Hochschule Wismar
Fakultät für Ingenieurwissenschaften
Bereich Elektrotechnik und Informatik

Eignung des Einsatzes von „PortableApps“ als anti-forensische Maßnahme

IT-Forensik Projekt II

eingereicht von: [redacted]
Studiengang Bachelor IT-Forensik

Betreuer: Prof. Dr.-Ing. Antje Raab-Düsterhöft

[redacted]

Aufgabenstellung

Überprüfung der forensischen Nachvollziehbarkeit des Einsatzes von ausgewählter Software unter Verwendung von ‚PortableApps.com Platform™' zwecks Feststellung der Eignung als antiforensisches Mittel.

Kurzreferat

„Keep Work and Personal Separate“ – mit diesem Slogan wirbt der Entwickler von ‚PortableApps.com Platform™‘ auf seiner Homepage und möchte damit den Mehrwert der Trennung von privat und beruflich genutzter Software hervorheben. Dieser Ansatz der Trennung dürfte auch beim forensischen Verwischen von Spuren (Anti-Forensik) auf genutzten Rechnern von hohem Interesse sein, sodass es sich bei der Software um ein geeignetes anti-forensisches Mittel handeln würde.

Die Software erlaubt es, ohne Installation der benötigten Apps auf dem Host selbst diese mit einem USB-Stick zu verwenden. Insgesamt können über 450 Apps aus unterschiedlichsten Einsatzgebieten wie beispielsweise „Entwicklerwerkzeuge“, „Dienstprogramme“ oder „Security“ auf diesem Wege verwendet werden.

Ziel dieser Projektarbeit ist es zu prüfen, inwiefern man Spuren von eingesetzter Software auf dem Host vorfindet und ob beziehungsweise wie tiefgehend die Rückverfolgung der durchgeführten Aktivitäten nachweisbar ist. Hierfür wurden die portablen Versionen der Apps ‚Thunderbird‘ und ‚Telegram‘ ausgewählt. Die forensische Analyse wurde, neben manueller Einsicht in Systemkonfigurationen, unter Zuhilfenahme der Analysetools MUICacheView, Wireshark sowie Volatility3 vorgenommen.

Die Überprüfung anhand des Testszenarios hat ergeben, dass es sich bei der Software ‚PortableApps.com Platform™‘ um eine teilweise geeignete antiforensische Maßnahme handelt. Es bedarf weiterer manueller Schritte oder des Einsatzes von Programmen, die gegebenenfalls als Portable-Version vorhanden sind, um den antiforensischen Erfolg zu komplettieren.

Inhalt

1 Einführung und Motivation

Im Digitalzeitalter ist die Privatsphäre eines der meistdiskutierten Themen in der Öffentlichkeit. Auch wenn die Mehrheit der Deutschen Zweifel daran hat, Kontrolle über ihren persönlichen Daten im Internet zu haben[1], ist vielen in diesem Zusammenhang nicht bewusst, wie viel digitale Spuren sie im Internet oder auf einer genutzten Hardware, teilweise aufgrund von fahrlässiger Nutzung, hinterlassen.

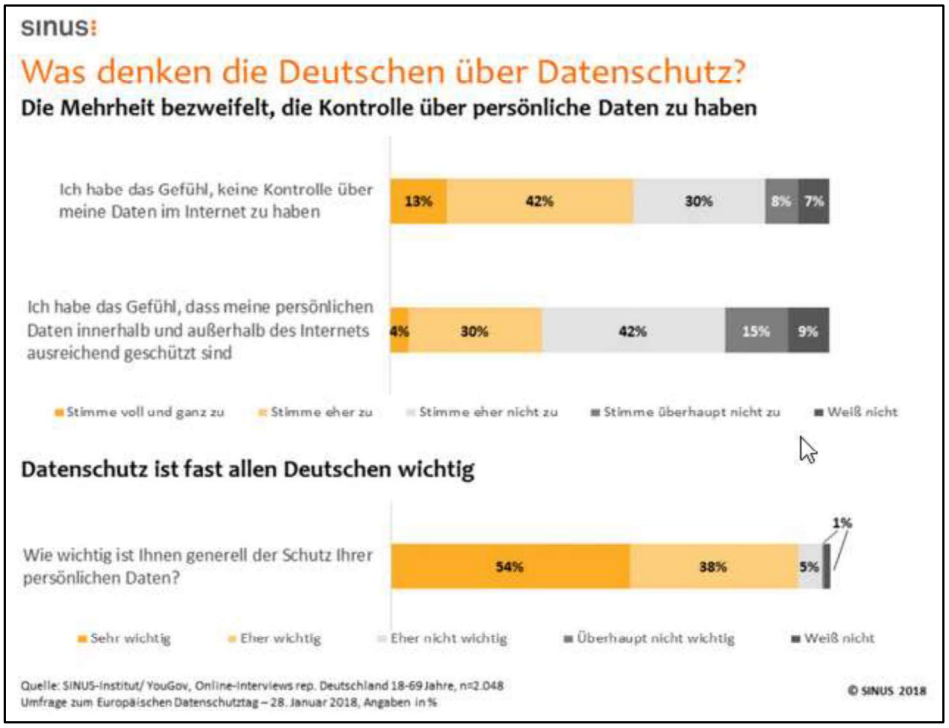


Bild 1: Umfrage zum Datenschutz

Eine Abhilfe zum Schutz seiner Daten soll die Software ‚PortableApps.com Platform™ ' geben. Sie ermöglicht die vom Endanwender genutzte Software stets bei sich zu haben und diese von einem externen Laufwerk an jedem beliebigen Rechner ausführen zu können, ohne Spuren zu hinterlassen. Die vermeintlich

---

1 https://www.sinus-institut.de/media-center/presse/mehrheit-der-deutschen-zweifelt-an-datensicherheit

gebotene Privatsphäre lädt allerdings dazu ein, die PortableApps zu antiforensischen Zwecken zu nutzen, um flexibel und unerkannt auf fremden Endgeräten zu agieren.

1.1 Was ist Anti-Forensik?

Bislang wurde keine offizielle Definition für Anti-Forensik seitens des BSI veröffentlicht. Im „Leitfaden für IT-Forensik“ findet sich lediglich eine formale Definition von IT-Forensik, wonach „IT-Forensik [ist] die streng methodisch vorgenommene Datenanalyse auf Datenträgern und in Computernetzen zur Aufklärung von Vorfällen unter Einbeziehung der Möglichkeiten der strategischen Vorbereitung insbesondere aus der Sicht des Anlagebetreibers eines IT-Systems[2] ist.[3] Daraus kann man sich zumindest eine sinngemäße Definition von Anti-Forensik als eine streng methodisch vorgenommene Datenspurenbeseitigung auf Datenträgern und in Computernetzen unter Einbeziehung der Möglichkeiten der strategischen Vorbereitung auf einen Hacking-Angriff aus Sicht des Hackers herleiten.

Ein weiterer Versuch, die Anti-Forensik auf Basis des verwendeten Vokabulars zu definieren, wurde von Ryan Harris unternommen. Hierbei bezieht er sich auf die Wortdefinition von „anti“, was gleichbedeutend mit „im Gegensatz zu“ oder „dagegen“ ist, sowie „forensics“ als die Anwendung der Wissenschaft auf die Straf- und Zivilgesetze, die von Polizeibehörden in einem Strafjustizsystem durchgesetzt werden. Als Kombination der beiden Begrifflichkeiten lässt sich Anti-Forensik vorläufig als Methode definieren, die verwendet wird, um die

---

[2] „Unter dem Begriff informationstechnisches System (IT-System) versteht man jegliche Art elektronischer datenverarbeitender Systeme.“ [https://de.wikipedia.org/wiki/Informationstechnisches_System]

[3] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2022/05_DER_Detektion_und_Reaktion/DER_2_2_Vorsorge_fuer_die_IT_Forensik_2022.pdf?__blob=publicationFile&v=3

Anwendung der Wissenschaft auf jene Straf- und Zivilgesetze zu verhindern (oder dagegen vorzugehen), die von Polizeibehörden in einem Strafjustizsystem durchgesetzt werden. Diese Definition bietet eine korrekte technische Beschreibung des Problems, ist jedoch für den Standardgebrauch zu umfangreich.[4]

Die Problematik der fehlenden formalen Definition für Anti-Forensik führt dazu, dass unter anderem Auswerter und Wissenschaftler auf eigene Erfahrungen und Definitionen zurückgreifen müssen und die Aussagen dahingehend entsprechend variieren.[5]

Die Methoden der Anti-Forensik sind insgesamt sehr breitflächig und umfassen tiefergehende Änderungen in den IT-Systemen, beispielsweise Löschungen von Registry-Einträge oder Metadaten, bis hin zu „primitiven“ Methoden wie physische Zerstörung der Hardware. Eine erweiterte Version der Anti-Computer-Forensik-Taxonomie von Rogers (2006)[6] umfasst tiefere, detailliertere Spezifikationen innerhalb der bestehenden Klassifizierungen.[7] Taxonomien sind für wissenschaftliche Bereiche nützlich, da sie strukturierte Klassifizierungen innerhalb einer Domäne aufzeigen.

Darüber hinaus benötigt es heutzutage keine tiefergehenden IT-Kenntnisse, um sich mit Anti-Forensik beschäftigen zu können. Viele Enduser setzen anti-forensische Mittel unbewusst im Alltag ein, indem sie beispielsweise VPN-Verbindungen und auf Privatsphäre fokussierte Suchmaschinen wie ‚DuckDuckGo‘ verwenden. Auch das Verwenden des Browser Private-Mode und

---

4 https://www.sciencedirect.com/science/article/pii/S1742287606000673

5 https://www.sciencedirect.com/science/article/pii/S1742287606000673

6 https://www.sciencedirect.com/science/article/pii/S1742287616300378

7 Anhang Taxonomie

das Löschen des Cache im Webbrowser stellen einen gewissen anti-forensischen Aspekt dar.
Mittlerweile sind die Methoden der Anti-Forensik ausgereift und versuchen, tiefere Instanzen als nur den angegriffenen/benutzten Computer zu manipulieren. Man kann von fortgeschrittener Anti-Forensik sprechen, wenn bewusst die Inhalte von einem zur forensischen Analyse bereitstehenden Hardware so manipuliert werden, dass die zur Forensik verwendete Software angegriffen wird. Ein Beispiel dafür ist eine gezielt abgelegte ZIP-Datei, die beim Entpacken Terabytes an Daten produziert und damit die vorhandenen Ressourcen ausschöpft.[8]

Es können also einige Veränderungen in den Konfigurationen oder ein nachträgliches Löschen von Registry-Einträgen/Logs zur erschwerten Durchführung einer erfolgreichen forensischen Analyse führen.
Die aktive Manipulation des Endgeräts wird in diesem Testaufbau vernachlässigt, da das Ziel des Projekts die Überprüfung ist, ob die Software-Suite ‚PortableApps' selbst als geeignetes antiforensisches Mittel fungieren kann.

1.2 Was sind ‚PortableApps' und wie verbindet man sie mit Anti-Forensik?

„Use PortableApps.com for your personal apps on your work PC or for your work apps on your personal PC"[9]

„The app does not leave any digital residues on the system."[10]

„…they don't interfere with any other programs installed on your PC, and they can

---

8 https://www.com-magazin.de/praxis/sicherheit/digitaler-spurensuche-mithilfe-it-forensik-1625707.html?page=3_anti-forensiker-vs.-forensiker

9 https://portableapps.com/

10 http://techzle.com/this-is-how-you-make-portable-apps-yourself

be used on PCs with restricted user permissions…“[11]

Nach Aussage des Anbieters ‚PortableApps.com Platform™‘, die auch von Fachzeitschriften gestützt wird, sollen die portablen Versionen von Programmen keine Spuren auf den genutzten Rechnern hinterlassen. Daraus lässt sich die Verbindung von der Software zu der Anti-Forensik leicht ableiten: keine Spuren, kein Erfolg der forensischen Analyse.

Insgesamt bietet ‚PortableApps.com Platform™‘ über 450 Apps/Programme an, die separat vom genutzten Betriebssystem gelagert und ausgeführt werden können. Die Programme können sowohl über den ‚PortableApps-Launcher‘ als auch nativ über den entsprechenden Installationspfad auf dem externen Speichermedium ausgeführt werden.[12] Dadurch soll neben Speicherplatz-Einsparung auch ein Mehrwert für die Privatsphäre entstehen. Dieser Mehrwert könnte über den Schutz der Privatsphäre hinweg zu kriminellen Zwecken erweitert werden.

Durch die Auslagerung der auszuführenden Programme auf ein externes Medium in der Software-Suite ‚PortableApps.com Platform™‘ sollte in erster Linie die Protokollierung, also die Nachweisbarkeit der Ausführung, verhindert werden. Unter der Voraussetzung, dass die entsprechende Nachweisbarkeit der Nutzung der Programme auf dem externen Medium nicht gegeben ist, kann die Software ‚PortableApps‘ durchaus mit Anti-Forensik in Verbindung gebracht werden.

1.3 Abgrenzung „live“ zu „post mortem“ Forensik

Insgesamt lassen sich die IT-forensischen Möglichkeiten grob in zwei Methoden unterscheiden: „post mortem“ und „live“.

---

[11] https://www.techradar.com/news/the-best-portable-apps

[12] Anhang PortableApps-Launcher

Bei der „post mortem“ Forensik spricht man von nachträglicher Analyse der Systeme nach einem stattgefundenen (Hacking-)Angriff. Hierbei wird versucht auf dem infizierten/beschädigten System nach Ursachen (beispielsweise ein Datenleck oder eine Sicherheitslücke) zu suchen, um den Angriff zu analysieren. Ein Vorteil dieser Methode ist, dass die zum Sicherungszeitpunkt vorliegenden Daten nicht mehr nachträglich unbemerkt manipuliert werden können.[13]

Wie der Begriff „live“ schon vermuten lässt, ist bei dieser Art der Forensik von einer Analyse am laufenden System beziehungsweise während des zu diesem Zeitpunkt andauernden Angriffs die Rede. Bei dieser Analysemethode werden die stattfindenden Ereignisse in der System- oder Netzwerkumgebung analysiert und es wird versucht die mögliche Angriffsquelle ausfindig zu machen und gegebenenfalls zu neutralisieren (zum Beispiel ein offener Port in der Firewall über den ein DDoS-Angriff stattfindet). Live-Forensik ist aufwändiger und gilt in der forensischen Welt als „Königsdisziplin“.[14]

Für diese Ausarbeitung werden die beiden Methoden kombiniert, um mehr Erkenntnisse sammeln zu können. Die Live-Forensik wird allerdings nicht, wie üblich, direkt angewendet und ausgewertet, sondern durch einen Live-Mitschnitt des Netzwerk-Traffics umgesetzt. Die Analyse des Traffics findet dann auf die Art der „post mortem“ Forensik statt.

---

13 https://www.com-magazin.de/praxis/sicherheit/digitaler-spurensuche-mithilfe-it-forensik-1625707.html?page=1_post-mortem-vs.-live-analyse

14 https://www.com-magazin.de/praxis/sicherheit/digitaler-spurensuche-mithilfe-it-forensik-1625707.html?page=2_live-ist-king

2 Durchführung

Für die Überprüfung der Eignung von ‚PortableApps' als anti-forensische Maßnahme wird zunächst eine Legende, unter der die Ausführung der Apps auf einem Windows-Rechner plausibilisiert wird, erstellt.

Ein Hacker hat demnach den vollen Zugriff auf die Hardware (Windows-Rechner) und benutzt diesen als eine Art „Man in the Middle", um mit externen Quellen zu kommunizieren und gegebenenfalls illegale Inhalte auszutauschen und Inhalte vom Endgerät zu verschicken. Um auch im Nachgang unerkannt zu bleiben, verwendet er seinen eigenen USB-Stick, auf dem die benötigten Programme über die Software ‚PortableApps.com Platform™' ausgeführt werden. Aufgrund der kurzen Zugriffszeit auf den Windows-Rechner wird lediglich die Windows-Aktivitäten Verfolgung manuell deaktiviert und keine weiteren anti-forensischen Maßnahmen getroffen, so dass seine einzige Absicherung die Software an sich ist.

Um den Aufwand für die forensische Untersuchung zu reduzieren, wird die Auswahl der verwendeten Apps als bekannt vorausgesetzt. Somit kann sich die anschließende forensische Auswertung speziell auf die Feststellung dieser App-bezogener Spuren, wie beispielsweise Standard-Portnummern, fokussieren.

2.1 Auswahl Hardware

2.1.1 Laptop

Für das Testszenario wird als Host ein „HP ProBook 650 G2" mit Intel Core i7 Prozessor und 16 GB Arbeitsspeicher verwendet. Beim Betriebssystem des Hosts handelt es sich um ein Windows 10 Pro OS.[15] Des Weiteren verfügt der

[15] Anhang Windows-Spezifikationen

Host über das lizensierte Antivirus-Programm ‚TrendMicro'[16].

Um sicherzugehen, dass die eingesetzten Programme uneingeschränkt genutzt werden können, wird der USB-Stick mit der Software ‚PortableApps.com Platform™' in einem mit Admin-Rechten ausgestatten User-Account eingebunden. Im vorliegenden Szenario wird angenommen, dass der Anwender auf unbekannte Art und Weise Zugang zu den erforderlichen Zugangsdaten des Users „Hackerman", der über die benötigte Rechte verfügt, erlangt hat.

Während des Software-Einsatzes wird zur Herstellung der Netzwerkkonnektivität die WLAN-Schnittstelle des Laptops genutzt und mit einem 2,4 Ghz WLAN-Netzwerk verbunden.[17]

Die einzige auf dem Endgerät vorgenommene Änderung bezieht sich auf den Windows-Aktivitätsverlauf. Hierbei handelt es sich um die Protokollierung jeglicher Windows-Aktivitäten und ist ohne tiefergehende Informatik-/Computerkenntnisse in den Windows-Einstellungen regelbar. Da diese Änderung keinen großen Zeitaufwand nach sich zieht, wird die Protokollierung ausgeschaltet.

2.1.2 USB-Stick

Bei dem eingesetzten USB-Stick, auf dem die Software installiert und ausgeführt wird, handelt es sich um einen handelsüblichen 16 GB USB-Stick der Marke ‚Transcend' ohne Verschlüsselung. Der USB-Stick erfüllt die Kompatibilitätsvoraussetzungen zum Datentransfer über eine USB3.0 Schnittstelle und wird bei diesem Testszenario über eine solche Schnittstelle eingebunden.

---

[16] Anhang TrendMicro „About"

[17] Anhang WLAN Spezifikationen

2.2 Auswahl und Einsatz der PortableApps

2.2.1 Software-Suite PortableApps

Die Installationsdatei ‚PortableApps.com_Platform_Setup_25.0.paf' wird direkt auf dem USB-Stick gespeichert und ausgeführt. Die Installation erfolgt mit den Standard-Einstellungen des Installation-Wizard.[18] Die gesamte Installation wurde auf einem separaten Rechner durchgeführt, um die Testumgebung nicht im Voraus versehentlich zu manipulieren.

Nach Abschluss der Installation bestehen die Möglichkeiten den PortableApps-Launcher zu starten, über dem man die entsprechenden Programme ausführen kann, oder die entsprechenden Programme direkt über den Speicherort in der Ordnerstruktur mittels EXE-File auszuführen. Um möglichst viele Erkenntnisse sammeln zu können, wird je ein Programm über den Launcher und ein Programm über die normale Ordnerstruktur ausgeführt.

Zusätzlich zu den ausgewählten Hauptprogrammen wird die Portable-App „Don't sleep"[19] gestartet, damit der Rechner nicht aufgrund von möglicher Nichtaktivität in den Ruhemodus übergeht. Dies soll einerseits einen möglichst realitätsnahen Angriff simulieren und andererseits eine weitere Möglichkeit geben, bei dem Testszenario im Nachhinein Erkenntnisse zur Fremdnutzung des Geräts bei der forensischen Analyse festzustellen. Im Falle einer Erkennung des Einsatzes von „Don't sleep" kann man zumindest von einer verdächtigen Aktivität ausgehen und beim Vorfinden weiterer Indizien auf eine vorangegangene Rechnermanipulation oder Ähnliches schließen.

---

[18] Anhang Installation PortableApps-Suite

[19] Anhang Don't sleep

2.2.2 Mozilla Thunderbird Portable

Vorbereitung

Beim Programm ‚Mozilla Thunderbird' handelt es sich um ein weitverbreitetes, kostenloses Open Source E-Mail-Programm. Die Kernaufgabe des Programms ist der Austausch von E-Mails mit externen Kommunikationspartnern. Generell besteht die Möglichkeit, dass bei der Verwendung von personalisierten Postfächern persönliche Daten auf dem Rechner zurückbleiben und beispielsweise im Cache abgelegt werden. In der Beschreibung der Portable-Version wird allerdings explizit darauf hingewiesen, dass keine persönlichen Informationen auf dem ausgeführten Endgerät zurückbleiben und man somit seine Adressbücher und E-Mails überall sorgenfrei mitnehmen kann.[20] Dieser Hinweis war für die Entscheidung, dieses Programm für das Testszenario einzusetzen, von grundlegender Bedeutung.

Zur Vorbereitung des Einsatzes auf dem Zielrechner wird im Voraus ein Gmail-Mailkonto in Thunderbird eingerichtet, so dass man bei der Ausführung lediglich den Mailversand tätigen muss.

Ausführung

Unmittelbar nach der Ausführung des Programms über den PortableApps-Launcher öffnet sich neben Thunderbird der lokal auf dem Rechner installierte Webbrowser ‚Mozilla Firefox'. In dem automatisch geöffneten Fenster erscheint eine Webseite von thunderbird.net, auf der sich ein Spendenaufruf für die Mozilla-Organisation befindet.[21] Beide Programme gehören zu der US-amerikanischen Non-Profit-Organisation ‚Mozilla Foundation'.

---

[20] https://portableapps.com/apps/internet/thunderbird_portable

[21] https://www.thunderbird.net/de/thunderbird/102.0/eoy

Das unerwartete Öffnen des Browsers kann dazu führen, dass weitere Datenspuren auf dem Endgerät zurückbleiben. Um diese Datenspur erkennen zu können, muss der Auswerter allerdings Kenntnis von dem Zusammenhang zwischen ‚Mozilla Firefox' und ‚Mozilla Thunderbird' dahingehend kennen, dass eine automatisierte Webseite aufgerufen wird.

Nach der vollendeten Synchronisierung des im Thunderbird hinterlegten Gmail-Accounts wird eine unverschlüsselte Mail mit einer zuvor auf dem Endgerät erstellter Testdatei (Geheim.txt) im Anhang versendet. Dieser Vorgang soll, neben der Kommunikation, einen Datentransfer vom Endgerät zu einer externen Quelle simulieren. Nach dem erfolgreichen Versenden der E-Mail wird Thunderbird ordnungsgemäß beendet.

2.2.3 Telegram Portable

Vorbereitung

„Es ist oft sehr schwer, die Personen zu identifizieren." [22]

Wenn man über Schutz von persönlichen Daten im Zusammenhang mit aktuellen Messenger-Diensten spricht, landet man zwangsläufig beim Messenger-Dienst ‚Telegram'. Die Schwierigkeit Personen zu identifizieren, liegt allerdings nicht in Verbindung mit der besonders starken Verschlüsselung oder mangelnder Speicherung der Daten durch den Anbieter. Vielmehr ist es der fehlende Kooperationswille seitens Telegram, die gespeicherten Daten preiszugeben.[23] Dieses Problem der Sicherheitsbehörden nutzen viele Kriminelle und verwenden den Messenger-Dienst, um sich dort vermeintlich sicher auszutauschen.

---

22 https://www.wiwo.de/politik/ausland/staatsanwalt-ueber-umstrittenen-messengerdienst-aus-unserer-sicht-spricht-sehr-viel-dagegen-telegram-abzuschalten/28052446.html

23 https://www.wiwo.de/politik/ausland/staatsanwalt-ueber-umstrittenen-messengerdienst-aus-unserer-sicht-spricht-sehr-viel-dagegen-telegram-abzuschalten/28052446.html

Die Kombination dieser beiden Aspekte führt zu der Entscheidung, diese App als Portable-Version in das Testszenario einzubinden. Damit soll überprüft werden, ob der anti-forensische Gedanke bereits am Endgerät umsetzbar ist und man bereits vor dem Transfer der Inhaltsdaten auf die Telegram-Server die Forensiker beziehungsweise Analysten vor Schwierigkeiten stellt.

Ausführung

Bereits beim Download der Installationsdatei wird unter „App Notes“ ein Hinweis angezeigt, dass Telegram standardmäßig die hinterlegten Account-Informationen auf der lokalen Maschine hinterlegt und diese auch nach dem Beenden dort belässt. Weiterhin werden die notwendigen Vorkehrungen dargestellt, damit diese Informationen auch nach der Beendigung der App gelöscht werden. Dieser Hinweis erscheint ebenfalls, nachdem man die Telegram-App auf dem Endgerät startet.[24]

Der Login läuft standardisiert, wie auch bei der normalen Desktop-Version, ab. Es wird ein mobiles Endgerät benötigt, auf dem die Telegram-App bereits verwendet wird, um sich über ein QR-Code-Scan anmelden zu können.

Nach erfolgreich durchgeführter Anmeldung wird eine Nachricht sowie die Datei „Geheim.txt“ an eine in der Kontaktliste befindliche Person versendet und die Antwort abgewartet. Nachdem das „Gespräch“ beendet ist, wird die unter „App Notes“ vorgeschlagene Vorgehensweise zur Löschung der hinterlegten Account-Informationen auf dem Endgerät angewendet. Bereits beim ersten in der Anleitung dargestellten Schritt wird ersichtlich, dass es auf diese Art und Weise nicht umsetzbar ist. Nach Prüfung aller möglicher Einstellungen konnte die Option „Temp folder, cleared on logout“ nicht festgestellt werden. Aus diesem Grund erfolgt die ordnungsgemäße Abmeldung aus der App ohne die empfohlene Maßnahme.

---

[24] Anhang Telegram Hinweis

2.3 Forensische Analyse des verwendeten Endgeräts

Die Möglichkeiten eine IT-forensische Analyse unter Zunahme von Tools durchzuführen erweitern sich stetig, da das Grundgerüst der meisten Tools auf Open-Source Codes in einer Linux-Umgebung basiert. Bei Eingabe des Suchbegriffs *„wie viele tools für forensische analyse gibt es“* über die Google-Suche kommt man beim Aufrufen der ersten URL bereits zu einer Auflistung von 22 kostenlosen Untersuchungstools.[25] Hinzu kommen unzählige kommerzielle Tools, die die forensische Analyse erleichtern sollen.

In diesem Testszenario wird, neben der Anwendung einiger Open-Source-Tools, auch die Möglichkeit aufgezeigt, dass die forensische Analyse durchaus manuell durchgeführt werden kann. Der Nachteil einer manuellen Durchsicht liegt vor allem im zeitlichen Mehraufwand gegenüber automatisierter Analyse mit entsprechenden Tools. Zwar ist diese Option gegebenenfalls genauso zielführend, allerdings, vor allem bei Live-Forensik, weniger effizient.

2.3.1 Manuelle Durchsicht

<u>Gerätemanager</u>

Zu Beginn der forensischen Analyse wird eine einfache Durchsicht des Gerätemanagers nach verwendeten externen Geräten vorgenommen. Standardmäßig zeigt der Windows-Gerätemanager immer die aktuell angeschlossenen Peripherie-Geräte und extern über USB angeschlossenen Datenträger an. Damit auch die nicht mehr angeschlossenen Geräte angezeigt werden, bedarf es einer Änderung in den erweiterten Systemeigenschaften.[26] Bei den Umgebungsvariablen muss dafür unter den Systemvariablen der folgende Eintrag hinzugefügt werden:

---

[25] https://geekflare.com/de/forensic-investigation-tools/

[26] Anhang Umgebungsvariable

Bild 2: Umgebungsvariable

Sobald die Änderung vom System übernommen wurde, kann man unter dem Reiter „Ansicht“ des Gerätemanagers die Option „Ausgeblendete Geräte anzeigen“ auswählen und bekommt gegebenenfalls Geräte angezeigt, die nicht mehr angeschlossen sind.

In diesem Fall kann ein nicht mehr angeschlossenes „USB-Massenspeichergerät“ in der Auflistung festgestellt werden. Bei der Betrachtung der Eigenschaften des Geräts können Zeitstempel und die PID einer versuchten Migration festgestellt werden:

Bild 3: Zeitstempel und PID

Anhand der alleinigen Erkenntnis, dass ein USB-Stick zum Zeitpunkt X an das Endgerät angeschlossen war, lässt sich keine Schlussfolgerung hinsichtlich des Einsatzzwecks erörtern. Hierbei handelt es sich in erster Linie um ein Indiz, dass

es einen unbefugten Zugriff auf das Endgerät gegeben haben könnte. Gegebenenfalls ist diese Erkenntnis bei weitergehender Analyse verwertbar.

Activities Cache

Aufgrund dessen, dass die Aktivitäten-Verfolgung im Vorfeld deaktiviert wurde, können keine Einträge in der ActivitiesCache-Datenbank festgestellt werden.
Um die potenziellen forensischen Erkenntnisse aufzuzeigen, wird die Aktivitäten-Verfolgung eingeschaltet und der Testdurchlauf erneut durchgeführt. Durch die aktivierte Protokollierung kann unter dem Pfad

C:\Users\Hackerman\AppData\Local\ConnectedDevicesPlatform\L.PortableApps\

die von Windows automatisch erstellte Datenbank-Datei ‚ActivitiesCache.db' festgestellt werden. Diese wird mit der Software „Database Browser"[27] geöffnet und mit der Suchfunktion nach den verwendeten PortableApps recherchiert. Insgesamt können dabei mehrere Einträge festgestellt werden, die auf den Einsatz von ‚PortableApp' zurückzuführen sind:

- ➔ Insgesamt 71 Einträge „telegramdesktopportable"

Bild 4: Telegram – ActivitiesCache

- ➔ Insgesamt 38 Einträge „thunderbirdportable"

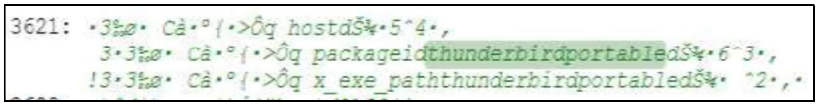


Bild 5: Thunderbird – ActivitiesCache

[27] https://portableapps.com/apps/development/database_browser_portable

➔ Insgesamt 132 Einträge „PortableApps.com“

Bild 6: PortableApp.com – ActivitiesCache

Eine genaue Betrachtung der Einträge findet hierbei nicht statt, da die Aktivitäten-Verfolgung aktiv für das Testszenario abgeschaltet wurde. Dies soll lediglich aufzeigen, dass eine reine unbemerkte Nutzung von Software ohne aktiven Eingriff in die Systemeinstellungen nicht möglich wäre.

Registry-Editor

Über den Registry Editor[28] können unter HKEY_CURRENT_USER\SOFTWARE\ beide Programme festgestellt werden.[29] Während man über den Telegram-Ordner keine weiterführenden Informationen erhält, so dass nicht eindeutig verifiziert werden kann, ob die Datei lokal oder von einem externen Medium ausgeführt wurde, kann beim Eintrag zu Thunderbird der komplette Pfad der ausgeführten EXE-Datei festgestellt werden:

Name	Typ	Daten
(Standard)	REG_SZ	(Wert nicht festgelegt)
E:\PortableApps\ThunderbirdPortable\App\Thunderbird64\thunderbird.exe|Telemetry	REG_DWORD	0x00000001 (1)

Bild 7: Registry-Dateipfad Thunderbird

TelegramDesktop

Name	Typ	Daten
(Standard)	REG_SZ	(Wert nicht festgelegt)

Bild 8: Registry-Eintrag Telegram

Hierbei fällt auf, dass die Thunderbird-App über den PortableApps-Launcher

---

[28] Anhang Registry Editor

[29] Anhang Registry Einträge PortableApps

ausgeführt wurde und dies der Grund dafür sein könnte, dass die Darstellung des Ausführungspfades anders als bei Telegram ist.

2.3.2 MUICacheView

Funktionsweise

Jedes Mal, wenn ein Programm auf einem Windows-System gestartet wird, wird aus dem zugehörigen EXE-File der Name extrahiert und im Registrykey ‚MuiCache' hinterlegt.

Mit dem Tool ‚MUICacheView' ist es möglich, diese Einträge vereinfacht in einer GUI einzusehen und gegebenenfalls zu bearbeiten/löschen. ‚MUICacheView' kann ohne Installation und ohne zusätzlichen DLLs, als EXE-File ausgeführt werden.[30] Somit wäre dieses Tool auch als antiforensische Software einsetzbar, was in dem Fall allerdings nicht berücksichtigt wird und sie lediglich zur Analyse von eingesetzter Software dienen soll.

Einsatz

Bei der Überprüfung des ‚MuiCache' können keine der über die PortableApps-Software gestarteten Programme festgestellt werden.[31]

2.3.3 Wireshark

Bei der Open Source Software Wireshark handelt es sich um eines der bekanntesten Live-Forensik Analysetools. Mithilfe dieser Software kann der Netzwerkverkehr auf der Basis von Datenprotokollen überwacht und analysiert

---

[30] Anhang ‚MUICacheView.chm' (HTML-Hilfedatei)'

[31] Anhang Auflistung Programme

werden.[32]

Im Gegensatz zu den anderen in diesem Testszenario angewendeten Methoden muss der Netzwerkmitschnitt vor dem Benutzen der PortableApps gestartet werden, um den Datenverkehr aufnehmen zu können. Um eine umfangreiche Analyse durchführen zu können, werden zwei unterschiedliche Aufnahmen gefertigt.

Zuerst wird das Addon „USBPcap“ ausgeführt, um alle neuen Aktivitäten an den USB-Schnittstellen des Endgeräts überwachen zu können.[33] Um die Datenmenge im USBPcap-Stream zu reduzieren, wird vor dem Start der Aufnahme die Einstellung „Capture from newly connected devices“ anstatt von „all“ vorgenommen.

Unmittelbar nach Anschluss des USB-Sticks können in der Wireshark-GUI diverse mitgeschnittene Datenpakete festgestellt werden,[34] woraufhin die Aufnahme wieder angehalten wird und der USB-Stick kurzzeitig wieder entfernt, damit eine neue Aufnahme gestartet werden kann.

Kurz bevor der USB-Stick erneut angeschlossen wird, wird die Netzwerküberwachung auf die WLAN-Schnittstelle des Endgeräts eingestellt und gestartet. Nach Beendigung des Einsatzes von PortableApps wird die Überwachung ausgeschaltet und die entstandenen Netzwerkmitschnitte analysiert.

---

[32] https://de.wikipedia.org/wiki/Wireshark

[33] Anhang Start Capture USB

[34] Anhang USB Datenpakete GUI

Analyse USBPcap-Mitschnitt

In der durch Wireshark erstellter USBPcap-Datei „Mitschnitt USB-Anschluss.pcapng“ kann ein „Transcend 16GB“ Gerät festgestellt werden, welches als „Removable“ markiert ist und somit als ein externes Speichermedium identifiziert werden kann.

```
SCSI Payload (Inquiry Response Data)
    [LUN: 0x0000]
    [Command Set:Direct Access Device (0x00) ]
    [SBC Opcode: Inquiry (0x12)]
    [Request in: 21]
    [Response in: 26]
  > Peripheral: 0x00, Qualifier: Device type is connected to logical unit, Device T
  > Inquiry RMB Flags: 0x80, Removable
    Version: Compliance to SPC-4 (0x06)
  > Inquiry ACA Flags: 0x02, Response Data Format: SPC-2/SPC-3/SPC-4
    Additional Length: 31
  > Inquiry SCCS Flags: 0x73, ACC, TPGS: Both Implicit and Explicit LU Access suppo
  > Inquiry BQue Flags: 0x6d, EncServ
  > Inquiry RelAdr Flags: 0x69
    Vendor Id: JetFlash
    Product Id: Transcend 16GB
    Product Revision Level: 1100
```

Bild 9: USBPcap Transcend 16GB

Anhand des USBPcap-Mitschnitts lässt sich keine Zuordnung zu einem Laufwerksbuchstaben herstellen. Allerdings kann diese Erkenntnis mit dem Ergebnis der Durchsicht des Gerätemanagers (siehe *‚2.3.1 Manuelle Einsicht‘*) in Verbindung gebracht werden, bei der keine eindeutige Identifizierung des USB-Massenspeichergeräts stattfinden konnte.

Analyse Netzwerkmitschnitt

Aufgrund dessen, dass ein Netzwerk-Mitschnitt über Wireshark sehr detailliert und umfangreich ist, werden für dessen Analyse spezielle Filter angewendet. Als erstes wird explizit nach den SMTP-Standardportnummern 25[35] und 465[36]

[35] Smtp-Port für unverschlüsselten Postausgang

[36] Smtp-Port bei SSL-Verschlüsselung

gefiltert, um einen möglichen Mailversand feststellen zu können:

tcp.port == 25 || tcp.port == 465 (zu lesen: zeige alle Ergebnisse mit TCP-Port 25 oder TCP-Port 465)

Hierbei kann eine Kommunikation zwischen dem Client[37] und einem Server über den Port 465 festgestellt werden. Bei einer genaueren Betrachtung des TCP-Streams kann ein Hinweis auf die Verwendung von einem Gmail-Server in Klartext festgestellt werden:

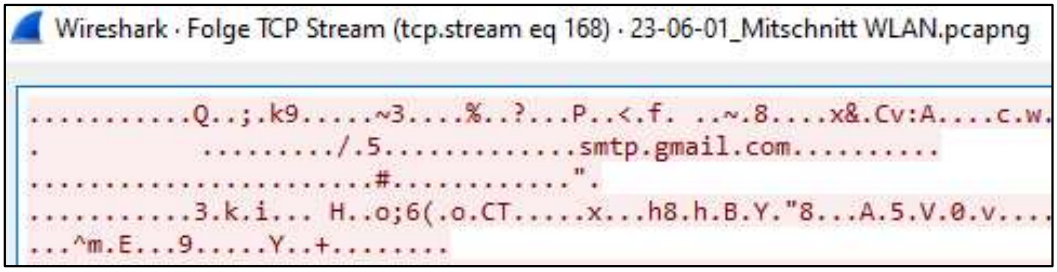


Bild 10: Gmail-Server

Bei der in diesem TCP-Stream als Server-IP hinterlegten IPv6-Adresse handelt es sich um eine von ‚Google Ireland Limited' registrierten Adressbereich, so dass man aufgrund dieser Feststellung von einem stattgefundenen Mailversand über die WLAN-Schnittstelle des Hosts ausgegangen werden kann.

Im Fall von Telegram lässt sich eine Filterung nicht eindeutig festlegen, da keine konkrete Angabe der genutzten Ports seitens Telegram vorliegt und gegebenenfalls Standard HTTP/S-Ports verwendet werden.[38] Aus diesem Grund wird eine Filterung, die sich auf die IP-Adresse der WLAN-Schnittstelle beschränkt, vorgenommen:

---

[37] IPv6 Adresse aus WLAN-Spezifikationen bekannt

[38] https://core.telegram.org/mtproto/transports

ip.addr == 192.168.0.8 (zu lesen: alle Einträge mit IP-Adresse 192.168.0.8)

Hierbei können mehrere Einträge von Kommunikation zwischen dem Host und verschiedener IP-Adressen aus dem augenscheinlich gleichem IP-Range, wie beispielsweise 149.154.167.50 oder 149.154.167.51,[39] festgestellt werden. Eine Überprüfung einer der IP-Adressen über WHOIS ergab, dass es sich um eine von „Telegram_Messenger_Network“ registrierte IP-Range handelt.[40]

2.3.4 RAM-Dump

Erstellung RAM-Dump

Die Erstellung eines Abbilds des physischen Speichers erfolgt über das Tool „WinPmem“.[41] Um die EXE-Datei „winpmem_mini_x64_rc2.exe“ unter Windows ausführen zu können, bedarf es gegebenenfalls einer Änderung in der „Windows Execution Policy“. Bei den „Execution Policies“ handelt es sich um Ausführungsrichtlinien, die bestimmen, ob man Konfigurationsdateien laden oder Skripte ausführen kann.[42] Nach Überprüfung der aktueller Ausführungsrichtlinie kann festgestellt werden, dass die Option „unrestricted“ gesetzt werden muss. Diese Änderung muss mit Administrator-Rechten über die PowerShell vorgenommen werden:

---

[39] Anhang IP Datenpakete GUI

[40] Anhang WHOIS Abfrage

[41] https://github.com/Velocidex/WinPmem

[42] https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.security/set-executionpolicy?view=powershell-7.3

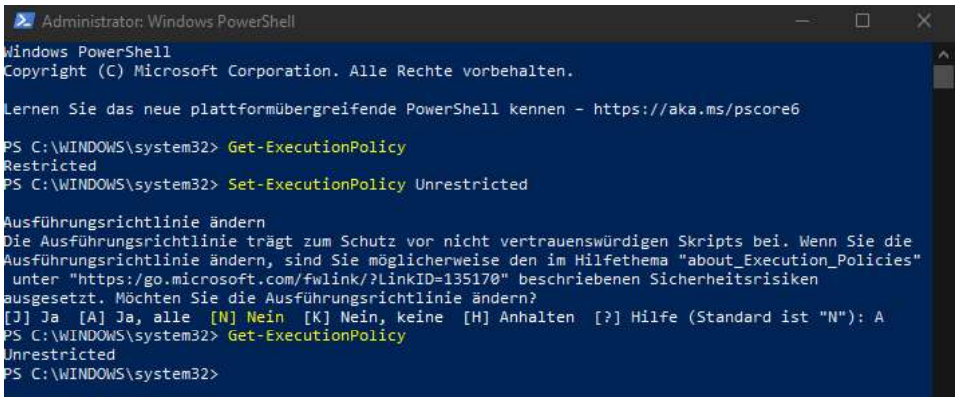


Bild 11: ExecutionPolicy

Nachdem die Änderung aktiv ist, wird die Kommandozeile als Administrator ausgeführt und mit dem Befehl

winpmem_mini_x64_rc2.exe RAM-Dump.raw

eine Image-Datei des physikalischen Speichers im RAW-Format erstellt.[43]

Analyse RAM-Dump

Die darauffolgende Analyse des Speicherabbilds erfolgt über das Analyse-Tool Volatility3.[44] Aufgrund der besseren Kompatibilität der Volatility-Software mit einer Linux-Umgebung, wird eine Linux-VM mit „Linux Mint 19.1 Tessa; 4.15.0-208-generic“ für die Analyse verwendet.[45]

Von den insgesamt 42 zur Verfügung stehenden Analyse-Optionen für einen Windows RAM-Dump, werden die Module

---

[43] Anhang Memory Dump

[44] https://www.volatilityfoundation.org/releases-vol3

[45] Anhang VM-Konfiguration

- windows.pstree.PsTree → Plugin for listing processes in a tree based on their parent process ID

  und

- windows.sessions.Sessions lists → Processes with Session information extracted from Environmental Variables

verwendet.[46]

Pstree (Prozessbaum)

Zur Erstellung des Pstree aus dem vorliegenden RAM-Dump mit der Ausgabe des Ergebnisses in eine Text-Datei wird der folgende Befehl verwendet:

python3.8 vol.py -f /media/sf_4n6/RAM-Dump.raw windows.pstree.PsTree >> /media/sf_4n6/pstree.txt[47]

In der erstellten Ausgabe lässt sie die Ausführung von der ‚PortableApps' Software wie folgt erkennen:

```
Volatility 3 Framework 2.4.2

PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId

****** 3460     8184    Start.exe       0x9c0905554080  0       -       1
******* 14256   3460    PortableAppsPl  0x9c090b3f3080  0       -       1
******** 11088  14256   DontSleepPorta  0x9c090574e080  5       -       1
********* 8900  11088   DontSleep_x64_  0x9c09054d5080  8       -       1
```

Bild 12: Pstree PortableApps

46 Anhang Volatility3 Manpage – Windows Befehle

47 Anhang Ausgabe Pstree

Lediglich das verwendete Tool „Don't Sleep“ wird unter den Prozessen aufgeführt. Auch wenn eine Ausführung der Programme ‚Thunderbird‘ und ‚Telegram‘ nicht erkennbar ist, können Rückschlüsse auf eine Verwendung dieser im Zusammenhang mit den unter Punkt *‚2.3.1 Manuelle Durchsicht‘* festgestellten Registry Einträgen gezogen werden.

Sessions

Zur Erstellung der Sessions-Auflistung aus dem vorliegenden RAM-Dump mit der Ausgabe des Ergebnisses in eine Text-Datei wird der folgende Befehl verwendet:

python3.8 vol.py -f /media/sf_4n6/RAM-Dump.raw windows.sessions.Sessions >> /media/sf_4n6/sessions.txt[48]

Aus der daraus entstandenen Auflistung der Sessions kann festgestellt werden, dass die Ausführung der PortableApps über den Account des Windows-Users „Hackermann“ stattgefunden hat:

```
Volatility 3 Framework 2.4.2

Session ID      Session Type    Process ID      Process User

1       -       3460    Start.exe       -
1       -       14256   PortableAppsPl  -
1       -       6908    HPSF.exe        -
1       Console 11088   DontSleepPorta  KLPC118/Hackermann
1       Console 8900    DontSleep_x64_  KLPC118/Hackermann
```

Bild 13: Sessions

48 Anhang Ausgabe Sessions

3 Zusammenfassung

3.1 Fazit

In der Projektarbeit sollte die Eignung der Software ‚PortableApps.com Platform™' als anti-forensische Maßnahme untersucht werden. Hierzu wurde ein Testszenario produziert, in dem die Portable-Versions von den Programmen ‚Thunderbird', ‚Telegram' und ‚Don't sleep' auf einem Windows-Host ausgeführt wurden.

Bei der darauffolgenden forensischen Untersuchung, die aus Kombination von manueller Durchsicht und automatisierte Sammlung von Datenspuren mittels entsprechender Analysetools bestand, konnten einige Hinweise/Belege für die Nutzung der Software-Suite ‚PortableApps.com Platform™' festgestellt werden. Die einzelnen Datenspuren können wie folgt aufgegliedert werden.

Zu der App ‚Thunderbird' konnten Registry-Einträge festgestellt werden, die einen Pfad beinhalten, in welchem die App ausgeführt wurde. Zusammen mit den Erkenntnissen aus der manuellen Durchsicht und der Analyse des Wireshark-Mitschnitts von USBPcap kann mit an Sicherheit grenzender Wahrscheinlichkeit von einer Nutzung der App ‚Thunderbird' über ein externes Speichermedium (USB-Stick) ausgegangen werden. Darüber hinaus konnten im Wireshark-Mitschnitt der WLAN-Schnittstelle Verbindungen mit dem SMTP-Server von Google (smtp.gmail.com) über Port 465 festgestellt werden. Damit kann nachgewiesen werden, dass ein Mailversand über ein Gmail-Konto stattgefunden hat.

Für die App ‚Telegram' konnte keine eindeutige Zuordnung zu einer Nutzung über ein externes Medium stattfinden. In den Registry-Einträgen kann lediglich ein Eintrag für „TelegramDektop", ohne den dazugehörigen Pfad, festgestellt werden. Des Weiteren wurde eine Netzwerkkommunikation mit mehreren IP-Adressen aus dem IP-Range von „Telegram_Messenger_Network" festgestellt, was ein weiteres Indiz für die Nutzung von Telegram-Messenger ist.

Die größte Informationsdichte lag bei der Portable-App „Don't sleep‘ vor. Anhand der zurückgelassenen Datenspuren im RAM-Dump konnte der Einsatz der ‚PortableApps.com Platform™‘ eindeutig nachgewiesen werden.

Der maßgebliche Unterschied der Datenspurenmenge sowie -qualität kann eventuell auf die unterschiedlichen Arten des Programmstarts (Launcher und EXE-File) zurückgeführt werden. Um eine eindeutige Bewertung erstellen zu können, bedarf es weiterer Tests mit gegebenenfalls weiteren Softwareprodukten aus der PortableApps-Umgebung.

Des Weiteren gilt die in diesem Testszenario verwendete Ausführung des Wireshark-Mitschnitts als eher unwahrscheinlich, da der Hacker dies am Endgerät bemerken würde. Aus diesem Grund ist die Rückverfolgung der Telegram-Kommunikation nur in diesem Testszenario relevant und kann gegebenenfalls nicht auf eine reelle Situation simultan übertragen werden. Es kann allerdings nicht ausgeschlossen werden, dass eine Netzwerküberwachung beispielsweise auf dem Standardgateway (Router) stattfindet und man ebenfalls an die IP-Protokolldaten rankommen kann. Bei einer über dem Gateway stattfindenden Netzweküberwachung wäre die Ausführung von USBPcap also ebenfalls nicht möglich und man hätte keine detaillierten Erkenntnisse über die Begebenheiten des eingesetzten USB-Sticks.

Aufgrund der forensischen Auswerteergebnisse kann die Eignung von ‚PortableApps.com Platform™‘ als reines, nur auf die Software-Suite selbst beruhendes, anti-forensisches Mittel nicht bestätigt werden.

3.2 Ausblick

Im vorliegenden Testszenario wurden bewusst keine Tools eingesetzt, die geeignet wären, aktive Anti-Forensik zu betreiben. Trotz der eindeutigen Erkenntnisse hinsichtlich der Nutzung von PortableApps, kann unter Hinzunahme solcher Tools der Wirkungsgrad der angewendeten anti-forensischen Maßnahmen erweitert werden. In der Bibliothek der ‚PortableApps.com Platform™‘ können solche Tools problemlos aus dem

Bereich „Utilities“ in der Software-Suite installiert und genutzt werden.

Des Weiteren konnten Unterschiede in der Art sowie in der Menge der zurückgelassenen Datenspuren der unterschiedlichen Apps festgestellt werden. Darauf aufbauend und nach Prüfung weiterer Apps kann die anti-forensische Methode vom Legen falscher Spuren ausgenutzt werden. Im vorliegenden Fall wäre die App ‚Don’t sleep‘ dafür geeignet, von den eigentlichen Tätigkeiten abzulenken, weil sie eindeutige Spuren im RAM-Dump hinterlassen hat.

Auch wenn die Software-Suite ‚PortableApps.com Platform™‘ nicht als reine anti-forensische Maßnahme geeignet ist, bietet sie ein gutes Grundgerüst, auf dem man diese Maßnahmen aufbauen und effizienter einsetzen kann.

4 Literaturverzeichnis

Auf digitaler Spurensuche mithilfe von IT-Forensik (2018). In *COM-Professional*, 11/20/2018. Available online at https://www.com-magazin.de/praxis/sicherheit/digitaler-spurensuche-mithilfe-it-forensik-1625707.html?page=3_anti-forensiker-vs.-forensiker, checked on 6/14/2023.

Auf digitaler Spurensuche mithilfe von IT-Forensik (2018). In *COM-Professional*, 11/20/2018. Available online at https://www.com-magazin.de/praxis/sicherheit/digitaler-spurensuche-mithilfe-it-forensik-1625707.html?page=1_post-mortem-vs.-live-analyse, checked on 6/14/2023.

Auf digitaler Spurensuche mithilfe von IT-Forensik (2018). In *COM-Professional*, 11/20/2018. Available online at https://www.com-magazin.de/praxis/sicherheit/digitaler-spurensuche-mithilfe-it-forensik-1625707.html?page=2_live-ist-king, checked on 6/14/2023.

Helfen Sie mit, Thunderbird am Leben zu erhalten! — Thunderbird (2023). Available online at https://www.thunderbird.net/de/thunderbird/102.0/eoy/, updated on 5/18/2023, checked on 6/16/2023.

Transports (2023). Available online at https://core.telegram.org/mtproto/transports, updated on 6/16/2023, checked on 6/16/2023.

Baxter, Daryl (2022): Best portable apps of 2023. In *TechRadar pro*, 7/1/2022. Available online at https://www.techradar.com/news/the-best-portable-apps, checked on 6/14/2023.

BSI (2021): Leitfaden IT-Forensik. Edited by BSI. Available online at https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2022/05_DER_Detektion_und_Reaktion/DER_2_2_Vorsorge_fuer_die_IT_Forensik_2022.pdf?__blob=publicationFile&v=3, checked on 6/14/2023.

Conlan, Kevin; Baggili, Ibrahim; Breitinger, Frank (2016): Anti-forensics: Furthering digital forensic science through a new extended, granular taxonomy. In *Digital Investigation* 18, S66-S75. DOI: 10.1016/j.diin.2016.04.006.

GitHub (2023): GitHub - Velocidex/WinPmem: The multi-platform memory acquisition tool. Available online at https://github.com/Velocidex/WinPmem, updated on 6/16/2023, checked on 6/16/2023.

Harris, Ryan (2006): Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem. In *Digital Investigation* 3, pp. 44–49. DOI: 10.1016/j.diin.2006.06.005.

Haseborg, Volker ter (2022): Telegram: Warum die Jagd auf Telegram-Kriminelle so schwer ist. In *Wirtschaftswoche*, 12/2/2022. Available online at https://www.wiwo.de/politik/ausland/staatsanwalt-ueber-umstrittenen-messengerdienst-aus-unserer-sicht-spricht-sehr-viel-dagegen-telegram-abzuschalten/28052446.html, checked on 6/14/2023.

Kumar, Chandan (2016): 22 KOSTENLOSE forensische Untersuchungstools für IT-Sicherheitsexperten. In *Geekflare*, 4/9/2016. Available online at https://geekflare.com/de/forensic-investigation-tools/, checked on 6/14/2023.

PortableApps.com - Portable software for USB, portable, and cloud drives (2023): Database Browser Portable (database management) | PortableApps.com. Available online at https://portableapps.com/apps/development/database_browser_portable, updated on 6/16/2023, checked on 6/16/2023.

PortableApps.com - Portable software for USB, portable, and cloud drives (2023): Mozilla Thunderbird Portable (email) | PortableApps.com. Available online at https://portableapps.com/apps/internet/thunderbird_portable, updated on 6/16/2023, checked on 6/16/2023.

PortableApps.com - Portable software for USB, portable, and cloud drives (2023): PortableApps.com - Portable software for USB, portable, and cloud drives. Available online at https://portableapps.com/, updated on 6/16/2023, checked on 6/16/2023.

Sdwheeler (2023): Set-ExecutionPolicy (Microsoft.PowerShell.Security) - PowerShell. Available online at https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.security/set-executionpolicy?view=powershell-7.3, updated on 6/16/2023, checked on 6/16/2023.

Studie zu Datenschutz: Deutsche zweifeln an Datensicherheit (2023): Studie zu Datenschutz: Deutsche zweifeln an Datensicherheit. Available online at https://www.sinus-institut.de/media-center/presse/mehrheit-der-deutschen-zweifelt-an-datensicherheit, updated on 6/16/2023, checked on 6/16/2023.

Techzle (2021): This is how you make portable apps yourself - Techzle. Available online at http://techzle.com/this-is-how-you-make-portable-apps-yourself, updated on 6/16/2023, checked on 6/16/2023.

volatilityfoundation (2023): Release Downloads | Volatility Foundation. Available online at https://www.volatilityfoundation.org/releases-vol3, updated on 6/16/2023, checked on 6/16/2023.

Wikipedia (Ed.) (2021): Informationstechnisches System. Available online at https://de.wikipedia.org/w/index.php?title=Informationstechnisches_System&oldid=211433483, updated on 4/29/2021, checked on 6/14/2023.

Wikipedia (Ed.) (2023): Wireshark. Available online at https://de.wikipedia.org/w/index.php?title=Wireshark&oldid=232664766, updated on 10/4/2023, checked on 6/14/2023.

5 Bilderverzeichnis

6 Anlagenverzeichnis und Anhänge

6.1 Anhang Taxonomie

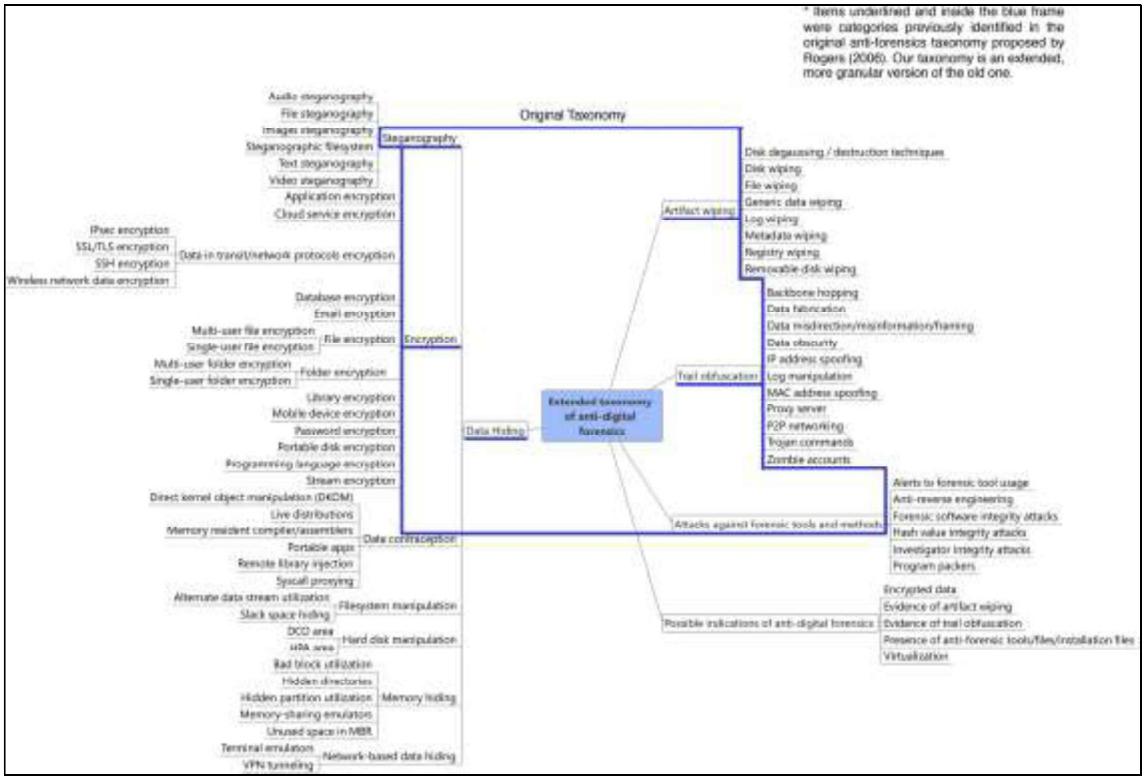


Bild 14 Anti-Forensik Taxonomie

6.2 Anhang PortableApps-Launcher

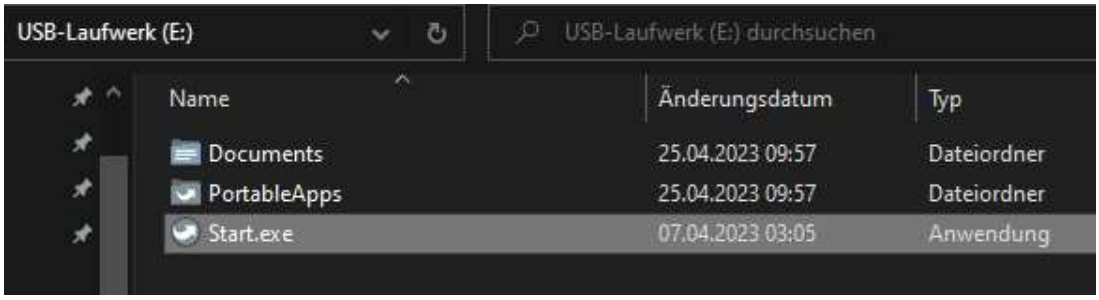


Bild 14 Launcher_0

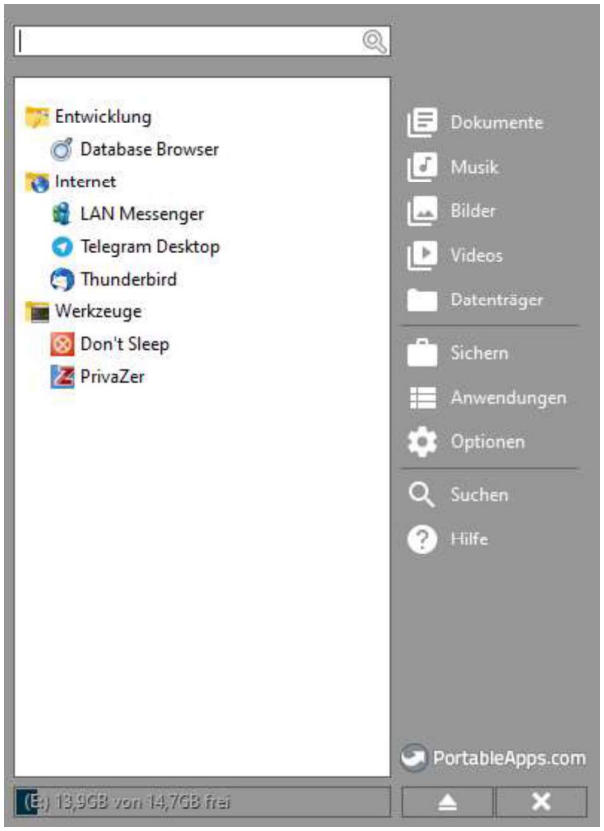


Bild 15 Launcher_1

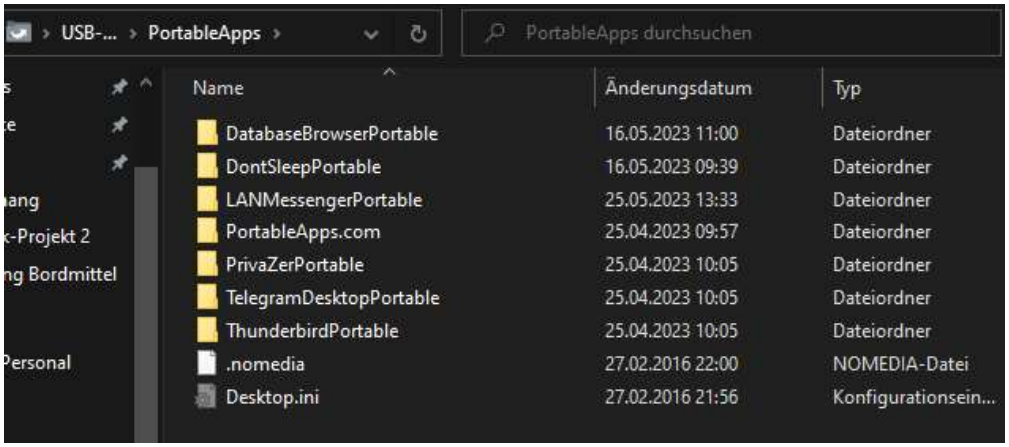


Bild 16 Launcher_2

6.3 Anhang Windows-Spezifikationen

Gerätespezifikationen

HP ProBook 650 G2

Gerätename	
Prozessor	Intel(R) Core(TM) i7-6820HQ CPU @ 2.70GHz 2.71 GHz
Installierter RAM	16,0 GB (15,9 GB verwendbar)
Geräte-ID	
Produkt-ID	
Systemtyp	64-Bit-Betriebssystem, x64-basierter Prozessor
Stift- und Toucheingabe	Für diese Anzeige ist keine Stift- oder Toucheingabe verfügbar.

Kopieren

Diesen PC umbenennen

Windows-Spezifikationen

Edition	Windows 10 Pro
Version	22H2
Installiert am	20.04.2021
Betriebssystembuild	19045.2846
Leistung	Windows Feature Experience Pack 120.2212.4190.0

Kopieren

Bild 17 Laptop

6.4 Anhang TrendMicro „About“

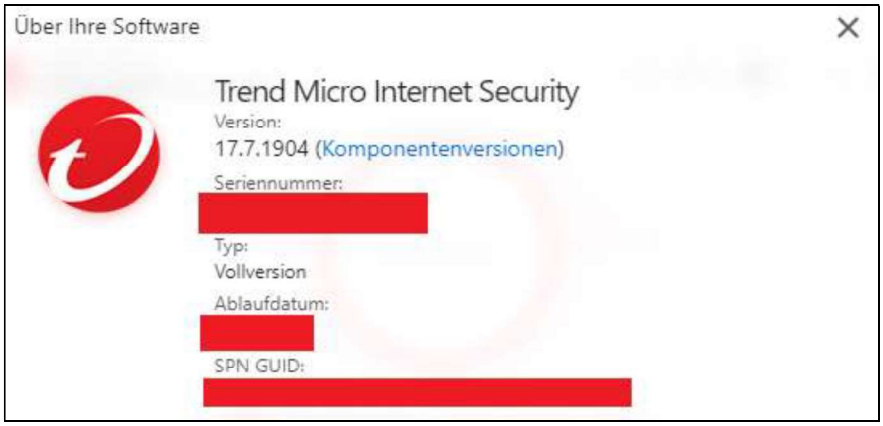
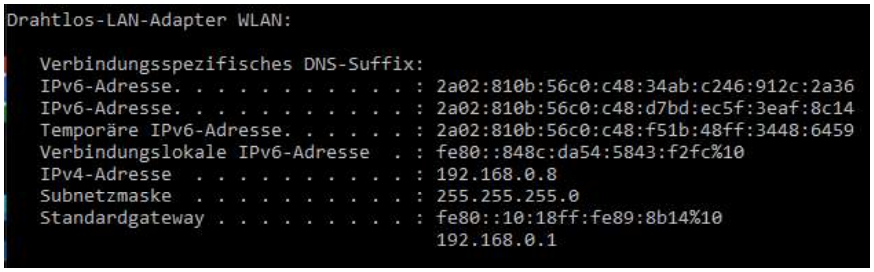


Bild 18 TrendMicro "About"

6.5 Anhang WLAN Spezifikationen

Bild 19 IP-Einstelliungen



```
Drahtlos-LAN-Adapter WLAN:

   Verbindungsspezifisches DNS-Suffix:
   IPv6-Adresse. . . . . . . . . . . : 2a02:810b:56c0:c48:34ab:c246:912c:2a36
   IPv6-Adresse. . . . . . . . . . . : 2a02:810b:56c0:c48:d7bd:ec5f:3eaf:8c14
   Temporäre IPv6-Adresse. . . . . . : 2a02:810b:56c0:c48:f51b:48ff:3448:6459
   Verbindungslokale IPv6-Adresse  . : fe80::848c:da54:5843:f2fc%10
   IPv4-Adresse  . . . . . . . . . . : 192.168.0.8
   Subnetzmaske  . . . . . . . . . . : 255.255.255.0
   Standardgateway . . . . . . . . . : fe80::10:18ff:fe89:8b14%10
                                       192.168.0.1
```

Bild 20 IP-Adresse

6.6 Anhang Installation PortableApps-Suite

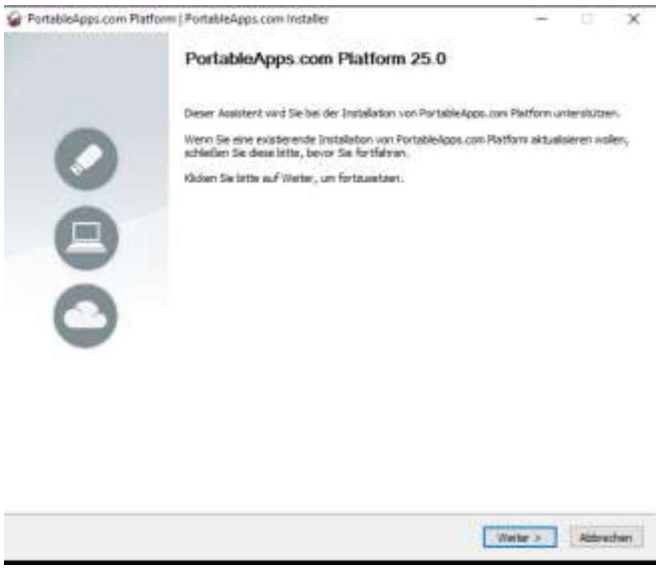


Bild 21 Suite_0

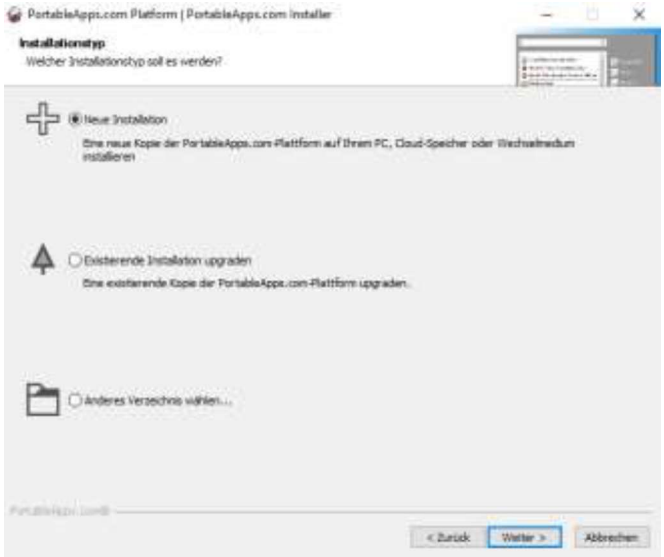


Bild 22 Suite_1

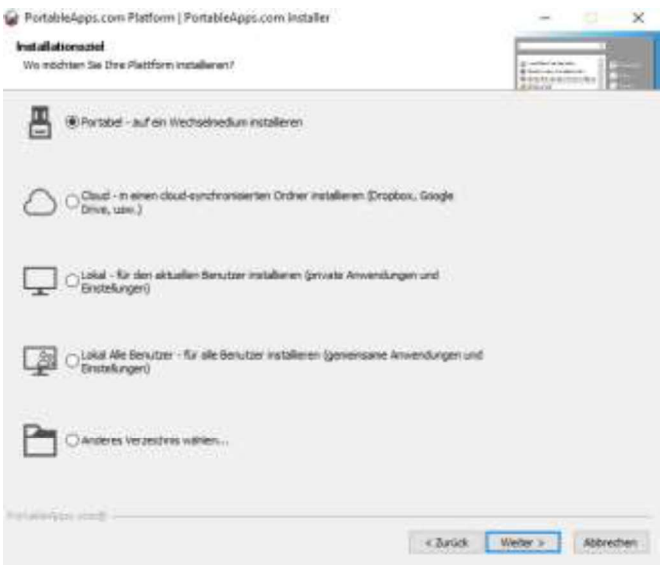


Bild 23 Suite_2

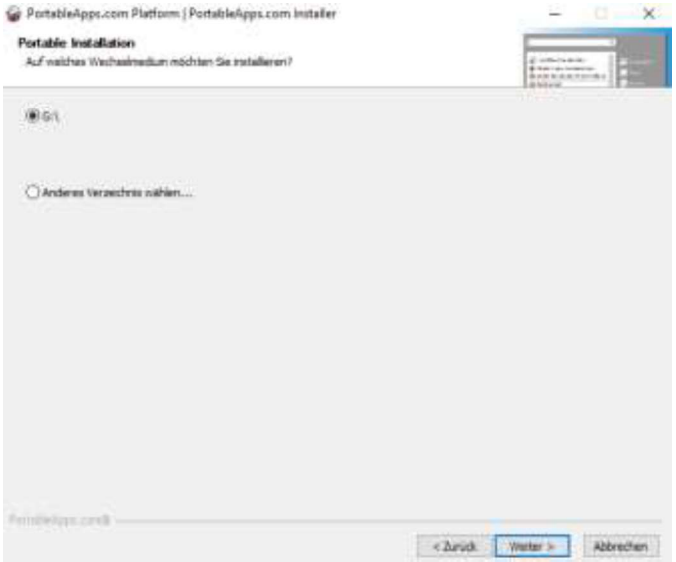


Bild 24: Suite_3

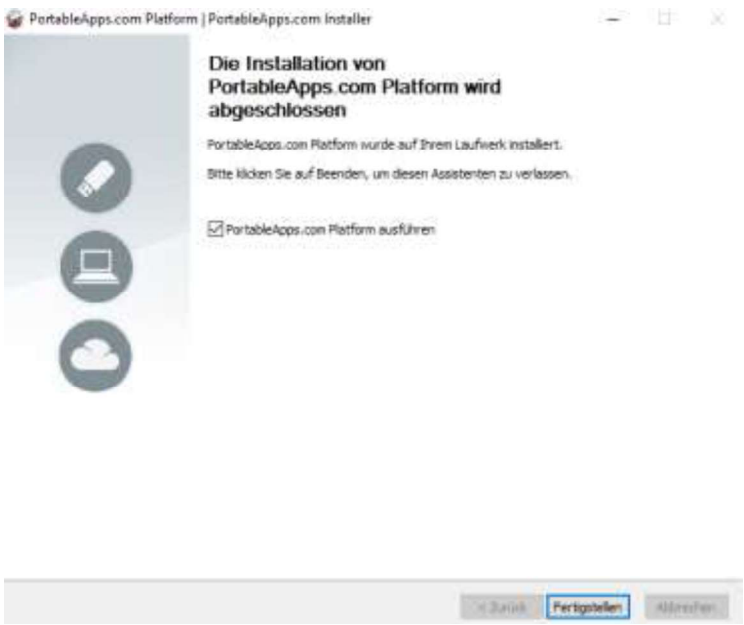


Bild 25 Suite_4

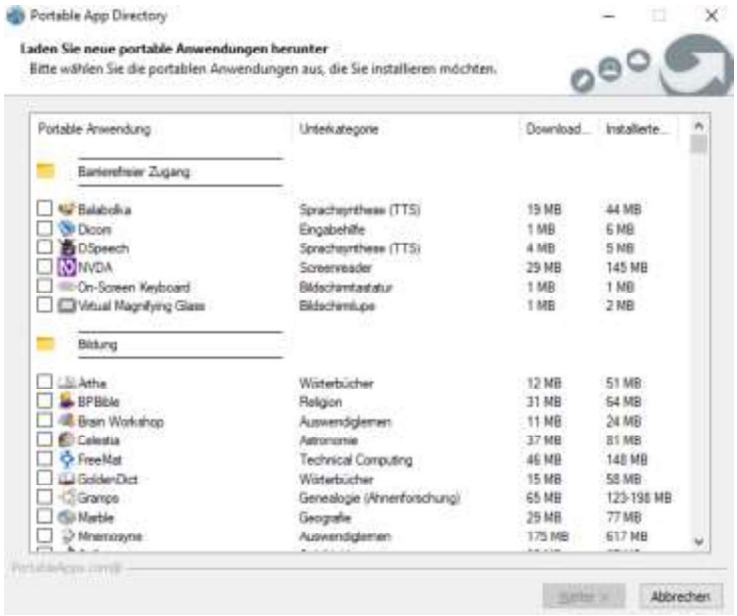


Bild 26 Suite_5

6.7 Anhang Don’t sleep

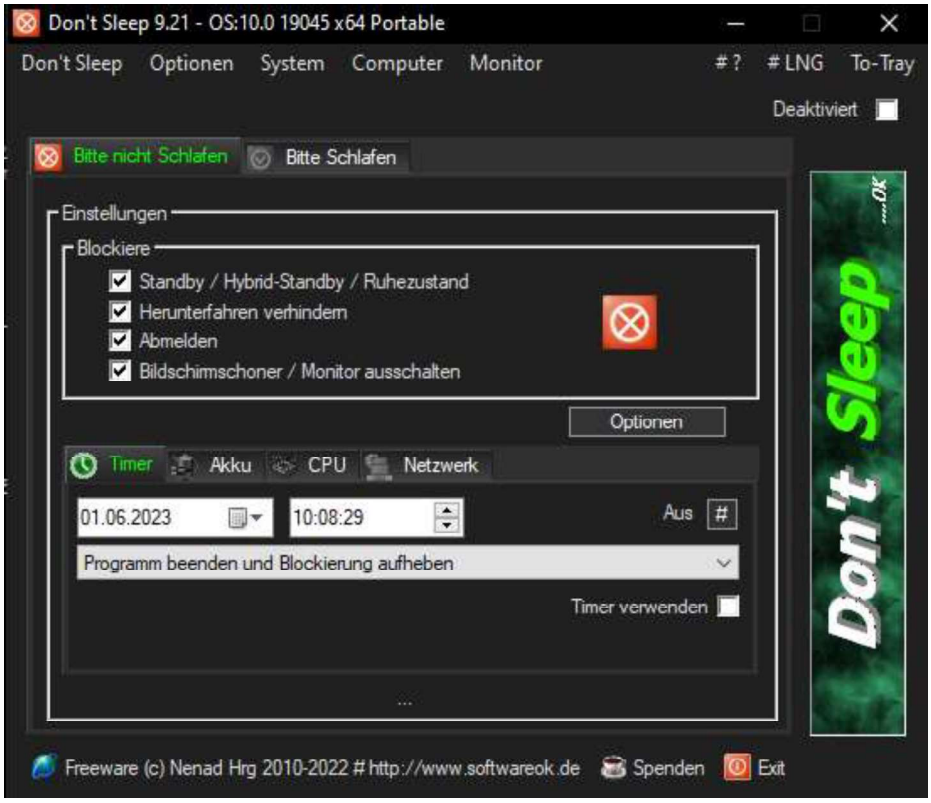


Bild 27 Don't Sleep GUI

6.8 Anhang Telegram Hinweis

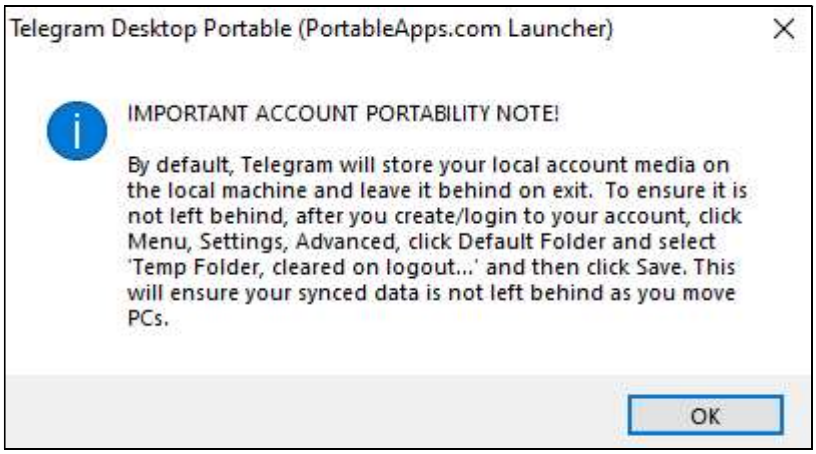


Bild 28 Telegram Hinweis

6.9 Anhang Umgebungsvariable

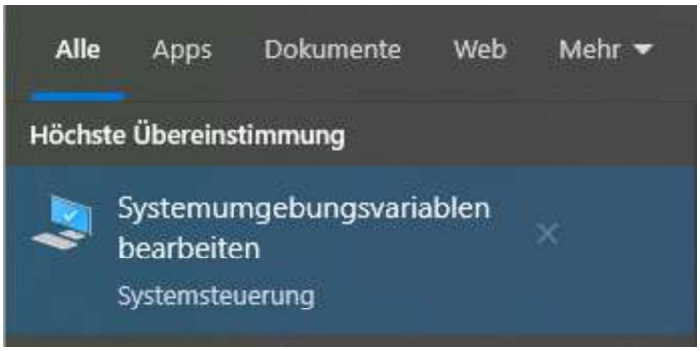


Bild 29 Variable_0

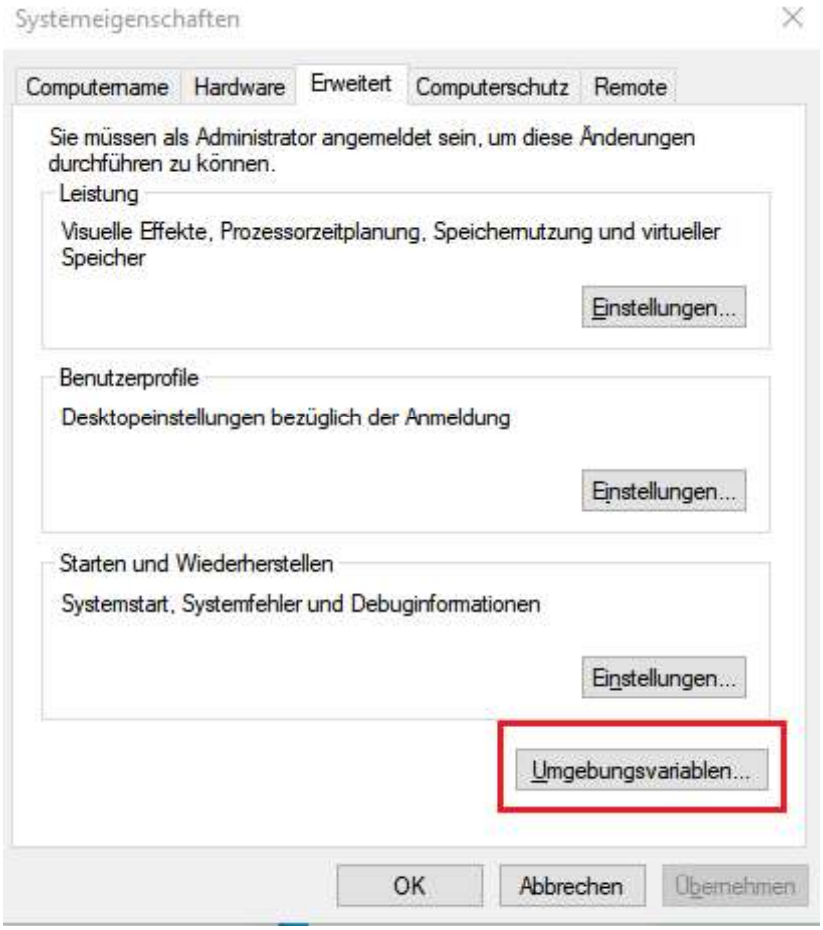


Bild 30 Variable_1

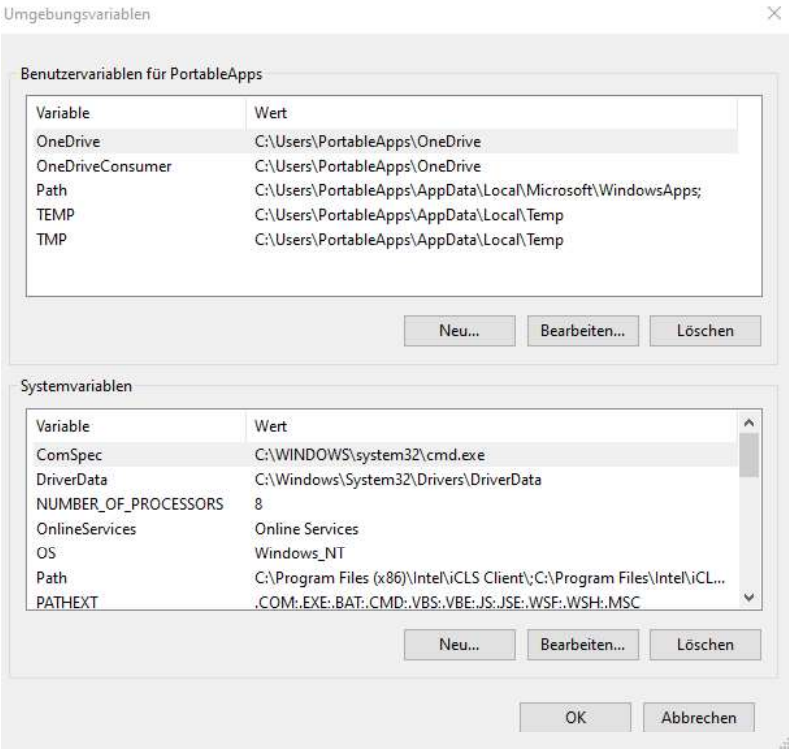


Bild 31 Variable_2

Bild 32 Variable_3

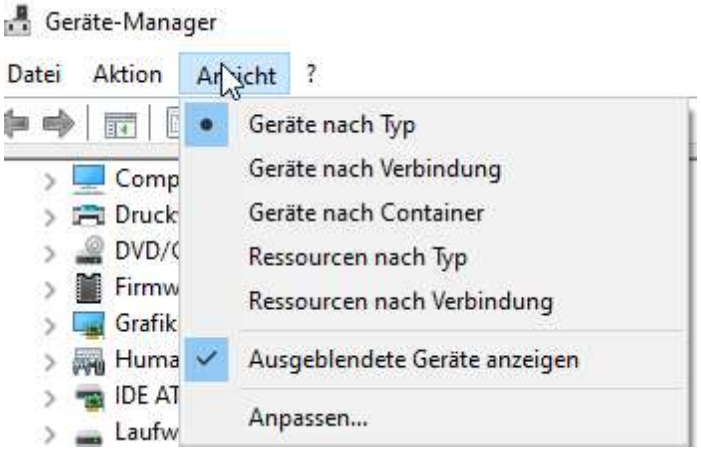


Bild 33 Gerätemanager_0

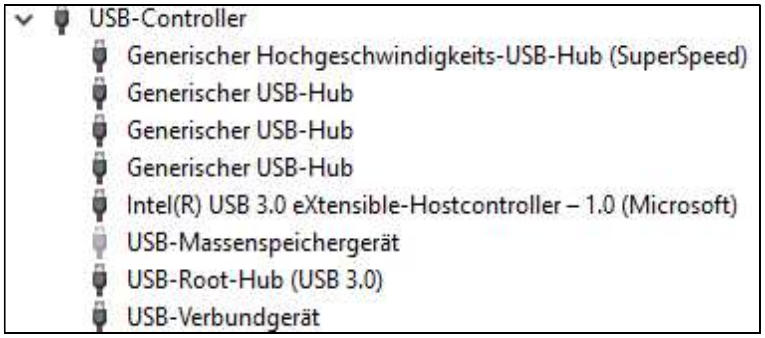


Bild 34 Gerätemanager_1

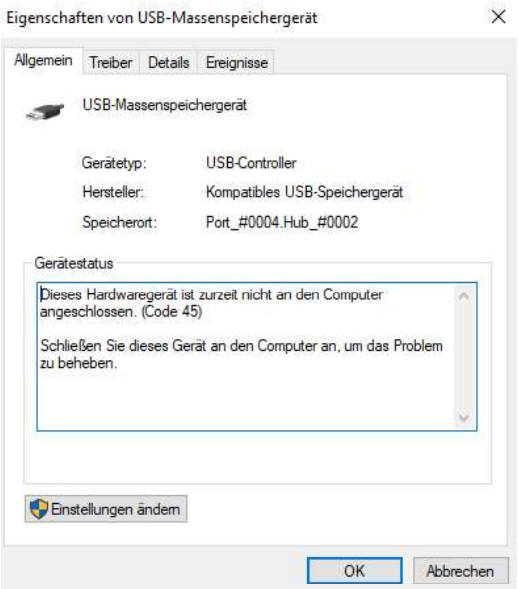


Bild 35 Gerätemanager_2

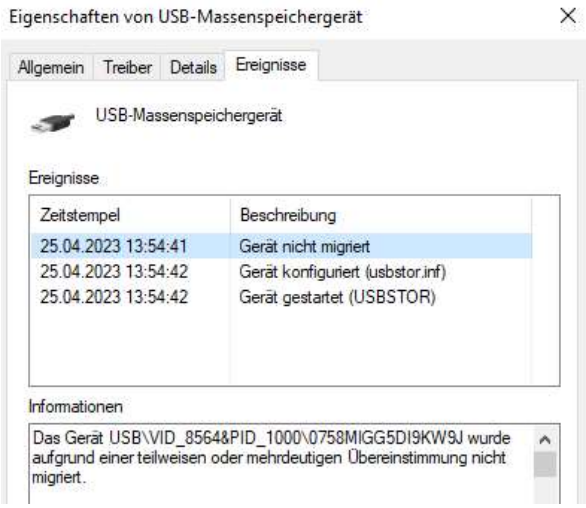


Bild 36 Gerätemanager_3

6.10 Anhang Registry Editor

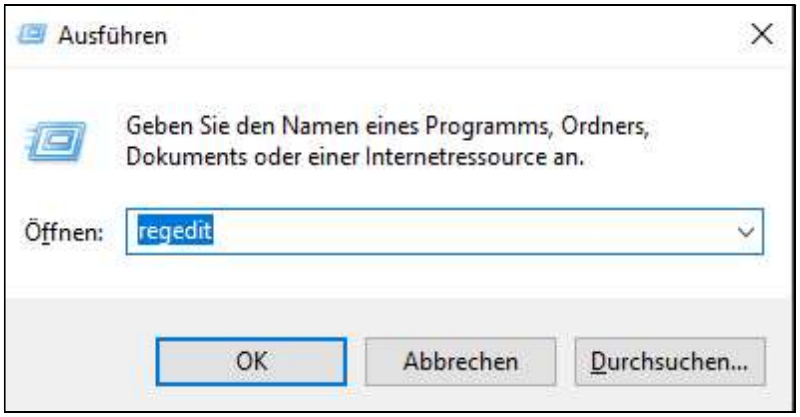


Bild 37 RegEdit_0

Bild 38 RegEdit_1

6.11 Anhang Registry Einträge PortableApps

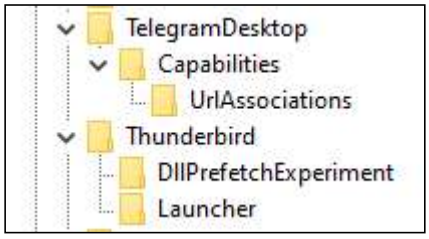


Bild 39 RegEdit_PortableApps

6.12 Anhang ‚MUICacheView.chm' (HTML-Hilfedatei)'

MUICacheView

MUICacheView v1.01
Copyright (c) 2008 - 2010 Nir Sofer
Web site: http://www.nirsoft.net

Description

Each time that you start using a new application, Windows operating system automatically extract the application name from the version resource of the exe file, and stores it for using it later, in Registry key known as the 'MuiCache'.

This utility allows you to easily view and edit the list of all MuiCache items on your system. You can edit the name of the application, or alternatively, you can delete unwanted MUICache items.
Be aware that even if your delete MUICache items, they'll reappear in the next time that you run the application.

The Location Of The MUICache Data in the Registry

In Windows 2000, Windows XP, Windows Server 2003, the MUICache data is stored under HKEY_CURRENT_USER\Software\Microsoft\Windows\ShellNoRoam\MUICache.
Starting from Windows Vista, the MUICache data is stored under HKEY_CURRENT_USER\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache

Version History

- Version 1.01 - Added sorting command-line option and fixed the icons problem in Windows 7/x64.
- Version 1.00 - First release.

Using MUICacheView

MUICacheView doesn't require any installation process or additional DLLs. In order to start using it, simply run the executable file - MUICacheView.exe
The main window of MUICacheView displays the list of all MUICache items. You can select one or more items and use the 'Delete Selected Items' option to delete them. You can also use the 'Properties' window to edit the application name of single MUICache item.

Bild 40 MUICacheView_help

6.13 Anhang Auflistung Programme

MUICache Items

Created by using MUICacheView

Application Path	Application Name
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe.FriendlyAppName	Adobe Acrobat Reader
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe.ApplicationCompany	Adobe Systems Incorporated
c:\Program Files (x86)\CyberLink\PowerDVD12\PowerDVD12.exe.ApplicationCompany	CyberLink Corp.
C:\WINDOWS\system32\NOTEPAD.EXE.FriendlyAppName	Editor
C:\Program Files\Mozilla Firefox\firefox.exe.FriendlyAppName	Firefox
C:\Program Files\Internet Explorer\IEXPLORE.EXE.FriendlyAppName	Internet Explorer
C:\Program Files\Internet Explorer\IEXPLORE.EXE.ApplicationCompany	Microsoft Corporation
C:\WINDOWS\system32\mspaint.exe.ApplicationCompany	Microsoft Corporation
C:\WINDOWS\system32\NOTEPAD.EXE.ApplicationCompany	Microsoft Corporation
C:\Program Files\Microsoft Office\Office16\WINWORD.EXE.ApplicationCompany	Microsoft Corporation
C:\Program Files (x86)\Windows Media Player\wmplayer.exe.ApplicationCompany	Microsoft Corporation
C:\Program Files\Windows NT\Accessories\WORDPAD.EXE.ApplicationCompany	Microsoft Corporation
C:\Program Files\Mozilla Firefox\firefox.exe.ApplicationCompany	Mozilla Corporation
C:\WINDOWS\system32\mspaint.exe.FriendlyAppName	Paint
c:\Program Files (x86)\CyberLink\PowerDVD12\PowerDVD12.exe.FriendlyAppName	PowerDVD 12
C:\Program Files\VideoLAN\VLC\vlc.exe.ApplicationCompany	VideoLAN
C:\Program Files\VideoLAN\VLC\vlc.exe.FriendlyAppName	VLC media player
C:\Program Files (x86)\Windows Media Player\wmplayer.exe.FriendlyAppName	Windows Media Player
C:\Program Files\Microsoft Office\Office16\WINWORD.EXE.FriendlyAppName	Word 2016
C:\Program Files\Windows NT\Accessories\WORDPAD.EXE.FriendlyAppName	WordPad

Bild 41 MUICache_Auflistung

6.14 Anhang Start Capture USB

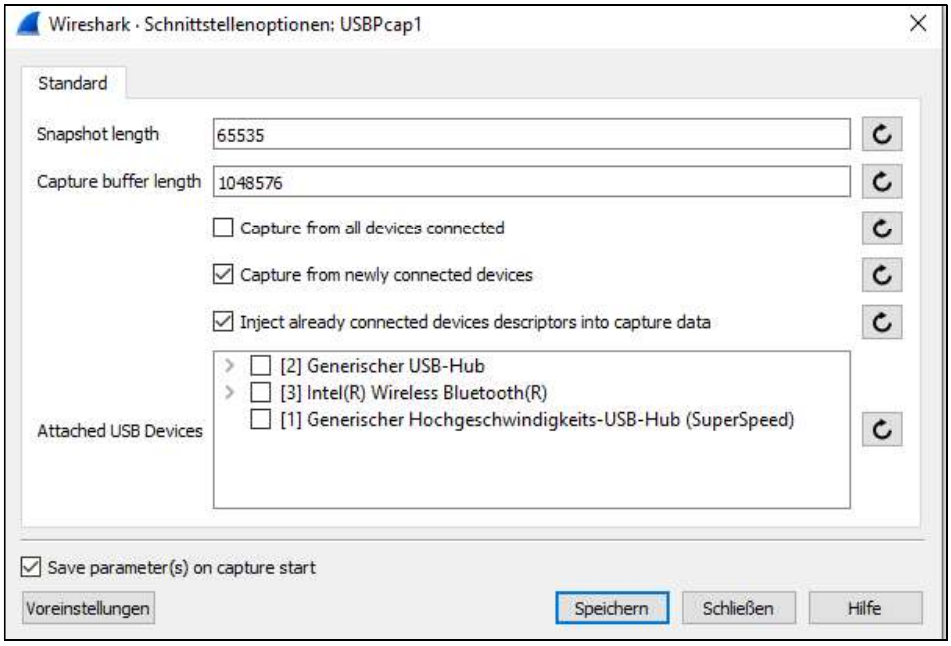


Bild 42 USBPcap_0

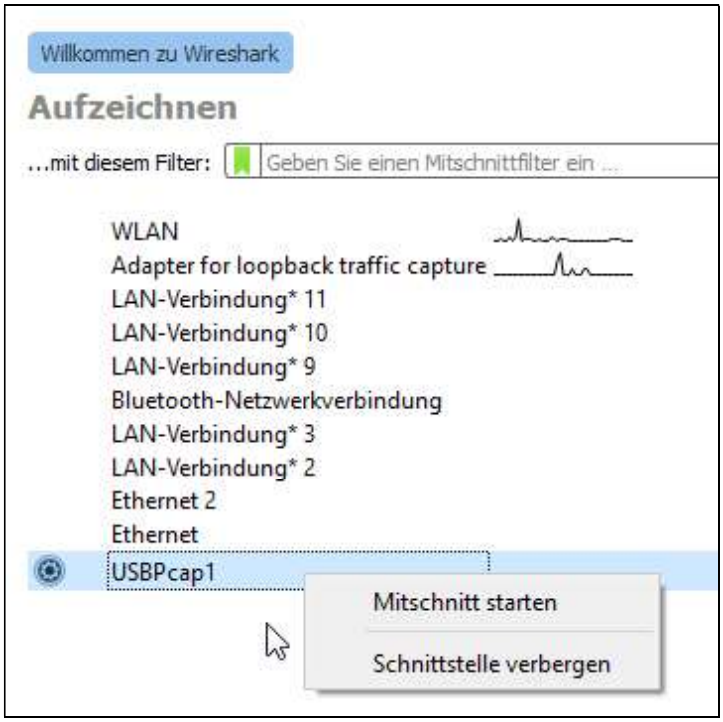


Bild 43 USBPcap_1

6.15 Anhang USB Datenpakete GUI

	Time	Source	Destination	Protocol	Length	Info
16	0.006334	1.8.0	host	USB	28	SET CONFIGURATION Response
17	0.006351	host	1.8.0	USB	36	SET INTERFACE Request
18	0.006895	1.8.0	host	USB	28	SET INTERFACE Response
19	0.006911	host	1.8.0	USBMS	36	GET MAX LUN Request
20	0.007406	1.8.0	host	USBMS	29	GET MAX LUN Response
21	0.007502	host	1.8.1	USBMS	58	SCSI: Inquiry LUN: 0x00
22	0.007535	1.8.1	host	USB	27	URB_BULK out
23	0.007537	host	1.8.2	USB	27	URB_BULK in
24	0.344081	1.8.2	host	USBMS	63	SCSI: Data In LUN: 0x00 (Inquiry Response
25	0.344106	host	1.8.2	USB	27	URB_BULK in
26	0.344387	1.8.2	host	USBMS	40	SCSI: Response LUN: 0x00 (Inquiry) (Good)
27	0.344464	host	1.8.1	USBMS	58	SCSI: Inquiry LUN: 0x00
28	0.344533	1.8.1	host	USB	27	URB_BULK out
29	0.344534	host	1.8.2	USB	27	URB_BULK in
30	0.344751	1.8.2	host	USBMS	63	SCSI: Data In LUN: 0x00 (Inquiry Response
31	0.344753	host	1.8.2	USB	27	URB_BULK in
32	0.345078	1.8.2	host	USBMS	40	SCSI: Response LUN: 0x00 (Inquiry) (Good)
33	0.345091	host	1.8.1	USBMS	58	SCSI Command: 0x23 LUN:0x00
34	0.345154	1.8.1	host	USB	27	URB_BULK out

Bild 44 USB_Datenpakete

6.16 Anhang IP Datenpakete GUI

No.	Time	Source	Destination	Protocol
10558	399.778698	192.168.0.8	149.154.167.50	TCP
10562	399.798290	149.154.167.50	192.168.0.8	TCP
10566	399.798792	192.168.0.8	149.154.167.50	TCP
10572	399.802099	192.168.0.8	149.154.167.50	TCP
10580	399.835859	192.168.0.8	149.154.167.50	HTTP
10586	399.869479	149.154.167.50	192.168.0.8	TCP
10589	399.870419	149.154.167.50	192.168.0.8	TCP
10590	399.870529	192.168.0.8	149.154.167.50	TCP

Bild 45 IP_Datenpakete

6.17 Anhang WHOIS Abfrage

Whois IP 149.154.167.50

Updated 2 days ago

```
% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See http://www.ripe.net/db/support/db-terms-conditions.pdf

% Note: this output has been filtered.
%       To receive output for a database update, use the "-B" flag.

% Information related to '149.154.164.0 - 149.154.167.255'

% Abuse contact for '149.154.164.0 - 149.154.167.255' is 'abuse@telegram.org'

inetnum:        149.154.164.0 - 149.154.167.255
netname:        Telegram_Messenger_Network
descr:          Telegram Messenger Network
country:        GB
geoloc:         52.379189 4.899431
admin-c:        ND2624-RIPE
tech-c:         ND2624-RIPE
abuse-c:        TMI12-RIPE
status:         ASSIGNED PA
mnt-by:         MNT-TELEGRAM
created:        2014-09-19T22:29:39Z
last-modified:  2018-06-12T10:52:20Z
source:         RIPE
```

Bild 46 WHOIS

6.18 Anhang Memory Dump

```
C:\Users\PortableApps\Desktop>winpmem_mini_x64_rc2.exe RAM-Dump.raw
WinPmem64
Extracting driver to C:\Users\PORTAB~1\AppData\Local\Temp\pme3F2E.tmp
Driver Unloaded.
Loaded Driver C:\Users\PORTAB~1\AppData\Local\Temp\pme3F2E.tmp.
Deleting C:\Users\PORTAB~1\AppData\Local\Temp\pme3F2E.tmp
The system time is: 06:21:21
Will generate a RAW image
 - buffer_size_: 0x1000
CR3: 0x00001AD002
 6 memory ranges:
Start 0x00001000 - Length 0x00057000
Start 0x00059000 - Length 0x00045000
Start 0x0009F000 - Length 0x00001000
Start 0x00100000 - Length 0xC6F0C000
Start 0xC7EFF000 - Length 0x00001000
Start 0x100000000 - Length 0x300000000
max_physical_memory_ 0x400000000
Acquitision mode PTE Remapping
Padding from 0x00000000 to 0x00001000
pad
 - length: 0x1000

00% 0x00000000 .
copy_memory
 - start: 0x1000
 - end: 0x58000

00% 0x00001000 .
Padding from 0x00058000 to 0x00059000
pad
 - length: 0x1000

00% 0x00058000 .
copy_memory
 - start: 0x59000
 - end: 0x9e000

00% 0x00059000 .
Padding from 0x0009E000 to 0x0009F000
pad
 - length: 0x1000

00% 0x0009E000 .
copy_memory
 - start: 0x9f000
 - end: 0xa0000
```

Bild 47 RAM-Dump_0

```
00% 0x0009F000 .
Padding from 0x000A0000 to 0x00100000
pad
 - length: 0x60000

00% 0x000A0000 .
copy_memory
 - start: 0x100000
 - end: 0xc700c000

00% 0x00100000 ..................................................
04% 0x32100000 ..................................................
09% 0x64100000 ..................................................
14% 0x96100000 ..................................................
Padding from 0xC700C000 to 0xC7EFF000
pad
 - length: 0xef3000

19% 0xC700C000 .
copy_memory
 - start: 0xc7eff000
 - end: 0xc7f00000

19% 0xC7EFF000 .
Padding from 0xC7F00000 to 0x100000000
pad
 - length: 0x38100000

19% 0xC7F00000 ..................................................
19% 0xC7F00000 .......
copy_memory
 - start: 0x100000000
 - end: 0x400000000

25% 0x100000000 ..................................................
29% 0x132000000 ..................................................
34% 0x164000000 ..................................................
39% 0x196000000 ..................................................
44% 0x1C8000000 ..................................................
49% 0x1FA000000 ..................................................
54% 0x22C000000 ..................................................
59% 0x25E000000 ..................................................
64% 0x290000000 ..................................................
68% 0x2C2000000 ..................................................
73% 0x2F4000000 ..................................................
78% 0x326000000 ..................................................
83% 0x358000000 ..................................................
88% 0x38A000000 ..................................................
93% 0x3BC000000 ..................................................
98% 0x3EE000000 ..................
The system time is: 06:23:40
Driver Unloaded.
```

Bild 48 RAM-Dump_1

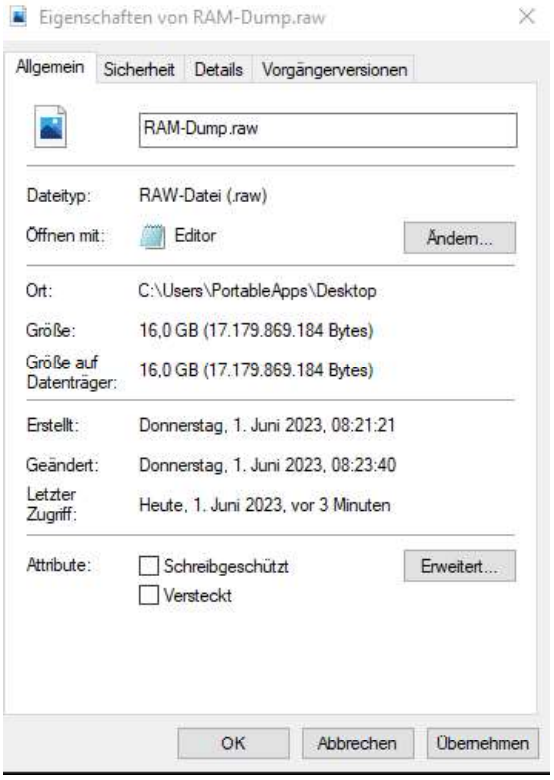


Bild 49 RAM-Dump_2

6.19 Anhang VM-Konfiguration

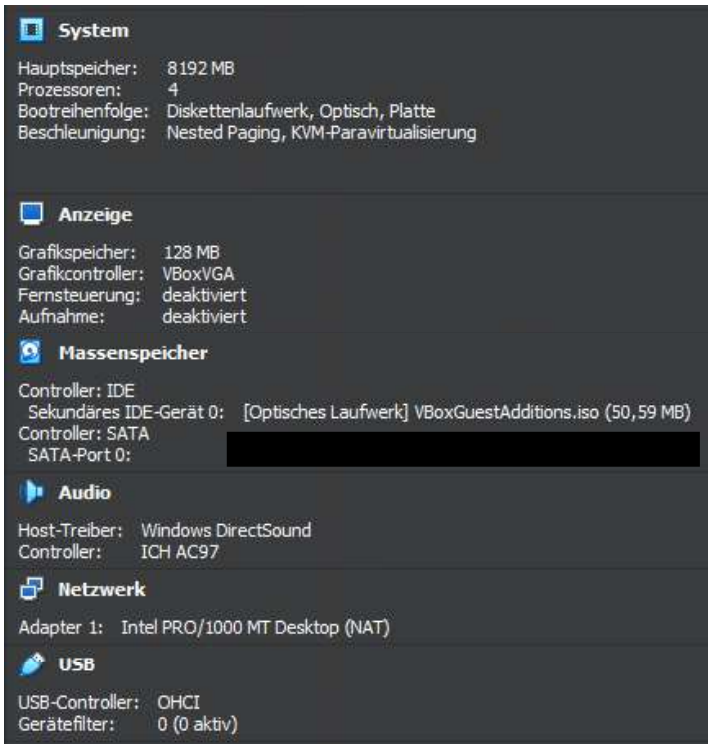


Bild 50 VM-Config

6.20 Anhang Volatility3 Manpage – Windows Befehle

windows.bigpools.BigPools

List big page pools.

windows.callbacks.Callbacks

Lists kernel callbacks and notification routines.

windows.cmdline.CmdLine

Lists process command line arguments.

windows.crashinfo.Crashinfo

Lists the information from a Windows crash dump.

windows.devicetree.DeviceTree

Listing tree based on drivers and attached devices in a particular windows memory image.

windows.dlllist.DllList

Lists the loaded modules in a particular windows memory image.

windows.driverirp.DriverIrp

List IRPs for drivers in a particular windows memory image.

windows.drivermodule.DriverModule

Determines if any loaded drivers were hidden by a rootkit

windows.driverscan.DriverScan

Scans for drivers present in a particular windows memory image.

windows.dumpfiles.DumpFiles

Dumps cached file contents from Windows memory samples.

windows.envars.Envars

Display process environment variables

windows.filescan.FileScan

Scans for file objects present in a particular windows memory image.

windows.getservicesids.GetServiceSIDs

Lists process token sids.

windows.getsids.GetSIDs

Print the SIDs owning each process

windows.handles.Handles

Lists process open handles.

windows.info.Info Show OS & kernel details of the memory sample being analyzed.

windows.joblinks.JobLinks

Print process job link information

windows.ldrmodules.LdrModules

Lists the loaded modules in a particular windows memory image.

windows.malfind.Malfind

Lists process memory ranges that potentially contain injected code.

windows.mbrscan.MBRScan

Scans for and parses potential Master Boot Records (MBRs)

windows.memmap.Memmap

Prints the memory map

windows.modscan.ModScan

Scans for modules present in a particular windows memory image.

windows.modules.Modules

Lists the loaded kernel modules.

windows.mutantscan.MutantScan

Scans for mutexes present in a particular windows memory image.

windows.poolscanner.PoolScanner

A generic pool scanner plugin.

windows.privileges.Privs

Lists process token privileges

windows.pslist.PsList

Lists the processes present in a particular windows memory image.

windows.psscan.PsScan

Scans for processes present in a particular windows memory image.

windows.pstree.PsTree

Plugin for listing processes in a tree based on their parent process ID.

windows.registry.certificates.Certificates

Lists the certificates in the registry's Certificate Store.

windows.registry.hivelist.HiveList

Lists the registry hives present in a particular memory image.

windows.registry.hivescan.HiveScan

Scans for registry hives present in a particular windows memory image.

windows.registry.printkey.PrintKey

Lists the registry keys under a hive or specific key value.

windows.registry.userassist.UserAssist

Print userassist registry keys and information.

windows.sessions.Sessions

lists Processes with Session information extracted from Environmental Variables

windows.ssdt.SSDT Lists the system call table.

windows.statistics.Statistics

Lists statistics about the memory space.

windows.strings.Strings

Reads output from the strings command and indicates which process(es) each string belongs to.

windows.symlinkscan.SymlinkScan

Scans for links present in a particular windows memory

image.

windows.vadinfo.VadInfo

Lists process memory ranges.

windows.vadwalk.VadWalk

Walk the VAD tree.

windows.virtmap.VirtMap

Lists virtual mapped sections.

6.21 Anhang Ausgabe Pstree

```
Volatility 3 Framework 2.4.2

PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime

4       0       System  0x9c08f9cbf240  245     -       N/A     False   2023-06-01 06:03:39.000000      N/A
* 696   4       smss.exe        0x9c090087f080  4       -       N/A     False   2023-06-01 06:03:39.000000      N/A
** 936  696     smss.exe        0x9c090a232200  0       -       1       False   2023-06-01 06:03:50.000000      2023-06-01 06:03:50.000000
*** 952 936     csrss.exe       0x9c090a233080  14      -       1       False   2023-06-01 06:03:50.000000      N/A
*** 1040        936     winlogon.exe    0x9c090917b1c0  6       -       1       False   2023-06-01 06:03:50.000000      N/A
**** 1448       1040    dwm.exe 0x9c090ac0b080  27      -       1       False   2023-06-01 06:03:50.000000      N/A
**** 1220       1040    fontdrvhost.ex  0x9c0909d510c0  6       -       1       False   2023-06-01 06:03:50.000000      N/A
**** 8164       1040    DPAgent.exe     0x9c09094dc080  26      -       1       True    2023-06-01 06:03:55.000000      N/A
***** 8972      8164    DpAgent.exe     0x9c0908cea080  2       -       1       False   2023-06-01 06:03:56.000000      N/A
**** 8136       1040    userinit.exe    0x9c0909f35080  0       -       1       False   2023-06-01 06:03:55.000000      2023-06-01 06:04:18.000000
***** 8184      8136    explorer.exe    0x9c09094dc080  80      -       1       False   2023-06-01 06:03:55.000000      N/A
****** 12356    8184    Greenshot.exe   0x9c090afdc080  19      -       1       False   2023-06-01 06:04:11.000000      N/A
****** 13252    8184    OneDrive.exe    0x9c0903d89080  42      -       1       False   2023-06-01 06:04:14.000000      N/A
******* 12700   13252   Microsoft.Shar  0x9c0903d87080  0       -       1       False   2023-06-01 06:04:16.000000      2023-06-01 06:14:18.000000
****** 3460     8184    Start.exe       0x9c0905554080  0       -       1       True    2023-06-01 06:06:59.000000      2023-06-01 06:07:00.000000
******* 14256   3460    PortableAppsP1  0x9c090b3f3080  0       -       1       True    2023-06-01 06:07:00.000000      2023-06-01 06:19:07.000000
******** 11088  14256   DontSleepPorta  0x9c090574e080  5       -       1       True    2023-06-01 06:08:12.000000      N/A
********* 8900  11088   DontSleep_x64_  0x9c09054d5080  8       -       1       False   2023-06-01 06:08:13.000000      N/A
****** 11688    8184    SecurityHealth  0x9c090b3ef080  9       -       1       False   2023-06-01 06:04:10.000000      N/A
****** 12332    8184    IAStorIconLaun  0x9c090afd8080  0       -       1       True    2023-06-01 06:04:11.000000      2023-06-01 06:05:11.000000
******* 13368   12332   IAStorIcon.exe  0x9c09012be080  10      -       1       True    2023-06-01 06:05:11.000000      N/A
****** 4688     8184    ONENOTEM.EXE    0x9c0903d8c080  3       -       1       False   2023-06-01 06:04:15.000000      N/A
****** 13144    8184    PtSessionAgent  0x9c09096bb080  6       -       1       False   2023-06-01 06:04:13.000000      N/A
****** 12340    8184    WINWORD.EXE     0x9c0901fe1080  20      -       1       False   2023-06-01 06:14:20.000000      N/A
****** 14996    8184    cmd.exe 0x9c0908a5c080  1       -       1       False   2023-06-01 06:19:50.000000      N/A
******* 18104   14996   winpmem_mini_x  0x9c090534e080  1       -       1       False   2023-06-01 06:21:20.000000      N/A
******* 14564   14996   conhost.exe     0x9c09062c1080  5       -       1       False   2023-06-01 06:19:50.000000      N/A
****** 12856    8184    pdf24.exe       0x9c090a6af080  11      -       1       False   2023-06-01 06:04:13.000000      N/A
** 788  696     smss.exe        0x9c0900aa9080  0       -       0       False   2023-06-01 06:03:44.000000      2023-06-01 06:03:50.000000
*** 944 788     wininit.exe     0x9c090a222080  5       -       0       False   2023-06-01 06:03:50.000000      N/A
**** 1016       944     services.exe    0x9c090aa5c8c0  16      -       0       False   2023-06-01 06:03:50.000000      N/A
***** 3588      1016    svchost.exe     0x9c0909ef0080  12      -       1       False   2023-06-01 06:03:51.000000      N/A
***** 4184      1016    svchost.exe     0x9c0908026180  5       -       0       False   2023-06-01 06:03:51.000000      N/A
****** 4268     4184    ctfmon.exe      0x9c090803880   15      -       1       False   2023-06-01 06:03:51.000000      N/A
***** 10764     1016    svchost.exe     0x9c0900bd70c0  8       -       0       False   2023-06-01 06:03:59.000000      N/A
***** 5140      1016    svchost.exe     0x9c0907890080  4       -       0       False   2023-06-01 06:03:52.000000      N/A
***** 1576      1016    svchost.exe     0x9c090ac6d080  5       -       0       False   2023-06-01 06:03:50.000000      N/A
***** 2600      1016    svchost.exe     0x9c0907c0e080  5       -       0       False   2023-06-01 06:03:51.000000      N/A
***** 1584      1016    svchost.exe     0x9c090ac71080  8       -       0       False   2023-06-01 06:03:50.000000      N/A
***** 3120      1016    svchost.exe     0x9c090adae080  7       -       0       False   2023-06-01 06:03:51.000000      N/A
***** 4144      1016    svchost.exe     0x9c090800c080  16      -       0       False   2023-06-01 06:03:51.000000      N/A
****** 4648     4144    wlanext.exe     0x9c08f9ccf080  4       -       0       False   2023-06-01 06:03:52.000000      N/A
******* 4664    4648    conhost.exe     0x9c08f9ce2080  4       -       0       False   2023-06-01 06:03:52.000000      N/A
***** 1600      1016    svchost.exe     0x9c090ac74080  9       -       0       False   2023-06-01 06:03:50.000000      N/A
***** 3648      1016    svchost.exe     0x9c0909f338c0  10      -       0       False   2023-06-01 06:03:51.000000      N/A
***** 6208      1016    IAStorDataMgrS  0x9c0909ed5080  10      -       0       True    2023-06-01 06:06:01.000000      N/A
***** 1608      1016    svchost.exe     0x9c090ac7a080  9       -       0       False   2023-06-01 06:03:50.000000      N/A
***** 5788      1016    svchost.exe     0x9c09079b0080  16      -       0       False   2023-06-01 06:03:52.000000      N/A
***** 4692      1016    mDNSResponder.  0x9c0907b54080  6       -       0       False   2023-06-01 06:03:52.000000      N/A
```

Bild 51 Pstree_0

***** 2144	1016	IntelCpHeci5vc	0x9c090a0c0080	7	-	0	False	2023-06-01 06:03:50.000000	N/A
***** 11364	1016	SecurityHealth	0x9c090b3f1080	18	-	0	False	2023-06-01 06:04:10.000000	N/A
***** 10856	1016	svchost.exe	0x9c090583d080	6	-	0	False	2023-06-01 06:06:02.000000	N/A
***** 5240	1016	svchost.exe	0x9c090141a080	10	-	0	False	2023-06-01 06:03:52.000000	N/A
***** 3196	1016	svchost.exe	0x9c090ad53080	15	-	0	False	2023-06-01 06:03:51.000000	N/A
***** 9856	1016	svchost.exe	0x9c09095af080	6	-	0	False	2023-06-01 06:14:10.000000	N/A
***** 4228	1016	svchost.exe	0x9c0907dd2080	16	-	0	False	2023-06-01 06:03:51.000000	N/A
***** 2180	1016	WUDFHost.exe	0x9c09056a8080	8	-	0	False	2023-06-01 06:06:04.000000	N/A
***** 5256	1016	XtuService.exe	0x9c090141e080	12	-	0	False	2023-06-01 06:03:52.000000	N/A
***** 1164	1016	svchost.exe	0x9c09091bc080	33	-	0	False	2023-06-01 06:03:50.000000	N/A
****** 5252	1164	UserOOBEBroker	0x9c0900b62080	6	-	1	False	2023-06-01 06:04:44.000000	N/A
****** 9248	1164	unsecapp.exe	0x9c090a6130c0	3	-	1	False	2023-06-01 06:03:57.000000	N/A
****** 9660	1164	RuntimeBroker.	0x9c090a4e70c0	27	-	1	False	2023-06-01 06:03:58.000000	N/A
****** 9792	1164	ShellExperienc	0x9c09052e9080	14	-	1	False	2023-06-01 06:04:49.000000	N/A
****** 9284	1164	StartMenuExper	0x9c090a61a080	64	-	1	False	2023-06-01 06:03:57.000000	N/A
****** 10052	1164	SearchApp.exe	0x9c090ae950c0	53	-	1	False	2023-06-01 06:03:58.000000	N/A
****** 10436	1164	RuntimeBroker.	0x9c0901fdc080	8	-	1	False	2023-06-01 06:04:50.000000	N/A
****** 4936	1164	RuntimeBroker.	0x9c090b0c80c0	26	-	1	False	2023-06-01 06:03:58.000000	N/A
****** 8524	1164	unsecapp.exe	0x9c0907e6a080	4	-	0	False	2023-06-01 06:03:56.000000	N/A
****** 11604	1164	RuntimeBroker.	0x9c0907aba080	6	-	1	False	2023-06-01 06:04:02.000000	N/A
****** 2804	1164	ApplicationFra	0x9c090b19a080	12	-	1	False	2023-06-01 06:04:43.000000	N/A
****** 2008	1164	SystemSettings	0x9c090a631080	25	-	1	False	2023-06-01 06:04:43.000000	N/A
****** 7384	1164	WmiPrvSE.exe	0x9c090b545080	9	-	0	False	2023-06-01 06:03:53.000000	N/A
****** 11484	1164	smartscreen.ex	0x9c0908cf0080	11	-	1	False	2023-06-01 06:04:10.000000	N/A
****** 7780	1164	RuntimeBroker.	0x9c09096cc080	5	-	1	False	2023-06-01 06:04:09.000000	N/A
****** 7144	1164	WmiPrvSE.exe	0x9c0908a5a080	10	-	0	False	2023-06-01 06:03:53.000000	N/A
****** 9064	1164	TextInputHost.	0x9c09052db080	12	-	1	False	2023-06-01 06:05:36.000000	N/A
****** 3696	1164	dllhost.exe	0x9c09093cc080	12	-	1	False	2023-06-01 06:19:38.000000	N/A
****** 5880	1164	FileCoAuth.exe	0x9c0907a70300	10	-	1	False	2023-06-01 06:04:44.000000	N/A
****** 12284	1164	PhoneExperienc	0x9c09088b1080	21	-	1	False	2023-06-01 06:04:06.000000	N/A
***** 1680	1016	svchost.exe	0x9c0909321080	9	-	0	False	2023-06-01 06:03:50.000000	N/A
***** 5776	1016	HotKeyServiceU	0x9c09079a40c0	14	-	0	False	2023-06-01 06:03:52.000000	N/A
****** 9756	5776	HPHotkeyNotifi	0x9c090a484080	7	-	1	False	2023-06-01 06:03:58.000000	N/A
***** 13968	1016	svchost.exe	0x9c090583c080	5	-	0	False	2023-06-01 06:06:02.000000	N/A
***** 10484	1016	SgrmBroker.exe	0x9c090535a080	7	-	0	False	2023-06-01 06:06:01.000000	N/A
***** 1192	1016	WUDFHost.exe	0x9c0909d0b240	8	-	0	False	2023-06-01 06:03:50.000000	N/A
***** 5384	1016	armsvc.exe	0x9c090544a080	6	-	0	True	2023-06-01 06:05:57.000000	N/A
***** 1736	1016	svchost.exe	0x9c090a04d0c0	13	-	0	False	2023-06-01 06:03:50.000000	N/A
***** 1744	1016	svchost.exe	0x9c090a051080	4	-	0	False	2023-06-01 06:03:50.000000	N/A
***** 1232	1016	svchost.exe	0x9c09084d7080	0	-	0	False	2023-06-01 06:08:51.000000	2023-06-01 06:08:57.000000
***** 2260	1016	svchost.exe	0x9c0909391080	11	-	0	False	2023-06-01 06:03:50.000000	N/A
****** 3392	2260	sihost.exe	0x9c0909e0c080	17	-	1	False	2023-06-01 06:03:51.000000	N/A
******* 13616	3392	msedge.exe	0x9c090838c2c0	0	-	1	False	2023-06-01 06:04:44.000000	2023-06-01 06:04:45.000000
***** 3284	1016	svchost.exe	0x9c0909e08080	18	-	0	False	2023-06-01 06:03:51.000000	N/A
****** 14288	3284	audiodg.exe	0x9c090a629080	5	-	0	False	2023-06-01 06:17:30.000000	N/A
***** 9948	1016	svchost.exe	0x9c090a5bd2c0	21	-	0	False	2023-06-01 06:03:58.000000	N/A
***** 11988	1016	svchost.exe	0x9c0907fed080	5	-	0	False	2023-06-01 06:04:03.000000	N/A
***** 4312	1016	spoolsv.exe	0x9c09080c7080	18	-	0	False	2023-06-01 06:03:51.000000	N/A
***** 8928	1016	HPSupportSolut	0x9c090554f080	10	-	0	False	2023-06-01 06:05:58.000000	N/A
***** 4836	1016	coreServiceShe	0x9c090aa0a080	253	-	0	False	2023-06-01 06:03:52.000000	N/A
****** 4960	4836	uiWatchDog.exe	0x9c09076e1080	4	-	0	False	2023-06-01 06:03:52.000000	N/A

Bild 52 Pstree_1

```
******* 12748   4960   uiSeAgnt.exe     0x9c0903c0f080  10   -   1   False   2023-06-01 06:04:12.000000   N/A
****** 5892    4836   coreFrameworkH   0x9c09079c7080  4    -   0   False   2023-06-01 06:03:52.000000   N/A
******* 5956   5892   conhost.exe      0x9c09074b5100  6    -   0   False   2023-06-01 06:03:52.000000   N/A
****** 12648   4836   DrSDKCaller.ex   0x9c0903c0e200  57   -   0   False   2023-06-01 06:04:12.000000   N/A
******* 12656  12648  conhost.exe      0x9c0903a750c0  4    -   0   False   2023-06-01 06:04:12.000000   N/A
****** 12172   4836   TeslaInstance64  0x9c090a161300  3    -   0   False   2023-06-01 06:04:06.000000   N/A
****** 5112    4836   conhost.exe      0x9c0907852080  6    -   0   False   2023-06-01 06:03:52.000000   N/A
***** 3304     1016   svchost.exe      0x9c09076f8080  22   -   0   False   2023-06-01 06:03:52.000000   N/A
***** 5864     1016   svchost.exe      0x9c09079c6080  8    -   0   False   2023-06-01 06:03:52.000000   N/A
***** 2796     1016   svchost.exe      0x9c0907ce0080  5    -   0   False   2023-06-01 06:03:51.000000   N/A
***** 11512    1016   svchost.exe      0x9c090536c080  13   -   1   False   2023-06-01 06:05:34.000000   N/A
***** 2816     1016   svchost.exe      0x9c0908192080  20   -   0   False   2023-06-01 06:03:51.000000   N/A
***** 3844     1016   svchost.exe      0x9c0909fc4080  8    -   0   False   2023-06-01 06:03:51.000000   N/A
***** 4360     1016   svchost.exe      0x9c0907853080  7    -   0   False   2023-06-01 06:03:52.000000   N/A
***** 3852     1016   svchost.exe      0x9c0909fc8080  6    -   0   False   2023-06-01 06:03:51.000000   N/A
***** 3860     1016   svchost.exe      0x9c0909fc5080  23   -   0   False   2023-06-01 06:03:51.000000   N/A
***** 4372     1016   svchost.exe      0x9c08f9c5e080  22   -   0   False   2023-06-01 06:03:52.000000   N/A
***** 5912     1016   LanWlanWwanSvc   0x9c09074b3080  11   -   0   False   2023-06-01 06:03:52.000000   N/A
***** 12572    1016   svchost.exe      0x9c0903c0b080  11   -   0   False   2023-06-01 06:04:12.000000   N/A
***** 3360     1016   svchost.exe      0x9c0909e4e080  26   -   0   False   2023-06-01 06:03:51.000000   N/A
***** 1316     1016   svchost.exe      0x9c0909d5b240  23   -   0   False   2023-06-01 06:03:50.000000   N/A
***** 1828     1016   svchost.exe      0x9c090a866080  24   -   0   False   2023-06-01 06:03:50.000000   N/A
****** 3808    1828   MicTray64.exe    0x9c0909f93080  7    -   1   False   2023-06-01 06:03:51.000000   N/A
****** 3784    1828   taskhostw.exe    0x9c0909f7c080  21   -   1   False   2023-06-01 06:03:51.000000   N/A
****** 9128    1828   taskhostw.exe    0x9c0908ce9080  8    -   1   False   2023-06-01 06:03:57.000000   N/A
****** 3692    1828   GoogleUpdate.e   0x9c0909f66080  0    -   0   True    2023-06-01 06:03:51.000000   2023-06-01 06:04:02.000000
******* 11488  3692   GoogleCrashHan   0x9c090a162080  5    -   0   False   2023-06-01 06:04:02.000000   N/A
******* 11468  3692   GoogleCrashHan   0x9c0901398080  5    -   0   True    2023-06-01 06:04:01.000000   N/A
****** 3824    1828   QLBController.   0x9c0909f94080  5    -   1   False   2023-06-01 06:03:51.000000   N/A
****** 6908    1828   HPSF.exe         0x9c090568d080  0    -   1   False   2023-06-01 06:07:52.000000   2023-06-01 06:08:02.000000
***** 2348     1016   svchost.exe      0x9c090824c080  6    -   0   False   2023-06-01 06:03:50.000000   N/A
***** 4400     1016   svchost.exe      0x9c08f9d6d080  12   -   0   False   2023-06-01 06:03:52.000000   N/A
***** 2884     1016   igfxCUIService   0x9c09081c8080  8    -   0   False   2023-06-01 06:03:51.000000   N/A
****** 4728    2884   igfxEM.exe       0x9c08f9dd9080  11   -   1   False   2023-06-01 06:03:52.000000   N/A
***** 4428     1016   svchost.exe      0x9c08f9d71080  7    -   0   False   2023-06-01 06:03:52.000000   N/A
***** 9548     1016   svchost.exe      0x9c090b5d8080  11   -   0   False   2023-06-01 06:03:57.000000   N/A
***** 8020     1016   svchost.exe      0x9c0908997080  30   -   0   False   2023-06-01 06:03:55.000000   N/A
***** 1368     1016   svchost.exe      0x9c090862f080  7    -   0   False   2023-06-01 06:03:50.000000   N/A
***** 3936     1016   svchost.exe      0x9c09074f080   9    -   0   False   2023-06-01 06:03:52.000000   N/A
***** 4460     1016   PtSvcHost.exe    0x9c09078560c0  20   -   0   False   2023-06-01 06:03:52.000000   N/A
****** 5648    4460   PtWatchDog.exe   0x9c0907e69080  9    -   0   False   2023-06-01 06:03:52.000000   N/A
***** 3948     1016   LMS.exe 0x9c0909f7d080  12   -   0   True    2023-06-01 06:06:01.000000   N/A
***** 5500     1016   svchost.exe      0x9c0907e820c0  8    -   0   False   2023-06-01 06:03:52.000000   N/A
***** 3452     1016   svchost.exe      0x9c0909ed2080  12   -   1   False   2023-06-01 06:03:51.000000   N/A
***** 1920     1016   IntelCpHDCPSvc   0x9c090a88b080  8    -   0   False   2023-06-01 06:03:50.000000   N/A
***** 6016     1016   svchost.exe      0x9c090ab22080  6    -   0   False   2023-06-01 06:08:51.000000   N/A
***** 4996     1016   svchost.exe      0x9c09076f3080  11   -   0   False   2023-06-01 06:03:52.000000   N/A
***** 13700    1016   svchost.exe      0x9c090131b080  20   -   0   False   2023-06-01 06:04:23.000000   N/A
***** 2440     1016   svchost.exe      0x9c0908262080  11   -   0   False   2023-06-01 06:03:51.000000   N/A
***** 5004     1016   svchost.exe      0x9c09076f6080  14   -   0   False   2023-06-01 06:03:52.000000   N/A
***** 2448     1016   svchost.exe      0x9c0908827c080 8    -   0   False   2023-06-01 06:03:51.000000   N/A
****** 2672    2448   dasHost.exe      0x9c0907c54080  15   -   0   False   2023-06-01 06:03:51.000000   N/A
```

Bild 53 Pstree_2

```
***** 6032     1016   svchost.exe      0x9c09076fb080  18   -   0   False   2023-06-01 06:03:52.000000   N/A
***** 10128    1016   SearchIndexer.   0x9c090aec70c0  58   -   0   False   2023-06-01 06:03:50.000000   N/A
***** 2964     1016   svchost.exe      0x9c090a330080  7    -   0   False   2023-06-01 06:03:51.000000   N/A
***** 5012     1016   CxMonSvc.exe     0x9c09076f7080  12   -   0   False   2023-06-01 06:03:52.000000   N/A
****** 6948    5012   sacpl.exe        0x9c0908a450c0  8    -   1   True    2023-06-01 06:03:53.000000   2023-06-01 06:03:55.000000
******* 7628   6948   SmartAudio3.ex   0x9c09095b0080  20   -   1   False   2023-06-01 06:03:55.000000   N/A
***** 2456     1016   svchost.exe      0x9c090827f080  8    -   0   False   2023-06-01 06:03:51.000000   N/A
***** 1948     1016   svchost.exe      0x9c090a0a7080  5    -   0   False   2023-06-01 06:03:50.000000   N/A
***** 2972     1016   svchost.exe      0x9c090a38e0c0  8    -   0   False   2023-06-01 06:03:51.000000   N/A
***** 5020     1016   CxUtilSvc.exe    0x9c09076fa080  6    -   0   True    2023-06-01 06:03:52.000000   N/A
***** 1956     1016   svchost.exe      0x9c090a0aa080  7    -   0   False   2023-06-01 06:03:50.000000   N/A
***** 5028     1016   svchost.exe      0x9c09076f1080  19   -   0   False   2023-06-01 06:03:52.000000   N/A
***** 3496     1016   PresentationFo   0x9c0909ed3080  8    -   0   False   2023-06-01 06:03:51.000000   N/A
***** 7088     1016   svchost.exe      0x9c09054b1080  12   -   0   False   2023-06-01 06:06:02.000000   N/A
***** 5036     1016   HotkeyService.   0x9c09076f2080  6    -   0   False   2023-06-01 06:03:52.000000   N/A
***** 1972     1016   svchost.exe      0x9c090a0ad080  5    -   0   False   2023-06-01 06:03:50.000000   N/A
***** 5048     1016   DpHostW.exe      0x9c09078230c0  29   -   0   False   2023-06-01 06:03:52.000000   N/A
****** 6864    5048   DpCardEngine.e   0x9c090857e080  6    -   0   False   2023-06-01 06:03:53.000000   N/A
***** 2488     1016   jhi_service.ex   0x9c090b5d7080  5    -   0   True    2023-06-01 06:06:01.000000   N/A
***** 1980     1016   svchost.exe      0x9c090a0a9080  6    -   0   False   2023-06-01 06:03:50.000000   N/A
***** 8124     1016   svchost.exe      0x9c0909eef080  3    -   0   False   2023-06-01 06:03:55.000000   N/A
***** 1988     1016   svchost.exe      0x9c090a0b30c0  4    -   0   False   2023-06-01 06:03:50.000000   N/A
***** 6084     1016   hpqwmiex.exe     0x9c09074e8080  8    -   0   True    2023-06-01 06:03:52.000000   N/A
***** 5576     1016   svchost.exe      0x9c0907ee50c0  15   -   0   False   2023-06-01 06:03:52.000000   N/A
***** 5068     1016   svchost.exe      0x9c090782b080  3    -   0   False   2023-06-01 06:03:52.000000   N/A
***** 2512     1016   svchost.exe      0x9c09082a0080  5    -   0   False   2023-06-01 06:03:51.000000   N/A
***** 7632     1016   svchost.exe      0x9c090a0b9080  12   -   0   False   2023-06-01 06:03:55.000000   N/A
***** 5076     1016   ibtsiva.exe      0x9c0907828080  6    -   0   False   2023-06-01 06:03:52.000000   N/A
***** 2520     1016   svchost.exe      0x9c09082a7080  10   -   0   False   2023-06-01 06:03:51.000000   N/A
***** 3036     1016   svchost.exe      0x9c090a3a0080  32   -   0   False   2023-06-01 06:03:51.000000   N/A
***** 5084     1016   svchost.exe      0x9c0907850080  5    -   0   False   2023-06-01 06:03:52.000000   N/A
***** 12252    1016   AMSPTelemetry5   0x9c090888b080  10   -   0   False   2023-06-01 06:04:06.000000   N/A
***** 2528     1016   svchost.exe      0x9c09082a3080  6    -   0   False   2023-06-01 06:03:51.000000   N/A
***** 5092     1016   pdf24.exe        0x9c0907851080  11   -   0   False   2023-06-01 06:03:52.000000   N/A
***** 5612     1016   svchost.exe      0x9c090744d080  5    -   0   False   2023-06-01 06:03:52.000000   N/A
***** 8604     1016   svchost.exe      0x9c09095ae080  8    -   1   False   2023-06-01 06:03:56.000000   N/A
***** 5104     1016   SynTPEnhServic   0x9c090784e080  6    -   0   False   2023-06-01 06:03:52.000000   N/A
****** 5444    5104   SynTPEnh.exe     0x9c09014b1080  11   -   1   False   2023-06-01 06:03:52.000000   N/A
******* 5816   5444   SynTPEnh.exe     0x9c09079ae080  0    -   1   False   2023-06-01 06:03:52.000000   2023-06-01 06:03:56.000000
******** 7844  5816   SynTPHelper.ex   0x9c09094da080  3    -   1   False   2023-06-01 06:03:55.000000   N/A
***** 3576     1016   HP3DDGService.   0x9c0909f61080  2    -   0   False   2023-06-01 06:03:51.000000   N/A
**** 88 944    lsass.exe       0x9c0908e56080  12   -   0   False   2023-06-01 06:03:50.000000   N/A
**** 1212      944     fontdrvhost.ex  0x9c0909d41080  6    -   0   False   2023-06-01 06:03:50.000000   N/A
*** 852 788    csrss.exe       0x9c0909093140  14   -   0   False   2023-06-01 06:03:48.000000   N/A
* 124   4       Registry        0x9c08f9ee7080  4    -   N/A False   2023-06-01 06:03:36.000000   N/A
* 2736  4       MemCompression  0x9c0907c88080  22   -   N/A False   2023-06-01 06:03:51.000000   N/A
11732   1336    firefox.exe     0x9c0907c4c080  0    -   1   False   2023-06-01 06:19:35.000000   2023-06-01 06:19:41.000000
```

Bild 54 Pstree_3

6.22 Anhang Ausgabe Sessions

```
Volatility 3 Framework 2.4.2

Session ID      Session Type    Process ID      Process User Name       Create Time

N/A     -       4       System  -       2023-06-01 06:03:39.000000
N/A     -       124     Registry        -       2023-06-01 06:03:36.000000
N/A     -       696     smss.exe        -       2023-06-01 06:03:39.000000
0       -       788     smss.exe        -       2023-06-01 06:03:44.000000
0       -       852     csrss.exe       /SYSTEM 2023-06-01 06:03:48.000000
0       -       944     wininit.exe     /SYSTEM 2023-06-01 06:03:50.000000
0       -       1016    services.exe    /SYSTEM 2023-06-01 06:03:50.000000
0       -       88      lsass.exe       /SYSTEM 2023-06-01 06:03:50.000000
0       -       1164    svchost.exe     [redacted]      2023-06-01 06:03:50.000000
0       -       1192    WUDFHost.exe    /SYSTEM 2023-06-01 06:03:50.000000
0       -       1212    fontdrvhost.ex  Font Driver Host/UMFD-0 2023-06-01 06:03:50.000000
0       -       1316    svchost.exe     [redacted]      2023-06-01 06:03:50.000000
0       -       1368    svchost.exe     [redacted]      2023-06-01 06:03:50.000000
0       -       1576    svchost.exe     NT-AUTORITÄT/Lokaler Dienst     2023-06-01 06:03:50.000000
0       -       1584    svchost.exe     NT-AUTORITÄT/Lokaler Dienst     2023-06-01 06:03:50.000000
0       -       1600    svchost.exe     NT-AUTORITÄT/Lokaler Dienst     2023-06-01 06:03:50.000000
0       -       1608    svchost.exe     NT-AUTORITÄT/Lokaler Dienst     2023-06-01 06:03:50.000000
0       -       1736    svchost.exe     [redacted]      2023-06-01 06:03:50.000000
0       -       1744    svchost.exe     NT-AUTORITÄT/Lokaler Dienst     2023-06-01 06:03:50.000000
0       -       1828    svchost.exe     [redacted]      2023-06-01 06:03:50.000000
0       -       1920    IntelCpHDCPSvc  [redacted]      2023-06-01 06:03:50.000000
0       -       1948    svchost.exe     NT-AUTORITÄT/Lokaler Dienst     2023-06-01 06:03:50.000000
0       -       1956    svchost.exe     [redacted]      2023-06-01 06:03:50.000000
0       -       1972    svchost.exe     [redacted]      2023-06-01 06:03:50.000000
0       -       1980    svchost.exe     [redacted]r Dienst      2023-06-01 06:03:50.000000
0       -       1988    svchost.exe     [redacted]r Dienst      2023-06-01 06:03:50.000000
0       -       1680    svchost.exe     [redacted]r Dienst      2023-06-01 06:03:50.000000
0       -       2144    IntelCpHeciSvc  [redacted]      2023-06-01 06:03:50.000000
0       -       2260    svchost.exe     [redacted]      2023-06-01 06:03:50.000000
0       -       2348    svchost.exe     [redacted]r Dienst      2023-06-01 06:03:50.000000
0       -       2440    svchost.exe     [redacted]r Dienst      2023-06-01 06:03:51.000000
0       -       2448    svchost.exe     [redacted]      2023-06-01 06:03:51.000000
0       -       2456    svchost.exe     [redacted]      2023-06-01 06:03:51.000000
0       -       2512    svchost.exe     [redacted]      2023-06-01 06:03:51.000000
0       -       2520    svchost.exe     [redacted]r Dienst      2023-06-01 06:03:51.000000
0       -       2528    svchost.exe     [redacted]      2023-06-01 06:03:51.000000
0       -       2600    svchost.exe     [redacted]r Dienst      2023-06-01 06:03:51.000000
0       -       2672    dasHost.exe     [redacted]r Dienst      2023-06-01 06:03:51.000000
0       -       2796    svchost.exe     [redacted]      2023-06-01 06:03:51.000000
0       -       2816    svchost.exe     [redacted]      2023-06-01 06:03:51.000000
0       -       2884    igfxCUIService  [redacted]      2023-06-01 06:03:51.000000
0       -       2964    svchost.exe     [redacted]      2023-06-01 06:03:51.000000
0       -       2972    svchost.exe     [redacted]r Dienst      2023-06-01 06:03:51.000000
0       -       3036    svchost.exe     [redacted]r Dienst      2023-06-01 06:03:51.000000
0       -       3120    svchost.exe     [redacted]r Dienst      2023-06-01 06:03:51.000000
0       -       3196    svchost.exe     [redacted]      2023-06-01 06:03:51.000000
0       -       3284    svchost.exe     [redacted]r Dienst      2023-06-01 06:03:51.000000
0       -       3360    svchost.exe     [redacted]r Dienst      2023-06-01 06:03:51.000000
0       -       3496    PresentationFo  [redacted]r Dienst      2023-06-01 06:03:51.000000
0       -       3576    HP3DDGService.  [redacted]      2023-06-01 06:03:51.000000
```

Bild 55 Sessions_0

```
0       -       3648    svchost.exe                     2023-06-01 06:03:51.000000
0       -       3692    GoogleUpdate.e                  06:03:51.000000
0       -       3844    svchost.exe                     r Dienst     2023-06-01 06:03:51.000000
0       -       3852    svchost.exe                     2023-06-01 06:03:51.000000
0       -       3860    svchost.exe                     r Dienst     2023-06-01 06:03:51.000000
0       -       4104    svchost.exe                     2023-06-01 06:03:51.000000
0       -       4144    svchost.exe                     2023-06-01 06:03:51.000000
0       -       4228    svchost.exe                     2023-06-01 06:03:51.000000
0       -       4312    spoolsv.exe                     2023-06-01 06:03:51.000000
0       -       4372    svchost.exe                     r Dienst     2023-06-01 06:03:52.000000
0       -       4408    svchost.exe                     r Dienst     2023-06-01 06:03:52.000000
0       -       4428    svchost.exe                     2023-06-01 06:03:52.000000
0       -       4648    wlanext.exe                     2023-06-01 06:03:52.000000
0       -       4664    conhost.exe                     2023-06-01 06:03:52.000000
0       -       4836    coreServiceShe                  n    2023-06-01 06:03:52.000000
0       -       4960    uiWatchDog.exe                  2023-06-01 06:03:52.000000
0       -       4996    svchost.exe                     2023-06-01 06:03:52.000000
0       -       5004    svchost.exe                     2023-06-01 06:03:52.000000
0       -       5012    CxMonSvc.exe                    2023-06-01 06:03:52.000000
0       -       5020    CxUtilSvc.exe                   2023-06-01 06:03:52.000000
0       -       5028    svchost.exe                     2023-06-01 06:03:52.000000
0       -       5036    HotkeyService.                  2023-06-01 06:03:52.000000
0       -       5048    DpHostW.exe                     2023-06-01 06:03:52.000000
0       -       5068    svchost.exe                     r Dienst     2023-06-01 06:03:52.000000
0       -       5076    ibtsiva.exe                     2023-06-01 06:03:52.000000
0       -       5084    svchost.exe                     2023-06-01 06:03:52.000000
0       -       5092    pdf24.exe                       2023-06-01 06:03:52.000000
0       -       5104    SynTPEnhServic                  2023-06-01 06:03:52.000000
0       -       5112    conhost.exe                     2023-06-01 06:03:52.000000
0       -       3936    svchost.exe                     2023-06-01 06:03:52.000000
0       -       3304    svchost.exe                     r Dienst     2023-06-01 06:03:52.000000
0       -       4360    svchost.exe                     2023-06-01 06:03:52.000000
0       -       4460    PtSvcHost.exe                   2023-06-01 06:03:52.000000
0       -       4692    mDNSResponder.                  2023-06-01 06:03:52.000000
0       -       5140    svchost.exe                     2023-06-01 06:03:52.000000
0       -       5240    svchost.exe                     2023-06-01 06:03:52.000000
0       -       5256    XtuService.exe                  2023-06-01 06:03:52.000000
0       -       5500    svchost.exe                     2023-06-01 06:03:52.000000
0       -       5576    svchost.exe                     2023-06-01 06:03:52.000000
0       -       5648    PtWatchDog.exe                  2023-06-01 06:03:52.000000
0       -       5708    svchost.exe                     2023-06-01 06:03:52.000000
0       -       5776    HotKeyServiceU                  2023-06-01 06:03:52.000000
0       -       5864    svchost.exe                     2023-06-01 06:03:52.000000
0       -       5892    coreFrameworkH                  2023-06-01 06:03:52.000000
0       -       5912    LanWlanWwanSwi                  2023-06-01 06:03:52.000000
0       -       5956    conhost.exe                     2023-06-01 06:03:52.000000
0       -       6032    svchost.exe                     2023-06-01 06:03:52.000000
0               6084    hpqwmiex.exe                    2023 06 01 06:03:52.000000
0       -       5612    svchost.exe                     r Dienst     2023-06-01 06:03:52.000000
```

Bild 56 Sessions_1

```
0        -        6864    DpCardEngine.e                    2023-06-01 06:03:53.000000
0        -        7144    WmiPrvSE.exe                      2023-06-01 06:03:53.000000
0        -        7384    WmiPrvSE.exe                      2023-06-01 06:03:53.000000
0        -        8020    svchost.exe                       2023-06-01 06:03:55.000000
0        -        8124    svchost.exe                       2023-06-01 06:03:55.000000
0        -        7632    svchost.exe                   r Dienst     2023-06-01 06:03:55.000000
0        -        8524    unsecapp.exe                      2023-06-01 06:03:56.000000
0        -        9548    svchost.exe                       2023-06-01 06:03:57.000000
0        -        9940    svchost.exe                       2023-06-01 06:03:58.000000
0        -        10128   SearchIndexer.                    2023-06-01 06:03:58.000000
0        -        10764   svchost.exe                   r Dienst     2023-06-01 06:03:59.000000
0        -        11468   GoogleCrashHan                    2023-06-01 06:04:01.000000
0        -        11488   GoogleCrashHan                    2023-06-01 06:04:02.000000
0        -        11988   svchost.exe                       2023-06-01 06:04:03.000000
0        -        12172   TmsaInstance64                    2023-06-01 06:04:06.000000
0        -        12252   AMSPTelemetryS                    2023-06-01 06:04:06.000000
0        -        11364   SecurityHealth                    2023-06-01 06:04:10.000000
0        -        12572   svchost.exe                       2023-06-01 06:04:12.000000
0        -        12648   DrSDKCaller.ex                    2023-06-01 06:04:12.000000
0        -        12656   conhost.exe                       2023-06-01 06:04:12.000000
0        -        13700   svchost.exe                       2023-06-01 06:04:23.000000
0        -        5304    armsvc.exe                        2023-06-01 06:05:57.000000
0        -        8928    HPSupportSolut                    2023-06-01 06:05:58.000000
0        -        6208    IAStorDataMgrS                    2023-06-01 06:06:01.000000
0        -        2488    jhi_service.ex                    2023-06-01 06:06:01.000000
0        -        3948    LMS.exe WORKGRO               3-06-01 06:06:01.000000
0        -        10404   SgrmBroker.exe                06:06:01.000000
0        -        10856   svchost.exe                       2023-06-01 06:06:02.000000
0        -        13968   svchost.exe                   r Dienst     2023-06-01 06:06:02.000000
0        -        7080    svchost.exe                   r Dienst     2023-06-01 06:06:02.000000
0        -        2180    WUDFHost.exe                  06:06:04.000000
0        -        1232    svchost.exe                   06:08:51.000000
0        -        6016    svchost.exe                       2023-06-01 06:08:51.000000
0        -        9856    svchost.exe                       2023-06-01 06:14:10.000000
0        -        14288   audiodg.exe                   r Dienst     2023-06-01 06:17:30.000000
1        -        936     smss.exe                      06:03:50.000000
1        -        952     csrss.exe                     06:03:50.000000
1        -        1040    winlogon.exe                  06:03:50.000000
1        -        1220    fontdrvhost.ex                FD-1 2023-06-01 06:03:50.000000
1        -        1448    dwm.exe /SYSTEM               .000000
1        -        3392    sihost.exe                        2023-06-01 06:03:51.000000
1        -        3452    svchost.exe                       2023-06-01 06:03:51.000000
1        -        3588    svchost.exe                       2023-06-01 06:03:51.000000
1        -        3784    taskhostw.exe                     2023-06-01 06:03:51.000000
1        -        3808    MicTray64.exe                     2023-06-01 06:03:51.000000
1        -        3824    QLBController.                06:03:51.000000
1        -        4260    ctfmon.exe                        2023-06-01 06:03:51.000000
1        -        4728    igfxEM.exe                        2023-06-01 06:03:52.000000
1        -        5444    SynTPEnh.exe                      2023-06-01 06:03:52.000000
1        -        5816    SynTPEnh.exe                  06:03:52.000000
1        -        6948    sacpl.exe                     06:03:53.000000
1        -        8136    userinit.exe                  06:03:55.000000
1        Console  8164    DPAgent.exe                       2023-06-01 06:03:55.000000
```

Bild 57 Sessions_2

1	Console	8184	explorer.exe	[redacted]	2023-06-01 06:03:55.000000
1	-	7628	SmartAudio3.ex	[redacted]	2023-06-01 06:03:55.000000
1	-	7844	SynTPHelper.ex	[redacted]	2023-06-01 06:03:55.000000
1	-	8684	svchost.exe	[redacted]	2023-06-01 06:03:56.000000
1	Console	8972	DpAgent.exe	[redacted]	2023-06-01 06:03:56.000000
1	-	9128	taskhostw.exe	[redacted]	2023-06-01 06:03:57.000000
1	-	9240	unsecapp.exe	[redacted]	2023-06-01 06:03:57.000000
1	-	9284	StartMenuExper	[redacted]	2023-06-01 06:03:57.000000
1	-	9660	RuntimeBroker.	[redacted]	2023-06-01 06:03:58.000000
1	-	9756	HPHotkeyNotifi	[redacted]	2023-06-01 06:03:58.000000
1	-	10052	SearchApp.exe	[redacted]	2023-06-01 06:03:58.000000
1	-	4936	RuntimeBroker.	[redacted]	2023-06-01 06:03:58.000000
1	-	11604	RuntimeBroker.	[redacted]	2023-06-01 06:04:02.000000
1	-	12284	PhoneExperienc	[redacted]	2023-06-01 06:04:06.000000
1	-	7780	RuntimeBroker.	[redacted]	2023-06-01 06:04:09.000000
1	-	11484	smartscreen.ex	[redacted]	2023-06-01 06:04:10.000000
1	Console	11688	SecurityHealth	[redacted]	2023-06-01 06:04:10.000000
1	-	12332	IAStorIconLaun	[redacted]	06:04:11.000000
1	Console	12356	Greenshot.exe	[redacted]	2023-06-01 06:04:11.000000
1	-	12748	uiSeAgnt.exe	[redacted]	06:04:12.000000
1	Console	12856	pdf24.exe	[redacted]	2023-06-01 06:04:13.000000
1	Console	13144	PtSessionAgent	[redacted]	2023-06-01 06:04:13.000000
1	Console	13252	OneDrive.exe	[redacted]	2023-06-01 06:04:14.000000
1	-	4688	ONENOTEM.EXE	[redacted]	06:04:15.000000
1	-	12700	Microsoft.Shar	[redacted]	06:04:16.000000
1	-	2008	SystemSettings	[redacted]	2023-06-01 06:04:43.000000
1	-	2004	ApplicationFra	[redacted]	2023-06-01 06:04:43.000000
1	-	5252	UserOOBEBroker	[redacted]	2023-06-01 06:04:44.000000
1	-	5880	FileCoAuth.exe	[redacted]	2023-06-01 06:04:44.000000
1	-	13616	msedge.exe	[redacted]	06:04:44.000000
1	-	9792	ShellExperienc	[redacted]	2023-06-01 06:04:49.000000
1	-	10436	RuntimeBroker.	[redacted]	2023-06-01 06:04:50.000000
1	Console	13368	IAStorIcon.exe	[redacted]	2023-06-01 06:05:11.000000
1	-	11512	svchost.exe	[redacted]	2023-06-01 06:05:34.000000
1	-	9064	TextInputHost.	[redacted]	2023-06-01 06:05:36.000000
1	-	3460	Start.exe	[redacted]	06:06:59.000000
1	-	14256	PortableAppsPl	[redacted]	06:07:00.000000
1	-	6908	HPSF.exe	[redacted]	06:07:52.000000
1	Console	11088	DontSleepPorta	[redacted]	2023-06-01 06:08:12.000000
1	Console	8900	DontSleep_x64_	[redacted]	2023-06-01 06:08:13.000000
1	Console	12340	WINWORD.EXE	[redacted]	2023-06-01 06:14:20.000000
1	-	11732	firefox.exe	[redacted]	06:19:35.000000
1	-	3696	dllhost.exe	[redacted]	2023-06-01 06:19:38.000000
1	-	14996	cmd.exe KLPC118/	[redacted]	23-06-01 06:19:50.000000
1	-	14564	conhost.exe	[redacted]	2023-06-01 06:19:50.000000
1	-	10104	winpmem_mini_x	[redacted]	2023-06-01 06:21:20.000000
N/A	-	2736	MemCompression	- 2023-06-01	06:03:51.000000

Bild 58 Sessions_3

7 Bilderverzeichnis des Anhangs

8 Verzeichnis der Abkürzungen

DDoS ..... Distributed Denial of Service
DLL ..... Dynamic Link Library
EXE ..... executable
GB ..... Gigabyte
GUI ..... Graphical User Interface
HTTP ..... Hypertext Transfer Protocol
IP ..... Internet Protokoll
MuiCache ..... Multilingual User Interface Cache
OS ..... Operating System
PID ..... Prozess-ID
Pstree ..... Process Tree
QR-Code ..... Quick-Response-Code
RAM ..... Random-Access Memory
SMTP ..... Simple Mail Transfer Protocol
TCP ..... Transmission Control Protocol
USB ..... Universal Serial Bus
USBPcap ..... Universal Serial Bus Packet Capture
VM ..... Virtuelle Maschine
ZIP ..... von englisch zipper ‚Reißverschluss'

9 Selbstständigkeitserklärung

Hiermit erkläre ich, dass ich die hier vorliegende Arbeit selbstständig, ohne unerlaubte fremde Hilfe und nur unter Verwendung der in der Arbeit aufgeführten Hilfsmittel angefertigt habe.

[redacted]

Ort, Datum **(Unterschrift)**