der Verwendung eines Proxys die Ziel-IP-Adresse meist die des Proxy Servers und somit des Laptops ist und über Burp Suite noch weitere Informationen zu IP-Adressen abgefangen werden können.

3.1.3.1 Wireshark

Wireshark ist eines der weltweit bekanntesten open-source Netzwerkanalyse Programme. Durch das Aufschlüsseln der Pakete, die über verschiedene Schnittstellen aufgenommen werden können (z.B. per WLAN, Ethernet oder USB), können Probleme im Netzwerk erkannt und analysiert werden, sowie durch die Analyse des Netzwerk-Traffics die Sicherheit erhöht werden²².

3.1.3.2 Burp Suite

Burp Suite ist eine Sicherheitstest-Plattform von Webanwendungen²³. Durch die integrierten Funktionen ist es möglich, „den gesamten Testprozess zu unterstützen, von der anfänglichen Zuordnung und Analyse der Angriffsfläche einer Anwendung bis hin zum Auffinden und Ausnutzen von Sicherheitslücken“²⁴.

3.1.3.3 Einrichtung

Bevor die Messungen erfolgen können, müssen zunächst Konfigurationen an den Geräten und den Tools vorgenommen werden, sodass die Messungen erfolgen können.

Burp Suite (Community Edition) ist standardmäßig auf dem Kali Linux OS implementiert. Nach dem Start wird man zunächst durch einen Projekt-Prozess geleitet, bei dem man auswählen kann, ob man die Standardeinstellungen von Burp Suite verwenden möchte oder ein spezifisches Config-File. In dieser Ausarbeitung wird die Standardkonfiguration von Burp Suite verwendet.

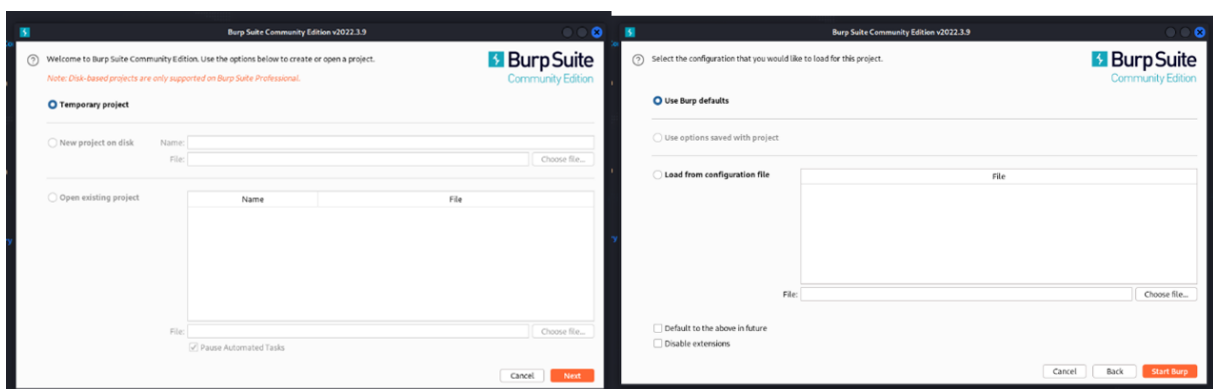


Abbildung 6: Burp Suite - Startbildschirm

²² vgl. CompTIA

²³ vgl. Kali Tools – Burp Suite

²⁴ vgl. Kali Tools – Burp Suite

Danach kann man Burp starten.

Da der Traffic über einen Proxy des Laptops geleitet wird, muss dieser im nächsten Schritt eingerichtet werden. Hierzu muss im Bereich **Proxy > Options** beim **Proxy Listeners** ein weiteres Interface eingetragen werden. Da standardtechnisch der Port 8080 für TCP-Verkehr belegt ist und oftmals für Proxy-Übertragungen oder die Verbindung zu Apache Tomcat verwendet wird, wird hier nun daher der Port 8085 für die Proxy-Verbindung verwendet, da dieser keine offizielle Belegung besitzt.

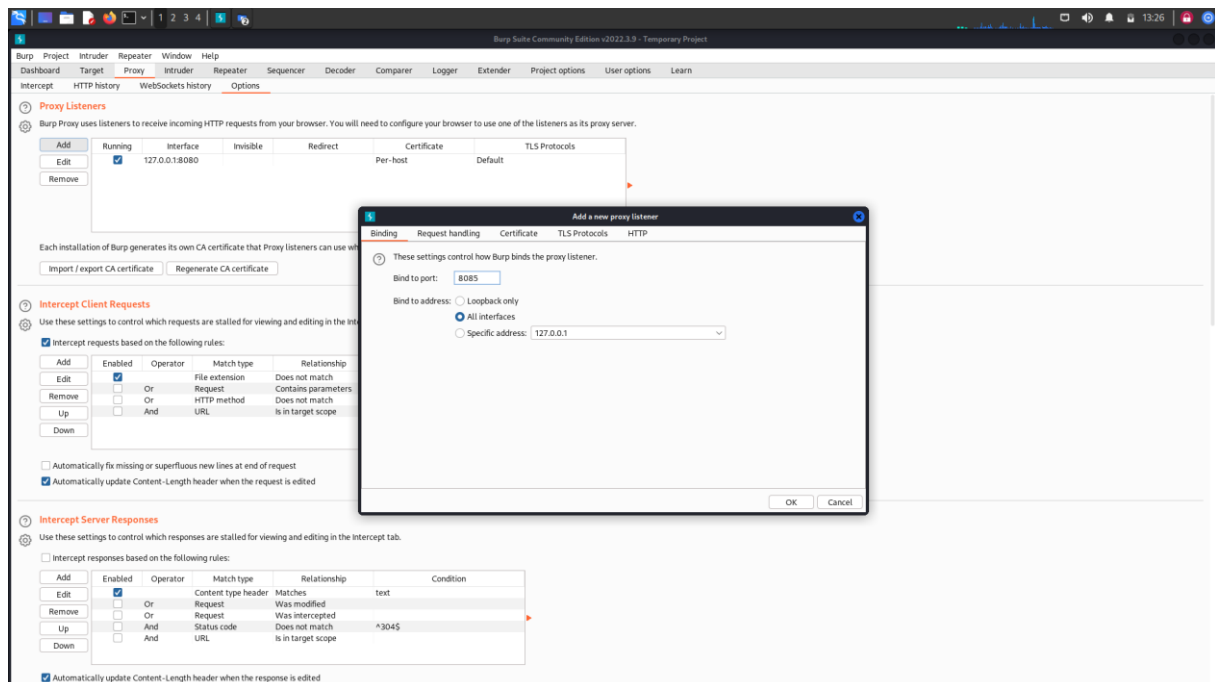


Abbildung 7: Burp Suite - Einstellung Proxy-Verbindung

Als nächster Schritt muss daraufhin am Smartphone die Proxy-Verbindung konfiguriert werden. Nach der Verbindung mit dem WLAN muss manuell die IP-Adresse und der entsprechende Port des Proxy-Servers eingegeben werden. Die IP-Adresse muss die des Laptops sein, auf dem der Traffic aufgenommen wird, der Port der, der vorhin vergeben wurde. Danach erfolgt die Installation des CA-Zertifikates, sodass der Traffic überhaupt abgefangen werden kann.

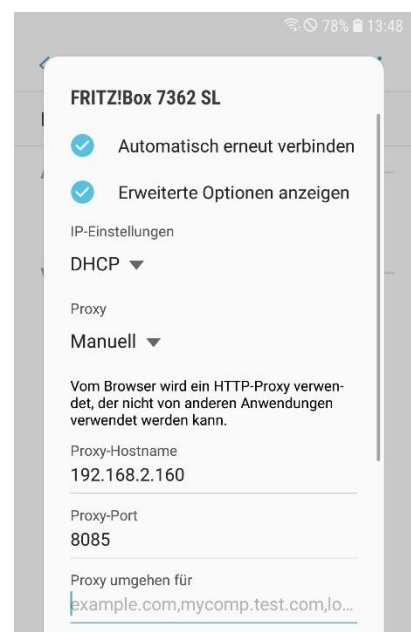


Abbildung 8: Samsung - Einstellung Proxy

3.1.4 Bestimmung Parameter

Für einen aussagekräftigen Vergleich des Netzwerk-Traffics müssen zunächst Parameter festgelegt werden.

3.1.4.1 Messzeitraum

Der Zeitraum, der untersucht werden soll, soll 60 Sekunden betragen. Dieser Zeitraum wird als ausreichend betrachtet, um genügend generierten Traffic zu erhalten. Diese 60 Sekunden werden zeitlich gemessen ab dem Start der Aufnahme des Netzwerk-Traffics.

3.1.4.2 Testszenarien

Folgende Testszenarien werden im Rahmen dieser Ausarbeitung durchgeführt und betrachtet:

1. Messung ohne Tracking-App, um einen Ausgangswert für den Traffic zu erhalten
2. Messung mit installierter, aber weder geöffneter noch eingerichteter Tracking-App
3. Messung bei eingerichteter, geschlossenen App
4. Messung bei eingerichteter, geöffneter App mit Befehlsausführung

3.1.4.3 Wiederholbarkeit

Um gesicherte Ergebnisse zu erhalten, wird jeder Test drei Mal wiederholt. Die Daten werden danach gesammelt und bei der anschließenden Auswertung in sinnvollen Bereichen mit durchschnittlichen Werten weitergearbeitet.

3.1.4.4 Durchführung der Messung

Bei der Durchführung der Messung gibt es Variationen, abhängig nach Art der Messung. Erfolgt eine Messung ohne Interaktion mit dem Testgerät (Testszenario 1, 2, und 3), so wird das Testgerät in den jeweiligen Testmodus versetzt und die Aufnahme des Traffics erfolgt ohne weitere Beachtung von anderen Kriterien oder Umständen. Erfolgt jedoch die Messung mit einer Ausführung einer Aktion (Testszenario 4), so wird die Aufnahme gestartet, während die Anwendung auf dem Testgerät bereits arbeitet. 10 Sekunden nach dem Start der Aufnahme wird daraufhin die Interaktion mit dem Testgerät vorgenommen.

3.1.5 Messungen

Zur späteren Filterung des gesamten Netzwerk-Traffics, der per Wireshark aufgenommen wurde, muss zunächst die IP-Adresse der Testgeräte ermittelt werden.

Bei dem Smartphone Testgerät kann man die IP-Adresse ermitteln, indem man über den Pfad **Einstellungen > Verbindungen > WLAN** die Netzwerkeinstellungen des verbundenen WLANs aufruft (**Netzwerkeinstellungen verwalten**). Dort kann nun die IP-Adresse **192.168.2.101** für das Smartphone entnommen werden.

Bei dem Laptop kann dagegen einfach per Kommandozeilenbefehl **ifconfig** die Netzwerkdaten des Gerätes abgerufen werden. Hier wird nun die IP-Adresse **192.168.2.160** abgelesen.

Um bei Wireshark allein den Traffic zu erhalten, der das Smartphone betrifft, wird der Filter **ip.addr==192.168.2.101** gesetzt. Hierdurch erhält man jeweils die Netzwerkpakete angezeigt, die vom Smartphone ausgehen (Source), als auch die, die an das Smartphone zurückgesendet werden (Destination).

3.1.5.1 Messung ohne Tracking-App – Grundzustand

Im Grundzustand wurden in den gesamten gemessenen 180 Sekunden insgesamt 206 Pakete vom Testgerät empfangen und gesendet, mit einer Gesamtgröße von 0,02MB. Diese Statistik erhält man in Wireshark mit gesetztem Anzeigefilter über den Pfad **Statistiken > Eigenschaften der Mitschnittdatei**.

Statistik

Messwerte	Aufgezeichnet	Angezeigt
Pakete	1363	206 (15.1%)
Zeitspanne, s	554.736	545.954
Durchschnittliche pps	2.5	0.4
Durchschnittliche Paketgröße, B	115	98
Byte	156298	20216 (12.9%)
Durchschnittliche Byte/s	281	37
Durchschnittliche Bit/s	2254	296

Abbildung 9: Wireshark – Grundzustand - Statistik

Ebenfalls kann man eine Übersicht der „Packets/ 1 Sek.“, also der Anzahl der Pakete pro vergangener Sekunde, über den Pfad **Statistiken > I/O Graph** erstellen. Wie man in Abbildung 10 erkennen kann, sind die beiden ersten Messung recht ähnlich von der Paketverteilung. Die letzte Messung dagegen ist keinesfalls vergleichbar mit den vorherigen.

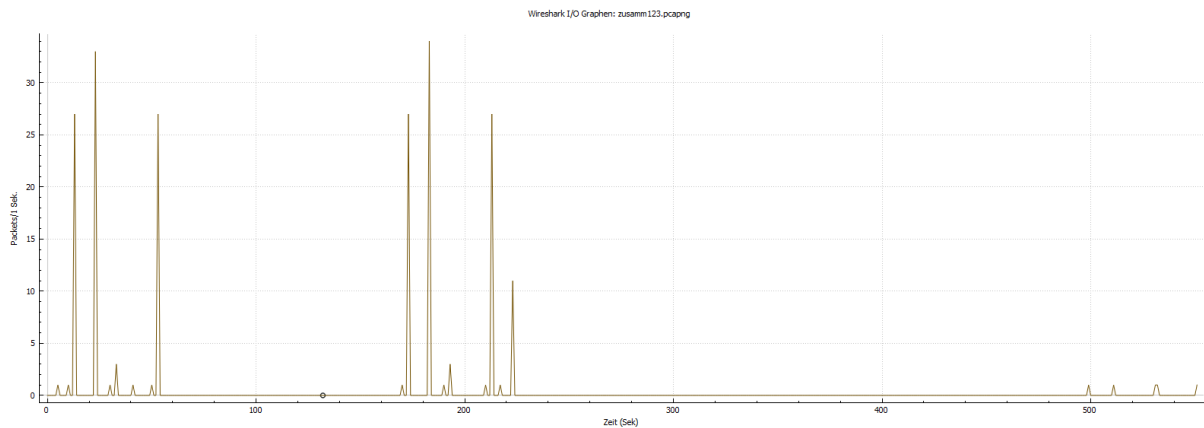


Abbildung 10: Wireshark – Grundzustand - I/O Graph

Dennoch kann man erkennen, dass eine regelmäßige Kommunikation stattfindet. Bei der Betrachtung der Endpunkte lässt sich feststellen, dass im Grundzustand Pakete nur zwischen den Testgeräten (IP-Raum **192.168.2.X**) und zwei weiteren IP-Adressen erfolgt.

Wireshark · Endpoints · grund1.pcapng

Ethernet · 4	IPv4 · 4	IPv6	TCP · 22	UDP · 2						
Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	AS Number	AS Organization
192.168.2.101	35	3888	35	3888	0	0	—	—	—	—
192.168.2.160	30	3360	0	0	30	3360	—	—	—	—
224.0.0.22	2	120	0	0	2	120	—	—	—	—
224.0.0.251	3	408	0	0	3	408	—	—	—	—

Abbildung 11: Wireshark – Grundzustand - Endpoints

Bei der Durchsicht der Aufnahme in Wireshark kann zu den zunächst unbekannten IP-Adressen erkannt werden, dass es sich hier um Multicast-Adressen handelt.

IP-Adresse **224.0.0.22** ist zuständig für das *IGMPv3*-Protokoll, oder auch Internet Group Management Protocol. Dieses Protokoll hat als Aufgabe „dynamische Gruppen für IP-Multicast-Übertragungen zu verwalten“²⁵.

Hinter IP-Adresse **224.0.0.251** versteckt sich ein Dienst (*_googlecast._tcp.local*) des mDNS-Protokolls, der bei verschiedensten Produkten des Google Ökosystems implementiert ist²⁶.

²⁵ IONOS – IGMPv3

²⁶ vgl. Serverfault

3.1.5.2 Messung nach Installation der Tracking-App

Nachdem der grundlegende Netzwerkverkehr gemessen wurde, wird nun die entsprechende App auf dem Smartphone installiert. Da diese Ausarbeitung vom Netzwerk-Traffic einer Kinder Tracking-App handelt, wird auf dem Smartphone auch nicht die Verwaltungs- und Kontroll-App für die Eltern (FamiSafe: Kindersicherungs-App), sondern die tatsächliche Tracker-App (FamiSafe Jr-Bildschirmzeit & Family Locator) installiert.

Statistik

<u>Messwerte</u>	<u>Aufgezeichnet</u>	<u>Angezeigt</u>
Pakete	1531	285 (18.6%)
Zeitspanne, s	2857.505	2820.109
Durchschnittliche pps	0.5	0.1
Durchschnittliche Paketgröße, B	134	171
Byte	205763	48792 (23.7%)
Durchschnittliche Byte/s	72	17
Durchschnittliche Bit/s	576	138

Abbildung 12: Wireshark - installiert o. Konfiguration - Statistik

Bei der Betrachtung der Statistik ist keine großartige Veränderung der Paketmenge festzustellen. Bei den gesamt aufgenommenen Paketen ist ein Unterschied von 168 vorhanden, während bei den Paketen, die das Smartphone betreffen, ein Delta von 79 Paketen vorhanden ist.

Betrachtet man nun den zusammengeführten I/O Graph der drei Messungen, kann man erkennen, dass es hier nun erste Abweichungen gibt.

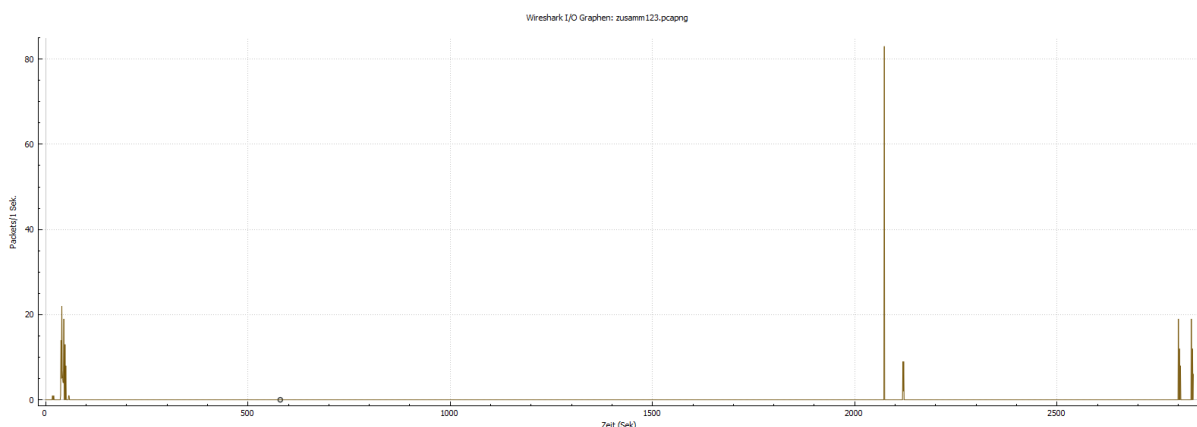


Abbildung 13: Wireshark - installiert o. Konfiguration - I/O Graph

Eine Regelmäßigkeit lässt sich bei keinem zu vergleichenden Messungspaar mehr feststellen. Auch sind die maximalen Pakete pro Sekunde verschieden. Während es beim Grundzustand bei Messung 1 und 2 jeweils 11 Pakete waren, die bei einem Maximum vorhanden waren, sind

es beim Testszenario installiert ohne Konfiguration nun für Messung 1 22 Pakete, bei Messung 2 78 Pakete und bei Messung 3 19 Pakete.

Die bei Wireshark aufgeführten Endpoints sind dieselben, wie bei der Messung im Grundzustand. Während dagegen beim Grundzustand bei Burp Suite keine Einträge in der http-Historie vorgefunden werden konnten, ändert sich dieses Bild für das neue Testszenario (Bsp. s. Abbildung 14).

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies	Time	Listener port
904	http://connectivitycheck.gstatic.com	GET	/generate_204			204	102						142.250.186.163		15:43:59.4 Jun...	8085
905	http://play.googleapis.com	GET	/generate_204			204	102						142.250.184.234		15:44:02.4 Jun...	8085
906	http://connectivitycheck.gstatic.com	GET	/generate_204			204	102						142.250.186.163		15:44:07.4 Jun...	8085
907	http://play.googleapis.com	GET	/generate_204			204	102						142.250.184.234		15:44:07.4 Jun...	8085
908	http://connectivitycheck.gstatic.com	GET	/generate_204			204	102						142.250.186.163		15:45:05.4 Jun...	8085
909	http://play.googleapis.com	GET	/generate_204			204	102						142.250.184.234		15:45:08.4 Jun...	8085
910	http://connectivitycheck.gstatic.com	GET	/generate_204			204	102						142.250.186.163		15:45:11.4 Jun...	8085
911	http://www.google.com	GET	/gen_204			204	229	HTML					172.217.16.132		15:45:14.4 Jun...	8085

Abbildung 14: Burp Suite - installiert o. Konfiguration - Messung 1 - http-Historie

Hier können folgende IP-Adressen erkannt werden.

IP-Adresse	Anbieter	Host-Adresse
172.217.16.132	Google LLC	google.com
142.250.186.163	Google LLC	connectivitycheck.gstatic.com
142.250.185.67	Google LLC	connectivitycheck.gstatic.com
142.250.184.234	Google LLC	play.googleapis.com
142.250.185.170	Google LLC	play.googleapis.com
172.217.23.106	Google LLC	play.googleapis.com

Tabelle 4: IP-Adressen Testszenario installiert o. Konfiguration

Es lässt sich deutlich erkennen, dass nach der Installation der App verschiedene Google-Dienste kontaktiert werden.

Mit der Verbindung zu *connectivitycheck.gstatic.com* wird ein Dienst aufgerufen, der überprüft, ob eine Anwendung im Netzwerk vorhanden ist, die eine Vorschaltseite mit Login oder Bestätigung von AGBs vor der Nutzung des Netzwerks erfordert²⁷.

Die Verbindung zu *play.googleapis.com* stellt eine Abfrage dar, ob installierte Anwendungen auf dem Android-Gerät, unter anderem auch der eigene Playstore, upgedatet werden müssen²⁸.

Weiterhin lassen sich sämtliche, den Filter berücksichtigende, HTTP-Requests anzeigen, wenn man über den Pfad **Statistik > HTTP > Anfragen** geht. Hier wird dann noch zusätzlich

²⁷ vgl. Appdated

²⁸ vgl. StackExchange

die URL der Google API ***gmscompliance-pa.googlapis.com*** erkennen. Hierzu lassen sich jedoch keine weiteren Informationen finden.

3.1.5.3 Messung mit konfigurierter, im Hintergrund laufenden App

Nach der Installation und Einrichtung der App, bei der dieser verschiedenste Berechtigungen erteilt werden, wird diese wieder über den Task-Manager des Smartphones geschlossen. Die App ist zwar nun nicht mehr aktiv geöffnet, dennoch ist bereits die Überwachung konfiguriert und läuft dauerhaft im Hintergrund mit.

Dies lässt sich auch bereits anhand der Statistik erkennen.

Statistik

Messwerte	Aufgezeichnet	Angezeigt
Pakete	5097	3283 (64.4%)
Zeitspanne, s	340.818	339.659
Durchschnittliche pps	15.0	9.7
Durchschnittliche Paketgröße, B	176	195
Byte	895543	640865 (71.6%)
Durchschnittliche Byte/s	2627	1886
Durchschnittliche Bit/s	21 k	15 k

Abbildung 15: Wireshark - konfig. App im Hintergrund– Statistik

Waren es noch bei den vorhergehenden Messungen maximal 285 Pakete im Netzwerk-Traffic, so sind es nach der Konfiguration der App bereits über dem 11-fachen, die vom Smartphone gesendet und empfangen werden. Auch anhand des I/O Graphen lässt sich ein überdimensionaler Anstieg der Paketmenge erkennen.

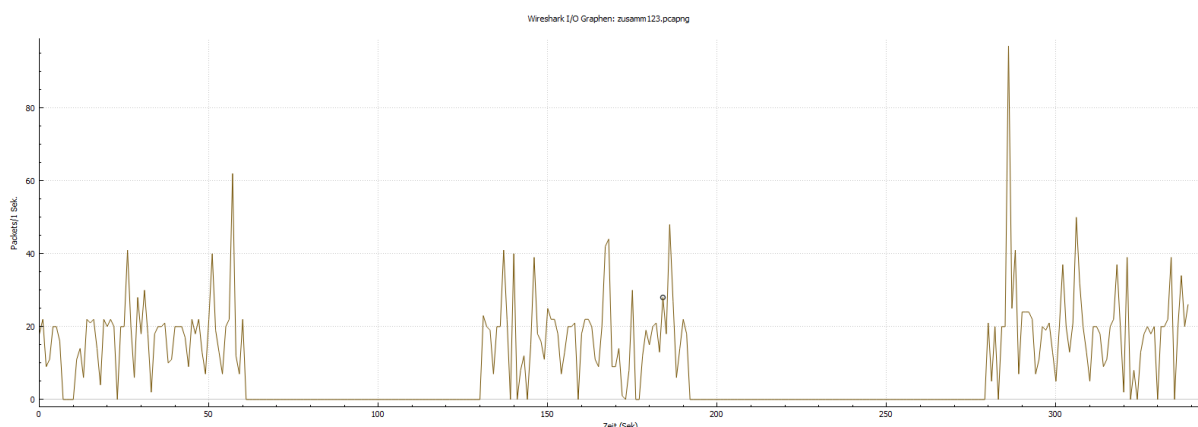


Abbildung 16: Wireshark - konfig. App im Hintergrund - I/O Graph

Auch bei dieser konsolidierten Messreihe in Wireshark werden außer des Smartphones und des Laptops keinerlei weitere Endpunkte mit angezeigt. Prüft man nun die Übersichten aus Burp Suite, kann man, wie bereits in der vorherigen Messreihe nach der Installation, verschiedene IP-Adressen aus dem Google-Umfeld wiederfinden.

IP-Adresse	Anbieter	Host-Adresse
172.217.16.132	Google LLC	google.com
142.250.186.163	Google LLC	connectivitycheck.gstatic.com
142.250.185.67	Google LLC	connectivitycheck.gstatic.com
142.250.184.234	Google LLC	play.googleapis.com
142.250.185.170	Google LLC	play.googleapis.com

Tabelle 5: IP-Adressen Testszenario App konfiguriert und im Hintergrund

Besonders interessant ist jedoch ein Eintrag bei der ersten Messung dieser Reihe mit der IP-Adresse **47.88.92.42**.

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies	Time	Listener port
78	https://us-west-data-api-famisa...	POST	/v1/gather/gsm/member_id=58106488...	✓		200	406	JSON				✓	47.88.92.42		11:48:24 6 Jun...	8085
79	http://connectivitycheck.gstatic...	GET	/generate_204			204	102						142.250.185.67		11:48:45 6 Jun...	8085
80	http://play.googleapis.com	GET	/generate_204			204	102						142.250.186.170		11:48:48 6 Jun...	8085
81	http://connectivitycheck.gstatic...	GET	/generate_204			204	102						142.250.185.67		11:49:16 6 Jun...	8085
82	http://play.googleapis.com	GET	/generate_204			204	102						142.250.186.170		11:49:16 6 Jun...	8085

Abbildung 17: Burp Suite - konf. App im Hintergrund - http-Historie

Dieser ist der erste Eintrag, der nichts mit Google zu tun hat. Bei Burp Suite wird als Host-Adresse die URL **us-west-data-api-famisa.com** angezeigt. Der erste Hinweis, dass die App mit dem Hersteller-Server zu kommunizieren scheint. Nach der Recherche der IP über einen IP-Lookup-Dienst erhält man die Information, dass dieser Dienst über einen Server der AliCloud gehostet wird, welcher an der Westküste der USA in Kalifornien positioniert ist.

IP Details For: 47.88.92.42

Decimal: 794319914

Hostname: 47.88.92.42

ASN: 45102

ISP: AliCloud

Services: Datacenter

Assignment: [Likely Static IP](#)

Country: United States

State/Region: California

City: San Mateo

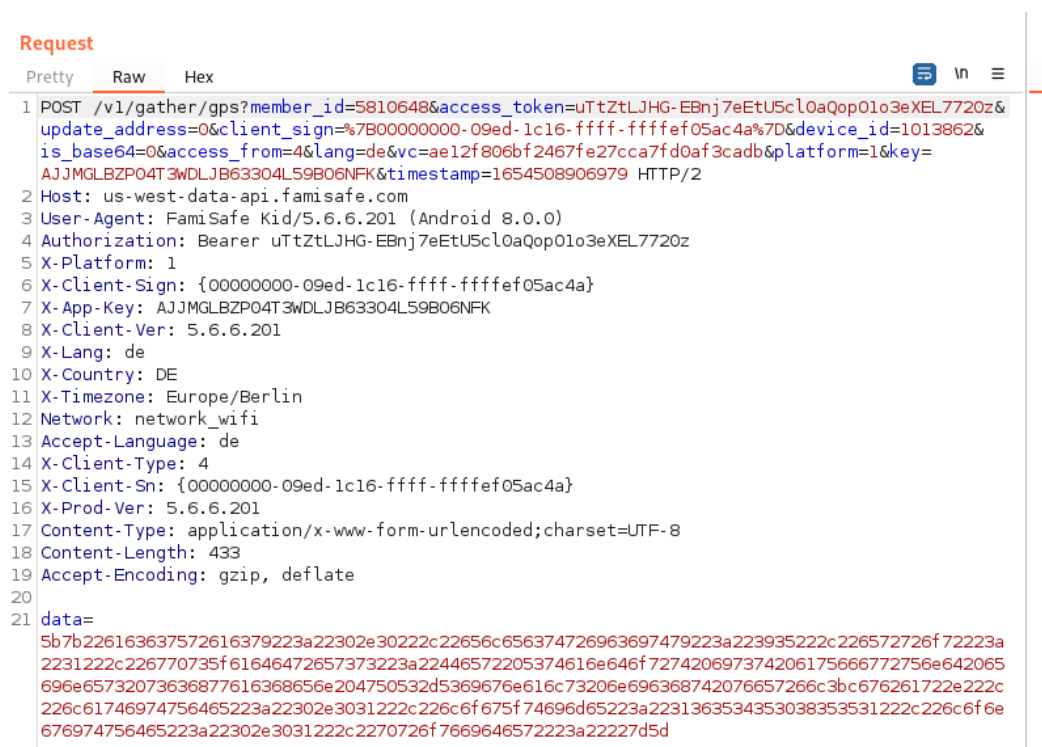
Latitude: 37.547424 (37° 32' 50.73" N)

Longitude: -122.330589 (122° 19' 50.12" W)

Leaflet | © OpenStreetMap Terms

Abbildung 18: IP-Lookup per <https://whatismyipaddress.com/ip/47.88.92.42>

Zwar ist laut Burp Suite die Kommunikation dieses Paketes per TLS (Nachfolgeverschlüsselung von SSL auf Ebene 5 des ISO/OSI Modells, welches z.B. für sichere HTTPS-Verbindungen verwendet wird²⁹) verschlüsselt, dennoch lassen sich einige Inhalt auslesen, wie den Inhalt des http-POST-Befehl, bei dem unter anderem anscheinend eine Member-ID, eine Geräte-ID, die App-Sprache als auch ein Key-Value versendet wurde. Auch kann man sehen, dass es sich bei dem Gerät, welches den Befehl versendet, um ein Gerät mit Android 8 handelt.



```
Request
Pretty Raw Hex
1 POST /v1/gather/gps?member_id=5810648&access_token=uTtZtLJHG-EBnj7eEtU5cl0aQop01o3eXEL7720z&
  update_address=0&client_sign=%7B00000000-09ed-1c16-ffff-ffffef05ac4a%7D&device_id=1013862&
  is_base64=0&access_from=4&lang=de&vc=ae12f806bf2467fe27cca7fd0af3cadb&platform=1&key=
  AJJMGLBZP04T3WDLJB63304L59B06NFK&timestamp=1654508906979 HTTP/2
2 Host: us-west-data-api.famisafe.com
3 User-Agent: FamiSafe Kid/5.6.6.201 (Android 8.0.0)
4 Authorization: Bearer uTtZtLJHG-EBnj7eEtU5cl0aQop01o3eXEL7720z
5 X-Platform: 1
6 X-Client-Sign: {00000000-09ed-1c16-ffff-ffffef05ac4a}
7 X-App-Key: AJJMGLBZP04T3WDLJB63304L59B06NFK
8 X-Client-Ver: 5.6.6.201
9 X-Lang: de
10 X-Country: DE
11 X-Timezone: Europe/Berlin
12 Network: network_wifi
13 Accept-Language: de
14 X-Client-Type: 4
15 X-Client-Sn: {00000000-09ed-1c16-ffff-ffffef05ac4a}
16 X-Prod-Ver: 5.6.6.201
17 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
18 Content-Length: 433
19 Accept-Encoding: gzip, deflate
20
21 data=
  5b7b226163637572616379223a22302e30222c22656c656374726963697479223a223935222c226572726f72223a
  2231222c226770735f61646472657373223a22446572205374616e646f727420697374206175666772756e642065
  696e65732073636877616368656e204750532d5369676e616c73206e696368742076657266c3bc676261722e222c
  226c61746974756465223a22302e3031222c226c6f675f74696d65223a2231363534353038353531222c226c6f6e
  676974756465223a22302e3031222c2270726f7669646572223a22227d5d
```

Abbildung 19: Burp Suite - konf. App im Hintergrund - http-Post-Befehl von FamiSafe

Ein ähnliches Bild wurde bei der zweiten und dritten Messung erhalten. Hier wurden ebenfalls ein http-POST-Befehl angezeigt, bei dem eventuell Werte für Datenbank-Einträge an einen Server der FamiSafe-Betreiber gesendet wurden.

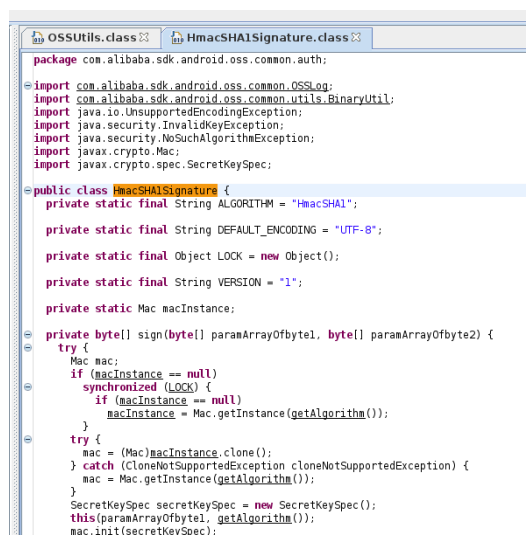
²⁹ vgl. Security Insider - TLS

Request

```
Pretty  Raw  Hex
5 X-Client-Sn: {00000000-09ed-1c16-ffff-ffffe05ac4a}
6 X-Prod-Ver: 5.6.6.201
7 Content-Type: application/json; charset=utf-8
8 Content-Length: 616
9 Accept-Encoding: gzip, deflate
10
11 [
12   {
13     "rows": [
14       {
15         "end_time": 1654500796,
16         "log_time": 0,
17         "name": "Galerie",
18         "package_name": "com.sec.android.gallery3d",
19         "start_time": 1654500768,
20         "type": 0,
21         "usage_count": 0,
22         "usage_date": "2022-06-06",
23         "usage_time": 28
24       }
25     ]
26   }
27 ]
```

Abbildung 20: Burp Suite - konf. App im Hintergrund – Messung 2 - Ausschnitt http-Post-Befehl an FamiSafe-Server Datenbank

Ob es sich bei den Werten in Abbildung 19 um solche handelt, mit denen bereits malizöse Aktionen gegenüber des Smartphone-Besitzers oder des Anbieters ausführen lassen könnten, kann weder mit Sicherheit gesagt werden, noch ist dies Bestandteil dieser Hausarbeit. Dennoch kann aufgrund einer kurzen Untersuchung der .apk-Datei, die aus der FamiSafe Jr-App erstellt wurde, gesagt werden, dass anscheinend eine HMACSHA1 Verschlüsselung verwendet wird. Zwar sind heutzutage Verschlüsselungen wie SHA256 oder AES256 gängiger, da bisher noch nicht ohne weiteres zu entschlüsseln, dennoch ist eine SHA1 Verschlüsselung lange nicht so unsicher wie eine unverschlüsselte Kommunikation, da sie für einen ungeübten Angreifer ein erstes Hindernis darstellt.



```
package com.alibaba.sdk.android.oss.common.auth;

import com.alibaba.sdk.android.oss.common.OSSLog;
import com.alibaba.sdk.android.oss.common.utils.BinaryUtil;
import java.io.UnsupportedEncodingException;
import java.security.InvalidKeyException;
import java.security.NoSuchAlgorithmException;
import javax.crypto.Mac;
import javax.crypto.spec.SecretKeySpec;

public class HmacSHA1Signature {
    private static final String ALGORITHM = "HmacSHA1";
    private static final String DEFAULT_ENCODING = "UTF-8";
    private static final Object LOCK = new Object();
    private static final String VERSION = "1";
    private static Mac macInstance;

    private byte[] sign(byte[] paramArrayOfbyte1, byte[] paramArrayOfbyte2) {
        try {
            Mac mac;
            if (macInstance == null) {
                synchronized (LOCK) {
                    if (macInstance == null) {
                        macInstance = Mac.getInstance(getAlgorithm());
                    }
                }
            }
            mac = (Mac)macInstance.clone();
        } catch (CloneNotSupportedException cloneNotSupportedException) {
            mac = Mac.getInstance(getAlgorithm());
        }
        SecretKeySpec secretKeySpec = new SecretKeySpec(
            this(paramArrayOfbyte1, getAlgorithm());
            mac.init(secretKeySpec);
        }
    }
}
```

Abbildung 21: Hinweis HMACSHA1-Verschlüsselung in FamiSafe.apk

Bei der Durchsuchung der HTTP-Requests in Wireshark konnten zudem noch weitere Host-URLs festgestellt werden.

- ws.famisafe.com
- playatoms-pa.googleapis.com
- firebaseinappmessaging.googleapis.com
- digitalassetlinks.googleapis.com
- analytics.300624.com

Die URL **ws.famisafe.com** spricht wieder dafür, dass hier eine Kommunikation mit dem Anbieter-Server vorhanden ist.

Bei **firebaseinappmessaging.googleapis.com** handelt es sich um einen Event-Listener, der im Rahmen der Firebase-Plattform verwendet wird³⁰. „Firebase ist eine Entwicklungsplattform für mobile Anwendungen von Google mit leistungsstarken Funktionen für die Entwicklung, Handhabung und Verbesserung von Anwendungen“³¹.

digitalassetlinks.googleapis.com ist eine API zum Erkennen von Beziehungen zwischen Online-Assets wie Websites oder mobilen Apps³².

Sucht man bei google.com nach **analytics.300624.com**, erhält man unter anderem als Ergebnis einen GitHub-Eintrag für AdGuard DNS-Listen, bei der die URL im Bereich Mobile Tracking und Spyware vorzufinden ist³³. Genaue Informationen lassen sich jedoch nicht finden.

Für die URL **playatoms-pa.googleapis.com** lassen sich keinerlei Informationen finden.

3.1.5.4 geöffnete App mit Interaktion

Die App besitzt die Möglichkeit, durch die Betätigung eines Buttons eine Anfrage an die Eltern, zu senden, um deren Position zu erhalten. Voraussetzung hierfür ist, dass ein Elternteil die Verwaltungs-App **FamiSafe: Kindersicherung** auf ihrem Gerät installiert hat.

In der letzten Messreihe lässt sich zum vorherigen Szenario ebenfalls wieder eine Abweichung zur vorherigen Messreihe erkennen, was das Volumen des Paketversandes im Netzwerk angeht.

³⁰ vgl. Firebase

³¹ vgl. back4app

³² vgl. Google Digital Asset Link

³³ GitHub - AdguardMobileSpyware.txt

Statistik

Messwerte	Aufgezeichnet	Angezeigt
Pakete	5722	3737 (65.3%)
Zeitspanne, s	1876.509	1873.249
Durchschnittliche pps	3.0	2.0
Durchschnittliche Paketgröße, B	164	190
Byte	936416	711390 (76.0%)
Durchschnittliche Byte/s	499	379
Durchschnittliche Bit/s	3992	3038

Abbildung 22: Wireshark - Interaktion – Statistik

Die gesamte Menge an Paketen steigt von 5097 im gesamten Testzeitraum der Messreihe 3, auf 5722 Pakete im gesamten Testzeitraum der Messreihe 4 an. Die Pakete, die das Testgerät Smartphone betreffen, steigen in der Anzahl um ca. 13% an.

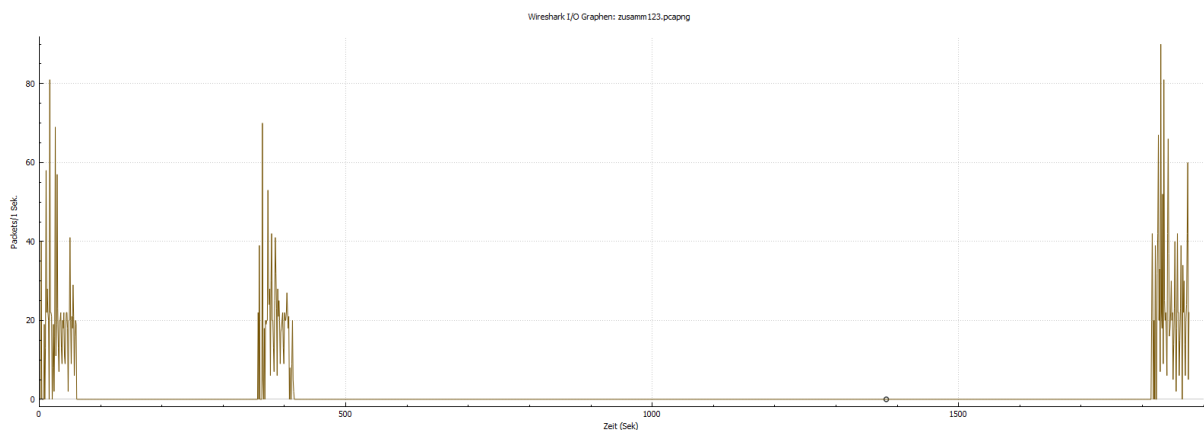


Abbildung 23: Wireshark - Interaktion - I/O Graph

Die Menge an Paketen, die mit unterschiedlichen Inhalten zu verschiedenen Zeitpunkten empfangen und gesendet werden, lassen hier eine Ähnlichkeit zwischen den einzelnen Messungen auch nicht mehr zu.

Im IP-Adress-Bereich in Burp Suite ist zu den bisher aufgefallenen IP-Adressen ein neues Ziel hinzugekommen. Die IP-Adresse **63.159.217.133**, die in Burp Suite die Host-URL **sparrow.wondershar.com** anzeigt, wird auf den Servern der **CenturyLink Communications LLC** gehostet. Da diese IP bzw. URL nur einmal bei 3 Messungen der Testreihe aufgetaucht ist, der Inhalt des http-POST-Befehls keine Rückschlüsse auf deren Aufgabe erschließen lässt und die Recherche der URL keine Ergebnisse erbrachte, kann jedoch keine weitere Aussage dazu gemacht werden.

Request

```
Pretty Raw Hex
1 POST /v1/file HTTP/1.1
2 Content-Type: multipart/form-data; boundary=70db372eb000e2ax0
3 Content-Length: 1054
4 User-Agent: Dalvik/2.1.0 (Linux; U; Android 8.0.0; SM-G930F Build/R16NW)
5 Host: sparrow.wondershare.com
6 Connection: close
7 Accept-Encoding: gzip, deflate
8
9
10 --70db372eb000e2ax0
11 Content-Disposition: form-data; name="sdk_log"
12
13 {7cbbc7e8-399b-417f-9b54-5bed88895499}
14
15
16 --70db372eb000e2ax0
17 Content-Disposition: form-data; name="proc_name"
18
19 sdk
20
21
22 --70db372eb000e2ax0
23 Content-Disposition: form-data; name="tid"
24
25 UA-192455216-1
26
27
28 --70db372eb000e2ax0
29 Content-Disposition: form-data; name="client_sign"
30
31 {98CD3FF75429BA9F-1B135054341A75A332594187EE14268C}
32
33
34 --70db372eb000e2ax0
35 Content-Disposition: form-data; name="file"; filename="
36 {7cbbc7e8-399b-417f-9b54-5bed88895499}"
37 Content-Type: application/octet-stream
38
39 'QÓ«pAMQt0iU;b!]Iä@h@Úq%KÁÍÓ4_É,ÔWS·r7i!rÒIU
40 ü«p1D»)9W<\Ä{±i{Ä½!BwOPé òÔòcJ4i4#)êxÝAb?ÜéÆÜJñmô2É\iaö#iÆæpw@i t9Ézá³mOKë*ÉM8Äñi
41 Q3-eC6æffñ«ÄÄ_Éiø}#9UBÄiÄÉ8Ê(¹äÔE,Ü-jJii#viiWIKHPiäÄJà§³ñø
42 ±i((ê+-8\L°+@O>{GgâtdwYñiÉP4$÷63úßÁ mE]ÖG8biÜ}p,«3]E,1eM±ó!BîiWCä½,
43 Êñ&x¿Oóváí²ÿ*ô«³=y ö5Ü´özà!¾U´·¹DÖP¶fñ«Ü-"É/7Óa
44 Y'èKióvßNBfT1/8i\ñóß£´O!!³IoA[0úú
```

Abbildung 24: Burp Suite - Interaktion – http-POST-Befehl sparrow.wondershare.com

3.2.1 Versuchsaufbau Hardware-Tracker

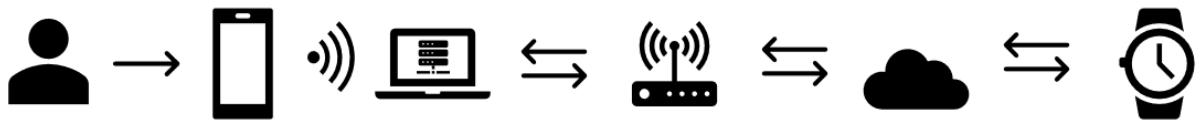


Abbildung 25: Versuchsaufbau Hardware-Tracker

Der Versuchsaufbau mit dem Hardware-Tracker unterscheidet sich von dem mit dem Software-Tracker insofern, dass das Smartphone zur Verwaltung des Trackers in Form der Smartwatch verwendet wird, Daten daher zwischen dem Smartphone und der Smartwatch versendet werden müssten, statt zwischen Smartphone und Elternportal.

3.2.2 Testgeräte

Aufgrund der sich nur marginal ändernden Situation an Testgeräten, wir hier nur die Smartwatch, die als Hardware-Tracker untersucht werden soll, als Testgerät mit hinzugefügt. Sämtliche Informationen zu den sonstigen Testgeräten kann Kapitel [3.1.2 Testgeräte](#) entnommen werden. Die Smartwatch bekommt weiterhin eine PrePaid-SIM-Karte (ALDI Talk), welches auf das Funknetz der Telefónica zurückgreift, sodass diese Befehle empfangen und senden kann.



Abbildung 26: Kinder-Tracker-Smartwatch mit Verpackung

3.2.3 Tools

Da weiterhin dieselben Tools verwendet werden, wie für die Untersuchung des Software-Trackers, sowie die Einrichtung der Testgeräte nicht weiter verändert wurde, sind diese Informationen aus Kapitel [3.1.3 Tools](#) zu erfahren.

3.2.4 Bestimmung Parameter

Für die Untersuchung des Hardware-Tracker-Traffics wird auf die Parameter aus Kapitel [3.1.4 Bestimmung Parameter](#) zurückgegriffen.

3.2.4.1 Messzeitraum

Es wird weiterhin in Wireshark ein Zeitraum von 60 Sekunden untersucht, welcher wieder ab Beginn des Aufnahmestarts gemessen wird.

3.2.4.2 Testszenarien

Bei den Testszenarien für die Smartwatch-Untersuchung wird das gleiche Prinzip gefahren, wie in Kapitel [3.1.4.2 Testszenarien](#). Jedoch, da bereits der Grundzustand des Smartphones gemessen wurde, entfällt dieses Testszenario in diesen Testreihen. Daher verbleiben folgende Testszenarien:

1. Messung mit installierter, aber weder geöffneter noch eingerichteter Tracking-App
2. Messung bei eingerichteter, geschlossenen App
3. Messung bei eingerichteter, geöffneter App mit Befehlsausführung

3.2.4.3 Wiederholbarkeit

Um auch hier wieder gesicherte Ergebnisse zu erhalten, wird jedes Testszenario drei Mal gemessen. Die Daten werden daraufhin im Einzelnen geprüft und in sinnvollen Bereichen kumuliert.

3.2.4.4 Durchführung der Messung

Zuletzt wird auch bei der Durchführung der Messung wie bei den vorherigen Messreihen vorgegangen. In Szenario 1 und 2 erfolgt die Messung, während das Smartphone bereits mit dem WLAN verbunden ist. Der Unterschied zum vorherigen Vorgehen besteht darin, dass die nun vorhandene Smartwatch als Bestandteil in dem Szenario betrachtet werden muss, welche bei allen Tests angeschaltet sein wird. Erst bei Szenario 3 wird wieder nach Ablauf von 10 Sekunden nach Start der Aufnahme bei Wireshark eine Interaktion durchgeführt. Diese Interaktion wird das Versenden einer Nachricht von der App zur Smartwatch sein.

3.2.5 Messungen

Für die Messungen müssen, aufgrund der dynamischen IP-Adressen-Zuteilung im WLAN dank DHCP an einem neuen Messtag, die IP-Adressen erneut abgefragt werden.

Beim Smartphone, da es sich dauerhaft im WLAN befunden hat, hat sich die IP-Adresse nicht verändert und ist weiterhin **192.168.2.101**. Beim Laptop dagegen hat sich die IP-Adresse auf **192.168.2.163** geändert.

3.2.5.1 Messung nach Installation der Tracking-App

Verglichen mit dem Grundzustand des Smartphones ist ein durchschnittlicher Anstieg des Paketvolumens um ca. 250% zu erkennen. Während der Grundzustand 206 Pakete enthielt, sind 520 Pakete nach der Installation der App, jedoch ohne Konfiguration, zu messen. Daher muss bereits, wie es bei dem Software-Tracker auch zu beobachten war, eine Kommunikation bzgl. der App vorhanden sein.

Statistik

Messwerte	Aufgezeichnet	Angezeigt
Pakete	1840	520 (28.3%)
Zeitspanne, s	327.882	267.931
Durchschnittliche pps	5.6	1.9
Durchschnittliche Paketgröße, B	128	165
Byte	235964	85703 (36.3%)
Durchschnittliche Byte/s	719	319
Durchschnittliche Bit/s	5757	2558

Abbildung 27: Wireshark - installiert o. Konfiguration – Statistik

Wirft man daraufhin einen Blick in die Wireshark-Aufnahme, lässt sich bei den Endpunkten jedoch nur eine Kommunikation zwischen dem Smartphone und dem Laptop erkennen. Die Begutachtung der http-Historie von Burp Suite zeigt nur die Kommunikation mit den bekannten Google-IP-Adressen.

IP-Adresse	Anbieter	Host-Adresse
172.217.16.132	Google LLC	google.com
142.250.186.163	Google LLC	connectivitycheck.gstatic.com
172.217.18.106	Google LLC	play.googleapis.com
142.250.184.234	Google LLC	play.googleapis.com

Tabelle 6: IP-Adressen Testszenario installiert o. Konfiguration

Zurück in Wireshark kann man sich wieder über den Pfad **Statistik > HTTP > Anfragen** sämtliche HTTP-Requests anzeigen lassen.

Neben der bekannten URL ***play.googleapis.com*** ist hier nun auch die URL ***infinitedata-pa.googleapis.com*** vorzufinden. Bis auf die Information, dass es sich hier um einen Tracker handelt, konnte nichts Spezifischeres gefunden werden.

3.2.5.2 Messung mit konfigurierter, im Hintergrund laufenden App

Wie auch bei dem Software-Tracker, wird die Verwaltungs-App nun auf dem Smartphone installiert. Durch einen QR-Code, der sowohl in der beiliegenden Anleitung abgedruckt als auch auf der Smartwatch aufrufbar ist, gelangt man zu einer Website mit der URL ***myaqsh.com***. Auf dieser gelangt man wiederum durch einen weiteren Klick, auf den jeweiligen App- bzw. Play-Store, um dort die jeweilige App herunterzuladen. Nach der Installation muss der App verschiedene Berechtigungen zugewiesen werden, sowie die Standortfreigabe aktiviert werden. Im Anschluss daran muss als letzter Schritt noch die Smartwatch mit der App verbunden werden, was wieder durch einen QR auf der Smartwatch erfolgt. Nach erledigter Einrichtung wird die App über den Taskmanager des Smartphones geschlossen. Dennoch ist zu erkennen, dass die App im Hintergrund weiterläuft.

Statistik

<u>Messwerte</u>	<u>Aufgezeichnet</u>	<u>Angezeigt</u>
Pakete	2740	1034 (37.7%)
Zeitspanne, s	2180.681	2166.318
Durchschnittliche pps	1.3	0.5
Durchschnittliche Paketgröße, B	138	172
Byte	377261	177415 (47.0%)
Durchschnittliche Byte/s	173	81
Durchschnittliche Bit/s	1384	655

Abbildung 28: Wireshark - konfig. App im Hintergrund–Statistik

Vergleichbar mit dem Software-Tracker, lässt sich auch hier erkennen, dass die Anzahl der Pakete zur vorherigen Messreihe gestiegen ist. Durch die Ansicht des I/O-Graphen kann man sehen, dass eine rege Kommunikation vom Smartphone aus ausgeht.

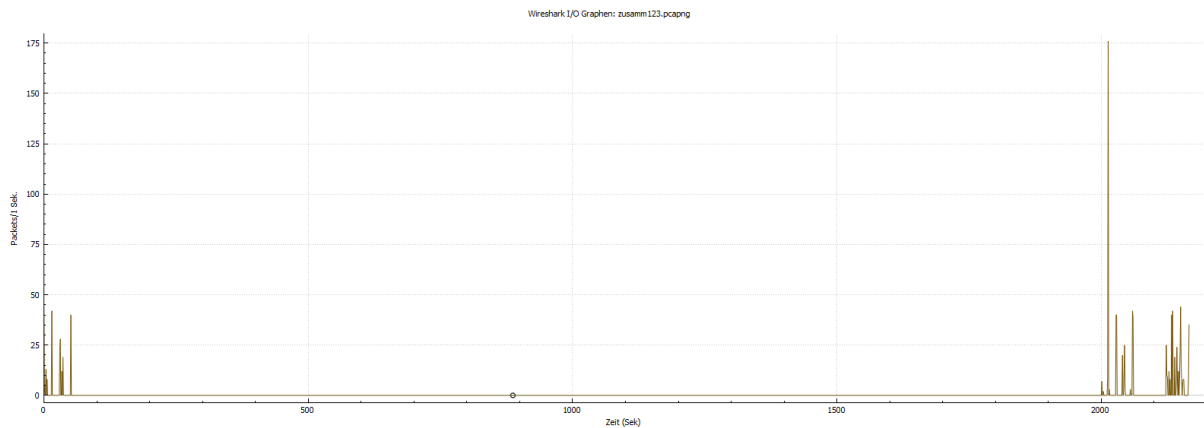


Abbildung 29: Wireshark - konfigur. App im Hintergrund - I/O Graph

Zwar werden in Wireshark immer noch nur die Endpunkte Laptop und Smartphone angezeigt, und in Burp Suite die bekannten IP-Adressen von **google.com**, **connectivitycheck.gstatic.com** und **play.googleapis.com**, in der http-Request-Übersicht von Wireshark kommen nun aber wieder zwei unbekannte URLs hinzu.

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
✓ HTTP Requests by HTTP Host	102				0,0000	100%	0,3200	2013,353
✓ www.google.com:443	9				0,0000	8,82%	0,0100	0,970
www.google.com:443	9				0,0000	100,00%	0,0100	0,970
✓ www.google.com	20				0,0000	19,61%	0,0900	2013,353
http://www.google.com/gen_204	6				0,0000	30,00%	0,0100	4,015
/gen_204	14				0,0000	70,00%	0,0900	2013,353
✓ playatoms-pa.googleapis.com:443	1				0,0000	0,98%	0,0100	2123,446
playatoms-pa.googleapis.com:443	1				0,0000	100,00%	0,0100	2123,446
✓ play.googleapis.com	15				0,0000	14,71%	0,0700	2013,370
http://play.googleapis.com/generate_204	4				0,0000	26,67%	0,0100	34,499
/generate_204	11				0,0000	73,33%	0,0700	2013,370
✓ pangolin16.isnssdk.com:443	21				0,0000	20,59%	0,0100	0,160
pangolin16.isnssdk.com:443	21				0,0000	100,00%	0,0100	0,160
✓ mdh-pa.googleapis.com:443	2				0,0000	1,96%	0,0100	2040,027
mdh-pa.googleapis.com:443	2				0,0000	100,00%	0,0100	2040,027
✓ connectivitycheck.gstatic.com	34				0,0000	33,33%	0,1600	2013,358
http://connectivitycheck.gstatic.com/generate_204	9				0,0000	26,47%	0,0100	0,965
/generate_204	25				0,0000	73,53%	0,1600	2013,358

Abbildung 30: Wireshark - HTTP-Requests

Über **pangolin16.isnssdk.com** scheint ein Tracker zu sein, der außerdem auch in der App **TikTok** verwendet wird³⁴.

Bei **mdh-pa.googleapis.com** lässt sich wieder nur herausfinden, dass es scheinbar ein Tracker ist. Wofür kann nicht beantwortet werden.

³⁴ vgl. GitHub.com - TheBlockListProject

3.2.5.3 geöffnete App mit Interaktion

Wie bereits einleitend in Kapitel [3.2.4.4 Durchführung](#) der Messung beschrieben, wird als Interaktion eine Nachricht von innerhalb der Verwaltungsapp an die Smartwatch geschickt. Der Text variiert pro Messung um 1 Zeichen mit dem Standardtext „test“ und der Nummer der Messung. Somit ergeben sich für die 3 Messungen jeweils die Texte „test1“, „test2“ und „test3“.

Statistik

Messwerte	Aufgezeichnet	Angezeigt
Pakete	2457	1058 (43.1%)
Zeitspanne, s	321.146	308.357
Durchschnittliche pps	7.7	3.4
Durchschnittliche Paketgröße, B	152	190
Byte	374507	201512 (53.8%)
Durchschnittliche Byte/s	1166	653
Durchschnittliche Bit/s	9329	5228

Abbildung 31: Wireshark - Interaktion – Statistik

Überraschender Weise gibt es keine signifikante Veränderung des Netzwerk-Traffics bei der Ausführung eines Befehls in der App. Vergleicht man die Werte aus dem Testszenario mit konfigurierter, aber im Hintergrund laufenden App, so ist nur ein Plus von 24 Paketen zu sehen.

Dennoch lässt sich erfassen, dass die Menge an geflossenen Bytes von ursprünglich ca. 86 kB, über 177 kB bis hin zu 201 kB angestiegen ist.

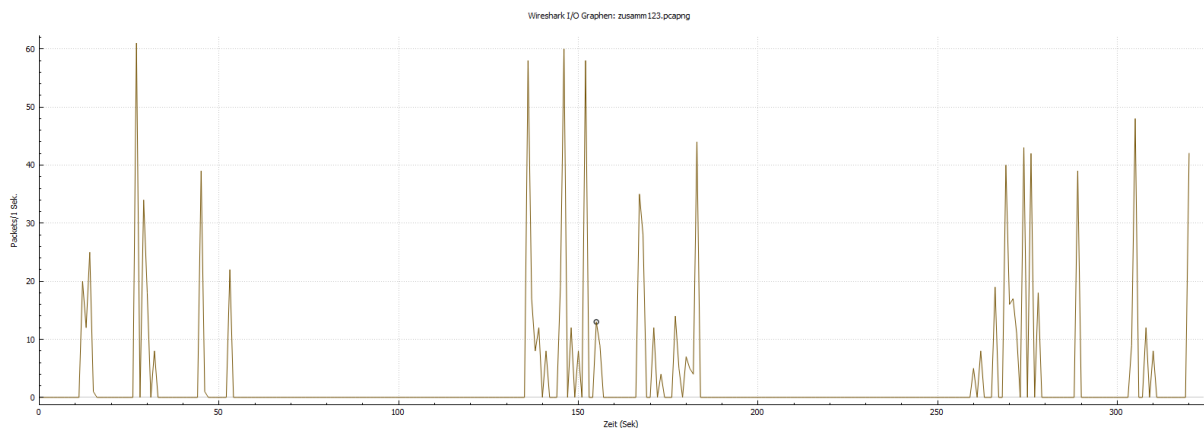


Abbildung 32: Wireshark - Interaktion - I/O Graph

Untersucht werden zuletzt auch wieder die Endpoints. Über die HTTP-Historie von Burp Suite gibt es keine neuen Erkenntnisse. Auch die Endpoints unter Wireshark sind weiterhin die gleichen. Bei dem HTTP-Request von Wireshark fügen sich nun zwei weitere URLs mit an.

geomobileservices-pa.googleapis.com ist voraussichtlich ein Tracker, der im Zusammenhang mit GPS oder dem Funknetz zu tun hat. Da jedoch keine belegenden Informationen hierzu zu finden sind, bleibt die vorherige Aussage eine Vermutung.

Mit **europa.myaqsh.com** wird hier wieder eine URL angezeigt, die im direkten Zusammenhang mit dem Anbieter steht. Dies lässt sich sagen, da **myaqsh.com** bereits zum Finden der zu installierenden App besucht werden musste.

Abschließend lässt sich zu allen 3 Testszenarien sagen, dass bei der Sichtung der Wireshark-Aufnahmen die Verschlüsselungen der Datenströme per TLSv1.2 und TLSv1.3 zu erkennen war.

4. Rechtliches und moralisches

Auch wenn in dieser Ausarbeitung keine direkten Hinweise auf Schwachstellen in der Datenübertragung gefunden werden konnten, können Geräte und Apps aus chinesischer Produktion für Misstrauen sorgen. Doch nicht nur Produkte aus dem asiatischen Raum müssen hier herangezogen werden, denn die Problemstellungen sind oftmals die gleichen. In einem Web-Artikel von dr-datenschutz.de lassen sich Argumente finden wie, dass „Daten teilweise auf weltweit verteilten Servern“³⁵ gespeichert werden und die „Datenschutzhinweise der Anbieter [...] oftmals unzureichend und intransparent“³⁶ sind. Man kann sich jedoch auch als Elternteil strafbar machen, sollte man ein Gerät anschaffen, welches über eine sogenannte Mithör- oder auch Monitorfunktion enthält, ein Mithören der Gespräche durch das Gerät, ohne einen optischen Hinweis auf das Abhören auf jenem anzuzeigen. Die Bundesnetzagentur hat solche Geräte als „verbotene Sendeanlagen“³⁷ definiert, wie es sich aus einer Pressemeldung der Behörde entnehmen lässt. Die Kombination aus GPS-Tracking und Mithörfunktion machen das Gerät zu einem Spionagegerät. Hier greift das TTDSG, das „Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei Telemedien“³⁸. In §8 TTDSG werden diese Punkt spezifiziert. Weiterhin sind Kinder auch Empfänger und Nutznießer der Grundrechte des Grundgesetzes. Die Verwendung solcher Geräte und Apps greifen auf das Recht der Privatsphäre und das Recht auf informationelle Selbstbestimmung ein, welches durch die Artikel 1 Abs. 1 und Artikel 2 Abs. 2 GG gedeckt sind. Auch die UN-Kinderrechtskonvention deckt das Recht auf Privatsphäre in Art. 16 ab. Hier heißt es:

„(1) Kein Kind darf willkürlichen oder rechtswidrigen Eingriffen in sein Privatleben, seine Familie, seine Wohnung oder seinen Schriftverkehr oder rechtswidrigen Beeinträchtigungen seiner Ehre und seines Rufes ausgesetzt werden.

(2) Das Kind hat Anspruch auf rechtlichen Schutz gegen solche Eingriffe oder Beeinträchtigungen.“³⁹

Zuletzt schützt auch die EU-weite Datenschutzgrundverordnung mit Erwägungsgrund 38 die Daten von Kinder, wofür der Bundes- und die Landesdatenschutzbeauftragten als oberste Instanzen zu sorgen haben⁴⁰.

³⁵ Dr. Datenschutz GPS-Überwachung

³⁶ Dr. Datenschutz GPS-Überwachung

³⁷ Bundesnetzagentur - Spionagegeräte

³⁸ TTDSG

³⁹ Unicef – UN-Kinderrechtskonvention

⁴⁰ EU-DSGVO Art. 57 Abs. 1b

Dagegen steht das Recht der Erziehung aus dem Grundgesetz. Darin ist festgehalten:

„Pflege und Erziehung der Kinder sind das natürliche Recht der Eltern und die zuvörderst ihnen obliegende Pflicht. Über ihre Betätigung wacht die staatliche Gemeinschaft.“⁴¹

Auch ist gesetzlich festgehalten, dass „die Eltern [...] die Pflicht und das Recht [haben], für das minderjährige Kind zu sorgen (elterliche Sorge). Die elterliche Sorge umfasst die Sorge für die Person des Kindes (Personensorge) und das Vermögen des Kindes (Vermögenssorge)“⁴². Weiter im Text heißt es, „[bei] der Pflege und Erziehung berücksichtigen die Eltern die wachsende Fähigkeit und das wachsende Bedürfnis des Kindes zu selbständigem verantwortungsbewusstem Handeln. Sie besprechen mit dem Kind, soweit es nach dessen Entwicklungsstand angezeigt ist, Fragen der elterlichen Sorge und streben Einvernehmen an“⁴³.

⁴¹ GG Art. 6 Abs. 2

⁴² BGB Art. 1626 Abs. 1

⁴³ BGB Art. 1626 Abs. 2

5. Fazit

In dieser Ausarbeitung konnten keine Schwachstellen in Form von unverschlüsselter Datenübertragung festgestellt werden, was zumindest bei den Anbietern der jeweiligen Apps auf ein gutes Sicherheitsverständnis bzgl. der Datenübertragung schließen lässt. Diese Feststellung lässt jedoch keine allgemeine Aussage bzgl. des Sicherheitsverständnisses chinesischer Hersteller und Entwickler treffen. Was jedoch festgestellt wurde ist, dass bereits die Installation einer App zu deutlich mehr Traffic auf dem Gerät führt. Durch die Konfiguration der jeweiligen App und die Ausführung von Befehlen darin steigt der Traffic noch weiter an. Inwiefern eine Übertragung an Dienste außerhalb der App-Anbieter stattfand oder welche Daten genau versendet wurden, kann aufgrund der TLS Verschlüsselung bei den Übertragungen nicht abschließend genannt werden. Aufgrund der weitreichenden Berechtigungen, die beide Apps jedoch erhalten, ist eine weitere Verwendung der Daten durch die Anbieter durchaus möglich.

Für aussagekräftigere Befunde müssten Langezeittests und die Sichtung der .apk-Quellcodes durch erfahrene Programmierer und Penetration Tester durchgeführt werden, die sich evtl. bereits mit dem Thema Smartwatches bzw. Kinder-Tracker beschäftigen haben.

Ein Learning aus dieser Hausarbeit war die Erkenntnis, für zukünftige Netzwerkmitschnitte eine Netzwerkkarte mit Monitoring-Funktion zu verwenden. Somit würde der Zwischenschritt des Proxy über z.B. Burp Suite entfallen und eine präzise Analyse der Ziel-IP-Adressen würde vorgenommen werden können.

Zuletzt wurde nach der Durchführung der Analysen und Auswertungen noch festgestellt, dass die WLAN-Funktionalität, im Vergleich zu den erwähnten Testgeräten im Internet-Artikel von Dr. Datenschutz (s. Seite 12), beim eigenen Testgerät nicht vorhanden war. Dieses Feature hätte eventuell noch einen weiteren Angriffsvektor dargestellt.

II. Literaturverzeichnis

Bloomberg. Wondershare Technology Group Co Ltd. *Bloomberg*. [Online] [Cited: 05 30, 2022.] <https://www.bloomberg.com/profile/company/300624:CH>.

Bundesamt für Justiz. 2002. Bürgerliches Gesetzbuch (BGB) § 1626 Elterliche Sorge, Grundsätze. *Bundesamt für Justiz*. [Online] Januar 2, 2002. [Cited: Juni 7, 2022.] https://www.gesetze-im-internet.de/bgb/___1626.html.

— **2021.** Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei Telemedien. *Bundesamt für Justiz*. [Online] Juni 23, 2021. [Cited: Mai 20, 2022.] <https://www.gesetze-im-internet.de/ttdsg/TTDSG.pdf>.

— **1949.** Grundgesetz für die Bundesrepublik Deutschland Art 6. *Bundesamt für Justiz*. [Online] Mai 23, 1949. [Cited: Juni 7, 2022.] https://www.gesetze-im-internet.de/gg/art_6.html.

Bundesamt für Sicherheit in der Informationstechnik Pressestelle. 2022. BSI warnt vor dem Einsatz von Kaspersky-Virenschutzprodukten. *Bundesamt für Sicherheit in der Informationstechnik*. [Online] März 15, 2022. [Cited: Mai 30, 2022.] https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2022/220315_Kaspersky-Warnung.html.

Bundeskriminalamt. 2022. Die polizeiliche Bearbeitung von Vermisstenfällen in Deutschland. *Bundeskriminalamt*. [Online] 2022. [Cited: Mai 20, 2022.] <https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/BearbeitungVermisstenfaelle/bearbeitungVermisstenfaelle.html;jsessionid=61AB567CFB70F04D0182740523E2A4C9.live292?nn=30666#doc19618bodyText3>.

Bundesnetzagentur. 2018. Pressemitteilung - Bundesnetzagentur geht gegen Ortungsgeräte. *Bundesnetzagentur*. [Online] April 5, 2018. [Cited: Mai 20, 2022.] https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Allgemeines/Presse/Pressemitteilungen/2018/20180405_GPSTracker.pdf?__blob=publicationFile&v=2.

Cisco Systems. 2018. Cisco Global Cloud Index: Forecast and Methodology, 2016–2021. *Cisco Systems*. [Online] Januar 2018. [Cited: Mai 30, 2022.] https://virtualization.network/Resources/Whitepapers/0b75cf2e-0c53-4891-918e-b542a5d364c5_white-paper-c11-738085.pdf.

CompTIA. What Is Wireshark and How Is It Used? *CompTIA*. [Online] [Cited: Juni 2, 2022.] <https://www.comptia.org/content/articles/what-is-wireshark-and-how-to-use-it>.

Dr. Datenschutz. 2021. GPS-Überwachung bei Kindern: Fürsorge oder naiver Kontrollzwang? *Dr. Datenschutz*. [Online] November 11, 2021. [Cited: Mai 20, 2022.] <https://www.dr-datenschutz.de/gps-ueberwachung-bei-kindern-fuersorge-oder-naiver-kontrollzwang/>.

Ebert, Bastian. 2021. Connectivitycheck – was steckt hinter dieser Webseite und eventuellen Fehlermeldungen? *APPDATED*. [Online] Juli 21, 2021. [Cited: Juni 6, 2022.] <https://www.appdated.de/2021/07/connectivitycheck-was-steckt-hinter-dieser-webseite-und-eventuellen-fehlermeldungen/>.

ESET. Über ESET. *ESET*. [Online] [Cited: Mai 29, 2022.] <https://www.eset.com/de/about/>.

-
- 2015.** Familienreport 2015. *statista.de*. [Online] 2015. [Cited: Mai 31, 2022.] <http://www.marketagent.com/webfiles/MarketagentCustomer/pdf/2280b5ee-b1df-4e99-bfcd-6a80859e2f67.pdf>.
- Firestore.** 2022. FirestoreInAppMessaging. *Firestore*. [Online] März 11, 2022. [Cited: Juni 7, 2022.] <https://firebase.google.com/docs/reference/android/com/google/firebase/inappmessaging/FirebaseInAppMessaging>.
- fmk.at.** 2021. *Mobilfunkmarkt Österreich 2020*. Mai 20, 2021.
- Google.** 2015. Digital Asset Links API. *Google Digital Asset Links*. [Online] Oktober 29, 2015. [Cited: Juni 7, 2022.] <https://developers.google.com/digital-asset-links/reference/rest>.
- intersoft consulting.** Art. 57 DSGVO Aufgaben. *intersoft consulting*. [Online] [Cited: Mai 20, 2022.] <https://dsgvo-gesetz.de/art-57-dsgvo/>.
- IONOS.** 2018. IGMP: Das steckt hinter dem Internet Group Management Protocol. *IONOS*. [Online] Dezember 6, 2018. [Cited: Juni 6, 2022.] <https://www.ionos.de/digitalguide/server/knowhow/igmp-internet-group-management-protocol/>.
- Ivanov, Sofia.** Was ist Firebase? Alle Geheimnisse entschlüsselt. *back4app*. [Online] [Cited: Juni 7, 2022.] https://blog.back4app.com/de/was-ist-firebase/#Was_ist_Google_Firebase.
- Kaspersky Lab.** 2022. KasperskySafe Kids. *Kaspersky Lab*. [Online] 2022. [Cited: Mai 30, 2022.] <https://www.kaspersky.de/safe-kids>.
- . 2022. Über uns. *Kaspersky Lab*. [Online] 2022. [Cited: Mai 29, 2022.] <https://www.kaspersky.de/about>.
- Kaspersky, Eugene.** 2022. Kollateralschaden – für die Cybersicherheit. *Kaspersky Lab*. [Online] März 16, 2022. [Cited: Mai 30, 2022.] <https://www.kaspersky.de/blog/collateral-damage-on-cybersecurity/28295/>.
- Luber, Stefan and Schmitz, Peter.** 2017. Was ist TLS (Transport Layer Security)? *Security Insider*. [Online] Dezember 28, 2017. [Cited: Juni 6, 2022.] <https://www.security-insider.de/was-ist-tls-transport-layer-security-a-673066/>.
- Morgenstern, Maik.** 2019. Produktwarnung! Chinesische Kinderuhr verrät tausende Kinder. *AV-Test Internet of Things Blog*. [Online] November 25, 2019. [Cited: Mai 20, 2022.] <https://www.iot-tests.org/de/2019/11/produktwarnung-chinesische-kinderuhr-verraet-tausende-kinder/>.
- mpfs.** 2020. Internetnutzung von Kindern und Jugendlichen. *statista.de*. [Online] 2020. [Cited: Mai 26, 2022.] Abschnitt: Anteil der Jugendlichen in Deutschland, die ein Smartphone besitzen, nach Altersgruppen im Jahr 2021. <https://de.statista.com/statistik/studie/id/40511/dokument/internetnutzung-durch-kinder-und-jugendliche-statista-dossier/>.
- . 2022. Mediennutzung von Kindern. *statista.de*. [Online] 2022. [Cited: Mai 26, 2022.] Abschnitt: Welche Geräte besitzt Ihr Kind. <https://de.statista.com/statistik/studie/id/26424/dokument/mediennutzung-von-kindern-statista-dossier/>.
- Nadar.** 2021. Googlecast SSDP and MDNS queries on network despite not having any chromecast applications installed in main computer. *Serverfault*. [Online] Dezember 17, 2021. [Cited: Juni 6,

2022.] <https://serverfault.com/questions/1005372/googlecast-ssdp-and-mdns-queries-on-network-despite-not-having-any-chromecast-ap>.

OffSec Services Ltd. 2022. Burpsuite. *Kali Tools*. [Online] Februar 10, 2022. [Cited: Juni 4, 2022.] <https://www.kali.org/tools/burpsuite/>.

r-a-y and XhmikosR. 2022. Usercontent - AdguardMobileSpyware. *GitHub*. [Online] Juni 6, 2022. [Cited: Juni 7, 2022.] <https://github.com/r-a-y/mobile-hosts/blob/master/AdguardMobileSpyware.txt>.

red/dpa/lsw. 2022. Fast 200 Kinder unter 14 gelten als vermisst. *Stuttgarter Nachrichten*. [Online] Mai 24, 2022. [Cited: Mai 26, 2022.] <https://www.stuttgarter-nachrichten.de/inhalt.baden-wuerttemberg-fast-200-kinder-unter-14-gelten-als-vermisst.25b49207-47c0-4ba3-a8a0-443dfccbe5c1.html>.

Robert. 2021. What are all these Google internet hosts (domains) and why is stripped-down Android connecting to all of them? *StackExchange*. [Online] Januar 27, 2021. [Cited: Juni 6, 2022.] <https://android.stackexchange.com/questions/233263/what-are-all-these-google-internet-hosts-domains-and-why-is-stripped-down-andr>.

Schäfer, Karolin. 2022. Russischer Cyberangriff auf Stromversorgung in der Ukraine: „Bedrohung auch für andere Länder“. *Frankfurter Rundschau*. [Online] April 13, 2022. [Cited: Mai 30, 2022.] <https://www.fr.de/politik/ukraine-krieg-russland-hacker-stromversorgung-sandstorm-cyberangriff-malware-energie-91478949.html>.

The Block List Project. 2022. TikTok List. *GitHub*. [Online] Februar 21, 2022. [Cited: Juni 7, 2022.] <https://github.com/blocklistproject/Lists/blob/master/tiktok.txt>.

Treanor, Michael. 2020. Who originally suggested that 'if you're not paying for the product, you are the product'? *Quora*. [Online] 2020. [Cited: Mai 30, 2022.] <https://www.quora.com/Who-originally-suggested-that-if-youre-not-paying-for-the-product-you-are-the-product#nAcUQ>.

unicef. DIE UN-KINDERRECHTSKONVENTION. *unicef*. [Online] [Cited: Mai 20, 2022.] <https://www.unicef.de/informieren/ueber-uns/fuer-kinderrechte/un-kinderrechtskonvention#pdf>.

III. Abbildungsverzeichnis

Abbildung 1: Ausschnitt der Statistik zur Anzahl der Kinder mit eigenem Smartphone / Handy; Quelle mpfs / statista.de	5
Abbildung 2: Statistik zum Anteil der Jugendlichen mit eigenem Smartphone nach Altersgruppen im Jahr 2021; Quelle: mpfs / statista.de	5
Abbildung 3: Statistik Prognose globaler Datenmengen; Quelle: Cisco Systems / statista.de	10
Abbildung 4: Anzeigen-Foto der Kinder-Smartwach von ebay.de	12
Abbildung 5: Versuchsaufbau Software-Tracker	13
Abbildung 6: Burp Suite - Startbildschirm	14
Abbildung 7: Burp Suite - Einstellung Proxy-Verbindung	15
Abbildung 8: Samsung - Einstellung Proxy	15
Abbildung 9: Wireshark – Grundzustand - Statistik	17
Abbildung 10: Wireshark – Grundzustand - I/O Graph	18
Abbildung 11: Wireshark – Grundzustand - Endpoints	18
Abbildung 12: Wireshark - installiert o. Konfiguration - Statistik	19
Abbildung 13: Wireshark - installiert o. Konfiguration - I/O Graph	19
Abbildung 14: Burp Suite - installiert o. Konfiguration - Messung 1 - http-History	20
Abbildung 15: Wireshark - konfig. App im Hintergrund– Statistik	21
Abbildung 16: Wireshark - konfig. App im Hintergrund - I/O Graph	21
Abbildung 17: Burp Suite - konf. App im Hintergrund - http-History	22
Abbildung 18: IP-Lookup per https://whatismyipaddress.com/ip/47.88.92.42	22
Abbildung 19: Burp Suite - konf. App im Hintergrund - http-Post-Befehl von FamiSafe	23
Abbildung 20: Burp Suite - konf. App im Hintergrund – Messung 2 - Ausschnitt http-Post-Befehl an FamiSafe-Server Datenbank	24
Abbildung 21: Hinweis HMACSHA1-Verschlüsselung in FamiSafe.apk	24
Abbildung 22: Wireshark - Interaktion – Statistik	26
Abbildung 23: Wireshark - Interaktion - I/O Graph	26
Abbildung 24: Burp Suite - Interaktion – http-POST-Befehl sparrow.wondershare.com	27
Abbildung 25: Versuchsaufbau Hardware-Tracker	28
Abbildung 26: Kinder-Tracker-Smartwatch mit Verpackung	28
Abbildung 27: Wireshark - installiert o. Konfiguration – Statistik	30
Abbildung 28: Wireshark - konfig. App im Hintergrund– Statistik	31
Abbildung 29: Wireshark - konfig. App im Hintergrund - I/O Graph	32
Abbildung 30: Wireshark - HTTP-Requests	32
Abbildung 31: Wireshark - Interaktion – Statistik	33
Abbildung 32: Wireshark - Interaktion - I/O Graph	33

IV. Tabellenverzeichnis

Tabelle 1: Ausschnitt Aufstellung Apps.....	7
Tabelle 2: Ausschnitt Vergleich der App-Funktionen	7
Tabelle 3: Anzahl der App-Funktionen.....	8
Tabelle 4: IP-Adressen Testszenario installiert o. Konfiguration	20
Tabelle 5: IP-Adressen Testszenario App konfiguriert und im Hintergrund	22
Tabelle 6: IP-Adressen Testszenario installiert o. Konfiguration	30