

Vergleich und Analyse des privaten Modus verschiedener Browser

Computer-Forensik und Vorfallsbehandlung

Carl Schünemann

Christoph Sell

29.08.2025

Inhaltsverzeichnis

1	Einleitung	1
2	Theoretischer Hintergrund	4
2.1	Private Browsing	4
2.2	Angreifermodell	6
2.3	Private Browsing Artefakte	8
3	Ziel der Arbeit	13
4	Methodik	16
4.1	Preparation Stage	16
4.1.1	Konfiguration der Versuchsumgebung	16
4.1.2	Browserauswahl	17
4.1.3	Browsing Szenario	17
4.2	Acquisition Stage	17
4.3	Analysis Stage	18
4.3.1	White-Box Analyse	18
4.3.2	Black-Box Analyse	20
5	Ergebnisse	23
5.1	Firefox	23
5.2	Tor	27
5.3	Chrome	28
5.4	Brave	28
6	Vergleich der Browser	29
7	Diskussion	30
8	Fazit	31
	Literaturverzeichnis	32
	Literatur	32

1 Einleitung

Steigende Beliebtheit private Browsing: [11] ■ Die Verwendung von PB wurde als die beliebteste Form der Online-Privatsphäre weltweit identifiziert. ■ Aufgrund der gestiegenen Sensibilität und Öffentlichkeit für den Schutz der Privatsphäre und die Regulierung des eigenen digitalen Fußabdrucks im Internet werden PB-Technologien wahrscheinlich häufiger auf den Geräten der Nutzer eingesetzt. ■ Auch wenn es schwierig ist, endgültige Nutzungsstatistiken für solche Aktionen zu erstellen, bietet der Konsens über den Online-Datenschutz einen Einblick. Im Jahr 2016 wurde die Verwendung eines PB-Fensters als die weltweit beliebteste Form der Online-Datenschutzmaßnahme identifiziert [1]. Allein in den USA nutzen Berichten zufolge rund 33 % der Nutzer ein PB-Fenster, wobei über 70 % zugeben, ihren Internetverlauf zu löschen [2]. - Eine umfassende Studie von Montasari und Peltola (2015) ergab, dass der Erfolg des privaten Modus bei verschiedenen Browsern sehr unterschiedlich ist

Vermeintliche Privatheit beim Browsen: [19] > Verschlüsselung ■ Datenschutz und Datenverwendung sind Hauptbedenken der Internetnutzer geworden [5]. ■ Fragen wie welche Daten von Unternehmen genutzt werden, mit wem sie geteilt werden und wie wertvoll sie sind, sind heute wichtige Themen. ■ Daher versuchen Benutzer, sich so weit wie möglich zu schützen, insbesondere durch Begrenzung der Datenweitergabe. ■ Lösungen wie Verschlüsselung auf HTTP-Ebene [6] und auf DNS-Ebene [7,8] sind Standard geworden und werden den Großteil des Datenverkehrs in den nächsten Jahren abdecken. ■ Sie können jedoch nur End-to-End-Konversationen verschlüsseln, d.h. IP- und TCP- oder UDP-Informationen sind immer noch verfügbar. > VPNs ■ Eine weitere beliebte Methode zum Schutz der Privatsphäre und zur Vermeidung von Datenverwendung ist die Verwendung von Virtual Private Networks (VPNs). ■ Obwohl VPNs immer beliebter geworden sind und die meisten von ihnen den IP-Verkehr verschlüsseln und tunneln können, kann der Datenverkehr tatsächlich am Endpunkt des VPNs überwacht werden. ■ Dies bedeutet, dass Akteure zwischen dem VPN-Servernetzwerk und dem Website-Server die Daten sehen und nutzen können. ■ Der VPN-Anbieter kann sogar noch weiter gehen, da er auch die Identität des Clients kennt. > Tor und Brave: 1. Die Endpunkte der verschlüsselten Verbindungen, die von Tor und Brave hergestellt werden, nicht vollständig verschlüsselt sind. Daher können einige Informationen, wie z.B. die IP-Adresse des Benutzers, an den letzten Servern in der Kette sichtbar sein. 2. Einige Tor-Ausgangsknoten haben in der Vergangenheit die Aktivität ihrer Benutzer ausspioniert, um Daten zu sammeln und möglicherweise zu verkaufen. 3. Obwohl die Verwendung von Brave und Tor dazu beitragen kann, dass Benutzer online nicht nachverfolgt werden, werden sie nicht vor Verfolgung durch andere Methoden wie Standortverfolgung oder Geräte-Fingerprinting geschützt. 4. Schließlich können auch andere Schwachstellen in der Implementierung oder Konfiguration von Tor oder Brave dazu führen, dass Daten durchsickern und somit die Privatsphäre der Benutzer kompromittiert wird.

Immer mehr Kriminelle im Internet [13]: > Das Internet und seine Nutzer wachsen ständig, aber auch die Anzahl organisierter Verbrechen und illegale Aktivitäten nehmen zu.

“Webbrowser immer beliebter bla bla ...“ [12] > Webbrowser sind heutzutage ein wichtiger Werkzeug für Online-Aktivitäten wie Online-Banking, Online-Shopping und soziale Netzwerke.

Immer mehr Internet-Nutzer:[12] ■ Im Jahr 2019 gab es laut [13] fast 4,5 Milliarden Internetnutzer.

Zunehmende Bestrebungen nach Privatheit erschwert forensische Ermittlungen [16] > Zunehmende Verwendung von verschlüsselten Daten in der Dateispeicherung und Netzwerkkommunikation erschwert Ermittlungen. > Besonders schwierig ist das Tor-Protokoll, das sich auf den Schutz der Privatsphäre des Nutzers konzentriert. > Tor-Browser hinterlässt digitale Artefakte, die von Ermittlern genutzt werden können.

Motivation Portable Browser [8] ■ Die Beliebtheit von tragbaren Webbrowsern nimmt aufgrund ihrer bequemen und kompakten Natur sowie des Vorteils, dass Daten einfach über einen USB-Stick gespeichert und übertragen werden können, zu. ■ Entwickler arbeiten an Webbrowsern, die tragbar sind und zusätzliche Sicherheitsfunktionen wie den privaten Modus-Browsing, eingebaute Werbeblocker usw. bieten. ■ Die erhöhte Wahrscheinlichkeit, tragbare Webbrowser für schädliche Aktivitäten zu nutzen, ist das Ergebnis von Cyberkriminellen, die der Ansicht sind, dass bei der Verwendung von tragbaren Webbrowsern im privaten Modus keine digitalen Fußabdrücke hinterlassen werden. ■ Das Forschungspapier zielt darauf ab, eine vergleichende Studie von vier tragbaren Webbrowsern, nämlich Brave, TOR, Vivaldi und Maxthon, zusammen mit verschiedenen Speichererfassungstools durchzuführen, um die Menge und Qualität der aus dem Speicherauszug wiederhergestellten Daten in zwei verschiedenen Bedingungen zu verstehen, nämlich wenn die Browser-Tabs geöffnet und geschlossen waren, um forensische Ermittler zu unterstützen.

Private Browsing Motivation und Ausnutzen von Kriminellen: [15] ■ Webbrowser werden täglich genutzt, um verschiedene Online-Aktivitäten durchzuführen. ■ Webbrowser speichern eine große Menge an Daten über Benutzeraktivitäten, einschließlich besuchter URLs, Suchbegriffen und Cookies. ■ Private Browsing-Modi wurden entwickelt, um Benutzern das Surfen im Internet zu ermöglichen, ohne Spuren zu hinterlassen. ■ Dies kann von Kriminellen ausgenutzt werden, um ihre Aktivitäten zu verschleiern. ■ Experimente werden auf jeder Browser-Modus durchgeführt, um zu untersuchen, ob sie Spuren auf der Festplatte oder im Arbeitsspeicher hinterlassen.

Motivation Private Browsing mit Portablen Browsern: [18] ■ Das Internet ist ein unverzichtbares Werkzeug für alltägliche Aufgaben. ■ Neben der üblichen Nutzung wünschen sich Benutzer die Möglichkeit, das Internet auf private Weise zu durchsuchen. ■ Dies kann zu einem Problem führen, wenn private Internetsitzungen vor Computerermittlern verborgen bleiben müssen, die Beweise benötigen. ■ Der Schwerpunkt dieser Forschung liegt darauf, verbleibende Artefakte aus privaten und portablen Browsing-Sitzungen zu entdecken. ■ Diese Artefakte müssen mehr als nur Dateifragmente enthalten und ausreichend sein, um eine positive Verbindung zwischen Benutzer und Sitzung herzustellen. ■ In den letzten 20 Jahren ist das Internet für alltägliche Aufgaben, die mit stationären und mobilen Computergeräten verbunden sind, drastisch unverzichtbar geworden. ■ Benutzer wünschen sich neben der üblichen Internetnutzung auch Privatsphäre und die Möglichkeit, das Internet auf private Weise zu durchsuchen. ■ Aus diesem Grund wurden neue Funktionen für das private Browsen entwickelt, die von allen gängigen Webbrowsern unterstützt werden. ■ Unsere Forschung konzentriert sich auf die Entdeckung von Informationen von lokalen Maschinen, da die meisten Computeruntersuchungen auf der Suche und Beschlagnahme von lokalen Speichergeräten beruhen. ■ Artefakte aus privaten und portablen Browsing-Sitzungen wie Benutzernamen, elektronische Kommunikation, Browsing-Verlauf, Bilder und Videos können für einen Computerermittler signifikante Beweise enthalten. ■ Wir

werden auch flüchtige Daten analysieren, die in einer gängigen Incident-Response-Umgebung verfügbar wären.

Schwachstellen in Browsern, durch die Daten "lecken" [24] ■ Private browsing ist seit 2005 eine beliebte Datenschutzfunktion in allen gängigen Browsern. ■ Laut einer Studie (-> TODO: welche?) leiden alle Browser unter einer Vielzahl von Schwachstellen, von denen viele zuvor nicht bekannt waren. ■ Die Probleme werden hauptsächlich durch eine laxere Kontrolle von Berechtigungen, inkonsistente Implementierungen der zugrunde liegenden SQLite-Datenbank, die Vernachlässigung von Cross-Mode-Interferenzen und eine fehlende Beachtung von Timing-Angriffen verursacht. ■ Alle Angriffe wurden experimentell verifiziert und Gegenmaßnahmen vorgeschlagen.

Private Browsing Motivation und Ausnutzen von Kriminellen [21] ■ Fast alle Aspekte des Lebens nutzen bereits das Internet, um auf das Internet zugreifen zu können, wird ein Webbrowser verwendet. ■ Die Einführung des Internets hat das Leben der Menschen in vielen Bereichen verändert, darunter auch im Bereich der Kriminalität, insbesondere in der Verwendung von Webbrowser-Software für Transaktionen und Prozesse im Internet. ■ Webbrowser speichern normalerweise Informationen wie URL-Verlauf, Suchbegriffe, Passwörter und andere Nutzeraktivitäten. ■ Aus Sicherheitsgründen wurden einige Funktionen von Webbrowsern entwickelt, um den privaten Modus zu ermöglichen. ■ Leider wird diese Funktion von einigen skrupellosen Menschen für kriminelle Aktivitäten durch die Anti-Forensik genutzt, um digitale Beweise in kriminellen Fällen zu minimieren oder zu verhindern.

Auswirkung von Darknet und Tor auf Forensiker [20] ■ Personen, die Inhalte aus dem Darknet abrufen möchten, müssen nicht nur in einem regulären Browser Schlüsselwörter eingeben, sondern müssen es anonym über den TOR-Browser zugreifen, um ihre Identität wie IP-Adresse oder physische Lage zu verbergen. ■ Aufgrund dieser Tatsachen ist es für Strafverfolgungsbehörden oder digitale forensische Experten schwierig, den Ursprung des Datenverkehrs, den Standort oder die Eigentümerschaft eines Computers oder einer Person im Darknet zu lokalisieren. ■ Die Auswirkungen des Darknets traten auf, als das Federal Bureau of Investigation (FBI) im Oktober 2013 die Website Silk Road abschaltete, die ein Online-Schwarzmarkt und der erste moderne Darknet-Markt für den Verkauf illegaler Drogen war. ■ Silk Road war nur über das TOR-Netzwerk zugänglich und vom Mainstream-Web verborgen. ■ Da die meisten Darknet-Sites Transaktionen über anonyme digitale Währungen wie Bitcoin durchführen, die auf kryptografischen Prinzipien basieren, ist es für digitale forensische Experten sehr schwierig, solche Transaktionen zu verfolgen, da Benutzer und Dienste anonym sind. ■ Das Ziel dieser Arbeit besteht darin, digitale forensische Techniken zu diskutieren, um solche Darknet-Verbrechen zu behandeln.

2 Theoretischer Hintergrund

Einleitend werden Struktur, Motivation und die abgeleiteten Forschungsfragen diskutiert.

2.1 Private Browsing

Definition Web Browser: > [21] ■ Der Webbrowser ist eine Softwareanwendung zum Abrufen, Präsentieren und Durchsuchen von Informationsressourcen im Internet oder World Wide Web (WWW).
■ Eine Informationsquelle wird durch einen Uniform Resource Identifier (URI) identifiziert und kann Webseiten, Bilder, Videos oder andere Inhalte enthalten.

> [12] ■ Ein Webbrowser ist eine Software, die es Benutzern ermöglicht, das Internet über den von ihrem Dienstanbieter bereitgestellten Zugang zu nutzen. ■ Die bekanntesten Webbrowser sind Google Chrome, Mozilla Firefox, Microsoft Edge und Brave. ■ Webbrowser werden für alltägliche Aktivitäten wie das Anschauen von Videos, das Durchsuchen von Webseiten, das Posten von Bildern oder Videos in sozialen Medien und das Herunterladen und Hochladen von Dateien genutzt. ■ Browser-Modi: Es gibt zwei verschiedene Browser-Modi: den normalen Browser-Modus und den privaten Browser-Modus.

Definition „Normal Browsing“: > [12] ■ Der normale Browser-Modus speichert alle Browser-Aktivitäten wie Caches, Cookies, Suchbegriffe, Login-Daten und URL-Verlauf auf dem Computer. ■ Die Cookies speichern Details des Benutzers wie z.B. Browsing-Muster, die anzeigen können, welche Websites der Benutzer häufig besucht oder welche Videos er/sie regelmäßig ansieht.

Definition "Private Browsing": > [22] - Deshalb wurde eine neue Funktion in die Webbrowser aufgenommen, die den Internetnutzern eine größere Kontrolle über ihre Privatsphäre ermöglicht. Diese Funktion ist als "Private Browsing" bekannt und soll es den Nutzern ermöglichen, im Internet zu surfen, ohne Datenspuren auf ihrem Computer zu hinterlassen.

> [11] - Private Browsing"(PB) ist ein allgemeiner Begriff, der sich auf Mechanismen, die verhindern sollen, dass ein Nutzer Beweise für sein Web-Browsing-Verhaltens auf seinem lokalen Gerät gespeichert werden. - Von Anfang an muss betont werden, dass sich privates Surfen in diesem Zusammenhang nur auf Plattformen bezieht, die lokale Privatsphäre bieten, und dass diese von Anwendungen wie Tor (siehe <https://www.torproject.org/>) zu unterscheiden sind, die sich ebenfalls auf die Online-Privatsphäre konzentrieren, sowie von Einrichtungen, die die Verfolgung und Überwachung aus der Ferne verhindern, wie z. B. der Tracking Preference Expression des W3C (auch bekannt als "Do Not Track"). - Je nach Browser des Nutzers wird eine zugehörige PB-Funktion mit unterschiedlichen Begriffen bezeichnet: Inkognito-Modus in Chrome, InPrivate in Edge und dem inzwischen nicht mehr unterstützten Internet Explorer sowie ein "privates Fenster" in Firefox.

Geschichte Private Browsing: > [22] - Die ADbC-Funktion "Privater Browsing-Modus" wurde erstmals 2005 mit Apple Safari 2.0 eingeführt. Drei Jahre später folgte Google Chrome 1.0 (Inkognito). Später,

im Jahr 2009, führten Microsoft Internet Explorer 8 und Mozilla Firefox 3.5 ihre Versionen von privaten Browsing-Modi ein, die als InPrivate bzw. Private Browsing bekannt sind (Dan, 2010).

> [15] ■ Private Browsing-Modi haben je nach Browser unterschiedliche Namen, z.B. Incognito-Modus in Chrome, InPrivate Browsing in Internet Explorer, "Private Browsing" in Firefox und Safari. ■ erstmals 2005 von Apple Safari eingeführt, gefolgt von Google Chrome und Microsoft in 2008 und Mozilla in 2009.

Grund des privaten Modus: > [12] ■ Private Browsing Mode wurde entwickelt, um die Privatsphäre und Anonymität beim Surfen im Internet zu verbessern, indem keine Spuren und Informationen von Browsing-Aktivitäten hinterlassen werden. ■ Alle neuen Caches, die während des Surfens gespeichert wurden, werden entfernt, sobald der Browser geschlossen wird. ■ Jeder Webbrowser bietet einen privaten Browser-Modus mit unterschiedlichen Bezeichnungen an, wie InPrivate Browsing für Internet Explorer und Microsoft Edge, Incognito-Modus für Google Chrome und "Private Browsing" für Mozilla Firefox. > [1] zwei wesentliche Ziele des privaten Browsing: 1. (local) Besuchte Websites sollten im privaten Modus keine Spuren auf dem Computer des Benutzers hinterlassen. Wenn ein Familienmitglied den Browserverlauf überprüft, sollte keine Evidenz von im privaten Modus besuchten Websites gefunden werden können. 2. (website) Benutzer möchten möglicherweise ihre Identität vor den Websites, die sie besuchen, verbergen, indem sie es beispielsweise für Websites schwierig machen, die Aktivitäten des Benutzers im privaten Modus mit seinen Aktivitäten im öffentlichen Modus zu verknüpfen. Dies wird als Datenschutz vor einem Webangreifer bezeichnet. > [15] ■ Private Modus Browser sollten in der Lage sein, die von besuchten Websites hinterlassenen Artefakte auf dem Computer des Benutzers zu verhindern. ■ Browser sollten es Websites unmöglich machen, herauszufinden, ob ein bestimmter Benutzer sie zuvor besucht hat, indem sie verhindern, dass Websites die Aktivitäten von Benutzern im privaten und öffentlichen Modus verknüpfen.

Stakeholder Private Browsing: > Forensiker - [13] ■ Die Entwicklung von Datenschutzfunktionen in Browsern stellt eine Herausforderung für digitale Forensiker dar, die Beweismittel sammeln möchten, um Kriminelle zu überführen. - [11] ■ Durch die Möglichkeit des privaten Browsens besteht eine erhöhte Gefahr für illegale und schädliche Online-Aktivitäten. ■ Die meisten privaten Browsing-Modi sind so konzipiert, dass sie lokal privat sind und Daten, die auf das Surfverhalten des Benutzers hinweisen, nicht auf dem Gerät gespeichert werden. ■ Diese Handlungen können die Verfügbarkeit von Beweismaterial beeinträchtigen und stellen eine Herausforderung für Untersuchungen dar. - [11] ■ Private browsing (PB) ist eine Funktion, die seit langem auf dem Radar von forensischen Praktikern steht. ■ Risiko: PB kann dazu führen, dass potenziell beweiskräftiger Inhalt nicht auf einem lokalen Gerät gespeichert wird, was zu Untersuchungsbedenken führt. ■ PB selbst hat viele legitime Anwendungen und ist nicht per se anti-forensisch, kann aber mit anti-forensischer Absicht verwendet werden. ■ Fehlende Internetinhalte stellen ein Problem für Beweissammlung ■ Private Browsing-Modi sollten die Aktivität des Nutzers vor forensischen Tools verbergen

> Kriminelle: - [13] ■ Kriminelle nutzen vermehrt private Browser, um ihre Spuren zu verwischen und ihre illegalen Handlungen zu verbergen. ■ Cyberkriminelle nutzen Private Browsing-Modi, um digitale Spuren auf dem Gerät zu verwischen und forensische Ermittler mit leeren Händen dastehen zu lassen. > Nutzerperspektive: - [11] ■ Die Verwendung von PB wurde als die beliebteste Form der Online-Privatsphäre weltweit identifiziert. ■ Aufgrund der gestiegenen Sensibilität und Öffentlichkeit für den Schutz der Privatsphäre und die Regulierung des eigenen digitalen Fußabdrucks im Internet werden PB-Technologien wahrscheinlich häufiger auf den Geräten der Nutzer eingesetzt. ■ Auch wenn es schwierig ist, endgültige Nutzungsstatistiken für solche Aktionen zu erstellen, bietet der Konsens

über den Online-Datenschutz einen Einblick. Im Jahr 2016 wurde die Verwendung eines PB-Fensters als die weltweit beliebteste Form der Online-Datenschutzmaßnahme identifiziert [1]. Allein in den USA nutzen Berichten zufolge rund 33 % der Nutzer ein PB-Fenster, wobei über 70 % zugeben, ihren Internetverlauf zu löschen [2].

- [11] ■ Die PB-Technologie wird aufgrund der gesteigerten Sensibilität und öffentlichen Aufmerksamkeit für den Schutz der Privatsphäre voraussichtlich häufiger auf Geräten verwendet. - [22] In den letzten Jahren (2010) haben jedoch viele der bekannten Webbrowser-Hersteller ihre Besorgnis über die Privatsphäre der Nutzer beim Surfen im Internet verstärkt. - Tatsächliche Gründe: [15] in [1] Experiment von Aggarwal et al.: Werbung auf Ad-Netzwerken geschaltet wurde, um verschiedene Kategorien von Websites einschließlich Erwachsenen- und Geschenk-Websites zu bewerben, um die Nutzung des privaten Modus mit der Art der besuchten Website zu korrelieren. -> Browsing-Modus auf Erwachsenen-Websites beliebter war als auf Geschenk-Websites. > Herstellerperspektive: - [15] Angeblich lt. Hersteller: o Einkaufen von Überraschungsgeschenken auf einem Familien-PC o Planung von Überraschungspartys

Stakeholder Private Browsing: > "Forensischer Ermittler [15] ■ forensischer Ermittler kann forensische Browsing-Artefakte mit forensischen Tools und Techniken wiederherstellen > "Nutzer": - [22] > Tatsächlich ergab eine Studie, dass Private Browsing auf Websites für Erwachsene beliebter ist als auf Websites für den Geschenkekauf oder für Nachrichten. Dies deutet darauf hin, dass die Anbieter von Webbrowsern den Hauptnutzen dieses Tools möglicherweise falsch einschätzen, wenn sie es als ein Tool zum Kauf von Überraschungsgeschenken beschreiben (Aggarwal, Boneh, Bursztein, und Jackson, 2010). > "Browser Entwickler [13] Die Entwickler von Browsern haben den Mangel an Benutzerdatenschutz erkannt und einen privaten Browsermodus eingeführt, der das Schreiben von Browserdaten auf die Festplatte einschränkt oder idealerweise verhindert. - [22] Einem Artikel zufolge (Belani, Jones, 2005) behaupten die Hersteller all dieser Webbrowser, dass keine der besuchten Websites, Formularfelddaten, in die Adressleiste eingegebenen Adressen, besuchten Links und Suchanfragen auf dem lokalen Computer des Nutzers gespeichert werden (Brookman, 2010).

2.2 Angreifermodell

Definition Local Attacker nach [1]: - Z.B. Forensischer Prüfer - hat physischen Zugriff auf den Computer des Benutzers - versucht, auf dessen privaten Browserverlauf zuzugreifen. - beispielsweise ein Familienmitglied oder ein Freund sein, der den Computer des Benutzers nutzt, um auf dessen Browserverlauf zuzugreifen. - kann darauf installierte Programme verwenden, um Informationen zu sammeln. - hat keinen Zugriff auf die Maschine des Benutzers, bevor der Benutzer das private Surfen beendet hat. Ohne diese Einschränkung ist Sicherheit gegen einen lokalen Angreifer unmöglich. (z.B: Keylogger installieren, Benutzeraktionen aufzeichnen) - Durch die Beschränkung des lokalen Angreifers auf "forensische Untersuchungen nach dem Ereignis" kann man hoffen, Sicherheit zu gewährleisten, indem der Browser persistenten Zustandsänderungen während einer privaten Surfsitzung ausreichend löscht. - Der Angreifer wartet, bis der Benutzer den privaten Browsing-Modus verlässt, und erhält dann die vollständige Kontrolle über die Maschine. Dies bedeutet, dass der Angreifer auf forensische Daten angewiesen ist. - Während der aktiven Phase kann der Angreifer nicht mit Netzwerkelementen kommunizieren, die Informationen über die Aktivitäten des Benutzers im privaten Modus enthalten. Dies bedeutet, dass die Implementierung von Browser-seitigen Datenschutzmodi untersucht wird, nicht die serverseitigen Datenschutzmodi.

- Das Ziel des Angreifers besteht darin, für eine bestimmte Menge von HTTP-Anfragen, die er wählt, festzustellen, ob der Browser eine dieser Anfragen im privaten Browsing-Modus ausgeführt hat oder nicht. Wenn der lokale Angreifer dieses Ziel nicht erreichen kann, gilt die Implementierung des privaten Browsers als sicher. -> Local Attacker weiß, wonach er sucht!
- Es wird darauf hingewiesen, dass die Definition impliziert, dass der Angreifer nicht feststellen kann, welche Websites der Benutzer besucht hat oder was der Benutzer auf einer bestimmten Website getan hat. Darüber hinaus wird auf die Eigenschaften des privaten Browsers nicht formal eingegangen, wenn der Benutzer den privaten Browsing-Modus nie verlässt.

Problem: Local Attacker muss überarbeitet werden: [15] ■ Es wurde festgestellt, dass das Konzept des lokalen Angreifers nicht ausreichend untersucht wurde und dass neue Experimente durchgeführt werden müssen, um ein besseres Verständnis für das Phänomen zu erlangen und herauszufinden, wie sich diese Funktion auf digitale forensische Untersuchungen auswirken könnte.

Definition Web Attacker nach [1] - Z.B. ISP - versucht Online-Aktivitäten des Benutzers im privaten Modus zu verfolgen und zu identifizieren, um diese mit seinen Aktivitäten im öffentlichen Modus in Verbindung zu bringen. - durch den Einsatz von Tracking-Tools oder das Sammeln von Informationen über die IP-Adresse des Benutzers oder andere Identifikationsmerkmale erfolgen. ■ Kontrolliert die von Benutzer besuchten Websites und kann Informationen über Benutzeraktivitäten sammeln (-> z.B. ISP), aber nicht über den Computer des Benutzers. ■ Webseiten können auch verschiedene Browser-Funktionen nutzen, um Browser zu identifizieren und sie über Privatsphäre-Grenzen hinweg zu verfolgen. ■ Die Electronic Frontier Foundation hat eine Website namens Panopticlick (-> TODO: In Demo zeigen?) erstellt, die zeigt, dass die meisten Browser eindeutig identifiziert werden können, was die Ziele (1) und (2) des privaten Surfers in allen Browsern unterbricht.

Anti-Forensische Grundsätze bei Browserentwicklung, um sich gegen Web-Attacker zu schützen nach [1] ■ Browser haben drei Ziele, um die Privatsphäre der Benutzer zu schützen. o Ziel 1: Ein Benutzer, der im privaten Modus surft, soll nicht mit demselben Benutzer verknüpft werden können, der im öffentlichen Modus surft. o Ziel 2: Ein Benutzer in einer privaten Sitzung soll nicht mit demselben Benutzer in einer anderen privaten Sitzung verknüpft werden können. o Ziel 3: Eine Website soll nicht erkennen können, ob der Browser im privaten Modus ist. ■ Ziele (1) und (2) sind schwierig zu erreichen, da die IP-Adresse des Browsers von Webseiten genutzt werden kann, um Benutzer über private Browsing-Grenzen hinweg zu verfolgen. ■ Das Torbutton Firefox-Erweiterung (ein Tor-Client) macht große Anstrengungen, um Ziele (1) und (2) zu erreichen, indem es die IP-Adresse des Clients über das Tor-Netzwerk versteckt und Schritte unternimmt, um das Browser-Fingerprinting zu verhindern.

Beispiel: Web Attacker Angriffe: > IP-Angriffe [19] ■ Obwohl Nutzer Verschlüsselung oder VPNs nutzen, ist ihre Privatsphäre oft ungeschützt, da mehrere Domains gleichzeitig besucht werden oder IP-Adressen von Cloud-Providern geteilt werden. ■ Eine neue Methode zur Identifizierung von Web-Browsing wird vorgestellt, die nur auf den IP-Adressen basiert, mit denen der Nutzer verbunden war, ohne DNS Reverse-Resolution durchzuführen. ■ Diese IP-Adresse-Sequenz wird in verschiedene Deep Learning Modelle eingespeist, um die tatsächlich besuchte Website zu identifizieren. ■ Untersucht wurden auch andere Faktoren wie Abhängigkeit vom DNS-Server, Genauigkeit bei Top-Domains, Datenverstärkung durch Paket-Sampling-Simulation, Auswirkungen auf Paket-Sampling und Skalierbarkeit der Methode. ■ Mit nur 10% der Pakete konnte die besuchte Website mit einer Genauigkeit und F1-Score von 94% bis 95% identifiziert werden. > ISP als „Web attacker“, um Kundenaktivität zu verfolgen [1] ■ ISP können unsere Ergebnisse nutzen, um den Datenverkehr ihrer Kunden zu identifizieren. ■ Dies ermöglicht

ISP, Daten für Marketingzwecke zu monetarisieren, sofern sie anonymisiert und mit Zustimmung der Kunden erfolgt. ■ ISP müssen jedoch darauf achten, wer Zugriff auf Netzwerkverkehrsdaten hat. ■ Das Weitergeben dieser Daten an Dritte kann zu potenziellen Datenschutzverletzungen bei Kunden führen. ■ Hauptaufgabe ist eigentlich einfach, aber es können viele Komplikationen auftreten ■ Hauptproblem ist das sogenannte "verwickelte Netz" ■ Beim Verbinden mit einer Website muss der Webbrowser eine Kaskade von Verbindungen zu anderen Websites öffnen ■ Grund dafür sind Bilder, Anzeigen, Banner, JavaScript-Bibliotheken, Social-Media-Links und vieles mehr

2.3 Private Browsing Artefakte

TODO: Common vs Uncommon Locations hier ansprechen

Residuale Daten > [12] ■ Überraschenderweise besteht der private Browser in Chrome und Firefox aus wenigen residuellen Daten, die jedoch Beweise für Interessen wie Suchbegriffe, E-Mail-IDs und Passwörter liefern können ■ Residuale Daten sind Daten, die von einem Gerät entfernt wurden, aber immer noch aufgespürt werden können. ■ Diese Daten können mithilfe spezieller Tools, meist in Dateiüberresten oder lokalen Ordnern, identifiziert werden. ■ Beispiele für residuale Daten sind Link-Dateien, Log-Dateien, Registry-Dateien, Prefetch-Dateien und Browser-Verlaufsdaten. ■ Digitale Forensik kann solide elektronische Beweise aus solchen Überresten und Artefakten sammeln, um sie in Gerichtsverfahren zu verwenden.

Browser Artefakte: > [12] ■ Jeder Browser hat unterschiedliche Artefakte im RAM des Geräts gespeichert ■ Im normalen Browsing-Modus werden die Browsing-History-Details des Benutzers vor und nach dem Löschen des Verlaufs im Speicher gespeichert ■ Benutzeraktivitäten und Daten beim Surfen können in normalen Browser-Modi wie Cookies, Caches, Downloads, Verlauf, anderen sensiblen Daten und temporären Dateien verfolgt und gespeichert werden, was digitalen Forensikern bei der Suche nach Beweisen hilft.

> [13] ■ Browser speichern eine Vielzahl von Nutzerdaten, die von besuchten URLs bis zu Benutzer-namen und Passwörtern reichen ■ Das Wissen, dass Browser private Surfdaten preisgeben, ist schon etwas, aber der Standort dieser Artefakte ist von größter Bedeutung

> [22] - Webbrowser sind so konzipiert, dass sie eine Vielzahl von Informationen über die Aktivitäten ihrer Benutzer aufzeichnen und speichern können. Dazu gehören Caching-Dateien, besuchte URLs, Suchbegriffe, Cookies und andere. - Diese Dateien werden auf dem lokalen Computer gespeichert und können von jeder Person, die denselben Computer verwendet, leicht aufgerufen und abgerufen werden. Dies macht es auch für forensische Prüfer relativ einfach, die Internet-Aktivitäten eines Verdächtigen in Fällen zu untersuchen, in denen fragwürdige Websites besucht oder kriminelle Handlungen über das Internet durchgeführt wurden.

> [3] ■ Bestimmte Datentypen aus HTTP-Protokoll-Transaktionen oder skriptgesteuerten Aktionen in HTML-Seiten werden separat im Dateisystem gespeichert und führen zu unterschiedlichen Datenbankeinträgen: Cookies, Web Storage und Indexed Database Storage.

Private Browsing Artefakte: > [1] 1. Änderungen, die von einer Website ohne jegliche Benutzerinteraktion initiiert werden. Beispiele hierfür sind das Setzen eines Cookies, das Hinzufügen eines Eintrags zur Verlaufsdatei und das Hinzufügen von Daten zum Browser-Cache. 2. Änderungen, die von einer Website

initiiert werden, aber eine Benutzerinteraktion erfordern. Beispiele hierfür sind das Generieren eines Client-Zertifikats oder das Hinzufügen eines Passworts zur Passwortdatenbank. 3. Änderungen, die vom Benutzer initiiert werden. Zum Beispiel das Erstellen eines Bookmarks oder das Herunterladen einer Datei. 4. Nicht benutzerspezifische Zustandsänderungen, wie das Installieren eines Browser-Patches oder das Aktualisieren der Phishing-Blockierungsliste. ■ "geschützte Aktionen- Browser Artefakt, dass beim Verlassen des privaten Surfens gelöscht werden muss

Wie entstehen "Leckagen" von privaten Browsing Artefakten? [11] 1. Ein Fehler im Design und in der Entwicklung des Browsers 2. Das Betriebssystem übernimmt mehr Kontrolle über den Browser als es sollte, was dazu führt, dass Daten von außen abgegriffen werden

Common Locations: > Ort der Browserartefakte ("common locations") ausführlich beschrieben in: [5]

> [12] ■ Die Artefakte von Webbrowsern werden in bestimmten Ordnern im Betriebssystem gespeichert. ■ Die genaue Lage variiert je nach Browser, die Dateiformate bleiben jedoch gleich. ■ Es ist wichtig zu wissen, wo die Dateien gespeichert sind, um sie während des normalen und privaten Browsing-Modus untersuchen zu können. ■ Tabelle 6 zeigt die Standorte der Artefakte von Google Chrome wie Verlauf, Caches und Cookies. ■ Tabelle 7 stellt die häufigsten Standorte von Firefox-Artefakten wie Cookies, Cache, Verlauf und Lesezeichen vor. ■ Alle Änderungen in Firefox, wie Lesezeichen, installierte Erweiterungen und gespeicherte Passwörter, werden im Profildrucker gespeichert. ■ Wie in der Tabelle gezeigt, werden Cookies in cookies.sqlite gespeichert, während Cache-Dateien im cache2-Ordner zu finden sind. ■ Alle heruntergeladenen Lesezeichen, Dateien und der Verlauf werden in places.sqlite gespeichert. ■ Mögliche Informationen, die aus der Browser-Forensik extrahiert werden können, sind Browsing-Verlauf, Cache, Cookies, Lesezeichen und Download-Liste.

> [21] ■ Digitale Beweise in einem Webbrowser umfassen mindestens Caches, Verlauf, Cookies, Download-Dateilisten und Sitzungen. ■ Zumindest ein Minimum an digitalen Beweisen aus einem Webbrowser ist sehr wichtig und wird von Ermittlern genutzt, um einen Fall bei Internetnutzung zu analysieren.

Gründe für Browser-Artefakte bei Private Browsing: [11] > Fehler im Design und Entwicklung des Browsers -> führt dazu, dass Daten von innen nach außen durchsickern, d. h. Browser ist schuld > Betriebssystem übernimmt mehr Kontrolle über den Browser als es sollte, was dazu führt, dass Daten von außen abgegriffen werden, d. h. Betriebssystem ist schuld

Definition private Browsing Artefakt: =====
Strings, die Aktionen des Browsing-Protokolls zugeordnet werden können: Keywords, URLs, HTML-Fragmente, E-Mail-Adressen, Betreffzeilen etc.

Warum Computer-Forensik: [13] ■ Die Untersuchung von digitalen Beweisen ist von großer Bedeutung, um Straftäter zu identifizieren und zur Rechenschaft zu ziehen.

Definition digitale Forensik [12] ■ Digitale Forensik konzentriert sich auf die Wiederherstellung von Speichermedien, um digitale Beweise für Cybercrime-Untersuchungen zu sammeln. ■ Die gewonnenen Beweise müssen jedoch in ihrem Originalzustand erhalten bleiben, um vor Gericht zulässig zu sein. ■ Der Prozess der Erwerbung, Untersuchung, Analyse und Berichterstattung von digitalen Beweisen muss forensisch einwandfrei durchgeführt werden. ■ Daher müssen Ermittlungsteams sich an die Phasen der digitalen Forensik halten, die auf weit verbreiteten Standards basieren. ■ Digitale Forensik-Investigatoren verlassen sich auf die Artefakte, die aus diesen Browser-Records auf dem Gerät zurückbleiben, und

verwenden forensische Techniken, um die Artefakte zu erfassen, um Beweismittel zu finden. ■ Die Artefakte werden im Computer-Speicher gespeichert, nachdem alle Browser-Verläufe, Caches und Cookies gelöscht wurden, was es für digitale forensische Gutachter einfach macht, die Daten zu extrahieren.

Definition Browser Forensics > [13] ■ Web-Browser-Forensik sammelt und identifiziert Beweise und Informationen im Zusammenhang mit einem Verbrechen aus wiederhergestellten Browser-Sitzungen - Forensische Analyse des Webbrowsers beinhaltet die Wiederherstellung von Browsing-Artefakten, die Informationen über die Online-Aktivitäten eines Verdächtigen offenbaren. - Browser-Forensik wird für Ermittler immer wichtiger, da Suchverlauf, Download-Aktivität und Seitenaufrufe das Verständnis für das kriminelle Motiv verbessern können.

Ziel digitale Forensik [12] ■ Digitale Forensik hat das Ziel, verwendbare Beweise für Computerkriminalität zu sammeln. ■ Cyberkriminalität wie Hacking, betrügerische Transaktionen und Diebstahl geistigen Eigentums erhöhen den Bedarf an digitaler Forensik, um auf Cyberkriminalität mit einem digitalen Gerät zu reagieren. (2022) A Comparative Analysis of Residual Data

Live-Forensik: unterschiedliche Definitionen in Literatur > Live-Forensik als "moderner Trend" der Computer-Forensik [7] Im Gegensatz zur traditionellen (toten) digitalen Forensik wird bei der Live-Forensik versucht, flüchtige Daten aufzubewahren und Gegenmaßnahmen für verschlüsselte Dateien auf einem Live-System zu ergreifen. > [9]: TODO! > [12] ■ „Live Forensics“ wird auch als „Live System Acquisition“ bezeichnet. ■ Diese Methode wird angewendet, wenn das System in Betrieb ist, um potenzielle Artefakte im flüchtigen Arbeitsspeicher (RAM) zu finden, die als Beweismittel genutzt werden können. ■ Viele Spuren von Computer-Sitzungen und Artefakte sind nur im flüchtigen Speicher zu finden und können nicht von externem Speicher aus ausgelesen werden. ■ Die Daten können jedoch nicht gesammelt werden, da sie verloren gehen, sobald das System gestoppt oder neu gestartet wird. ■ Die RAM-Daten müssen daher mit besonderen Verfahren behandelt werden, um ihre Integrität und Zuverlässigkeit während der Analyse zu gewährleisten. ■ „Live Forensics“ ist nützlich, um auch Ereignisse zu untersuchen, die nur während der Nutzung des Systems aufgetreten sind, und um Daten effizient im flüchtigen Arbeitsspeicher zu speichern. ■ Digitale Forensik kann dazu genutzt werden, die Gültigkeit von Beweismitteln bei Gerichtsverfahren zu untersuchen. ■ Nach der Identifikation und Sammlung von potenziellen Beweismitteln wird in den meisten Fällen eine exakte Kopie der Daten erstellt, um sie als Backup zu nutzen und Veränderungen zu vermeiden. ■ Es gibt zwei Arten von forensischen Techniken, um Speicherabbilder zu erstellen: „Dead Forensics“ und „Live Forensics“. ■ Bei „Live Forensics“ hingegen wird das System im laufenden Betrieb untersucht, was oft schwieriger ist, aber auch wertvolle Informationen liefern kann. > [21] ■ Forensische Untersuchung eines Systems, während es in Betrieb ist ■ Daten gehen verloren, wenn das System heruntergefahren oder neu gestartet wird ■ Verwendung bei flüchtigem Speicher wie RAM ■ RAM-Erfassung durch RAM-Forensik-Tool ■ Ziel ist es, den normalen Betrieb des Systems nicht zu beeinträchtigen ■ Live Forensics liefert wichtige Informationen für die Analyse ■ Analyse von digitalen Beweisen aus dem RAM mit Memory Analysis Tool. ■ Eine Lösung für dieses Problem ist die Live-Forensik, um Daten aus dem Arbeitsspeicher zu extrahieren, bevor sie gelöscht werden. ■ Diese Forschungsmethode wird verwendet, um Webbrowser im Allgemeinen und insbesondere tragbare Webbrowser zu analysieren.

Beispiele Live-Forensik > [24] ■ Volatiler Speicher (Memory Inspection) kann eine wichtige Informationsquelle für forensische Untersuchungen sein ■ DNS-Caching ist eine Bedrohung für private Browsing: Diese Schwachstelle entsteht, weil das Betriebssystem DNS-Anfragen des Browsers im Cache speichert, unabhängig davon, ob der Browser im privaten Modus ist oder nicht > [13] ■ Registry

Snapshots: Um Veränderungen im System-Registry aufgrund der Browserinstallation zu verfolgen, wurde Regshot verwendet, um vor der Installation einen Snapshot der Registry aufzunehmen. - Ein zweiter Snapshot wurde nach der Installation des Browsers aufgenommen und mit dem ersten verglichen. - Regshot generiert einen Bericht über die Ergebnisse, der die neuen Dateien und Ordner zeigt, die dem Registry-Schlüssel hinzugefügt wurden.

Vorteile Live-Forensik > In Literatur bekannt: Die meisten Informationen im RAM > [11] ■ Die meisten Daten können in den RAM-Speichergeräten des Betriebssystems gefunden werden. > [16] ■ Da es wahrscheinlich ist, dass RAM-Aufnahmen Inhalte der Browsing-Session (z.B. durch Caching) aufzeigen, wurde dies in das Projekt aufgenommen, insbesondere da Warren (2017) dies aufgrund von Zeitbeschränkungen nicht tun konnte. > [16] ■ Live Analyse während der Laufzeit einer Anwendung ist besonders vorteilhaft, um zu verstehen, wie das Betriebssystem und die Anwendung interagieren. ■ Live Analyse kann potenziell mehr Informationen zur Browsing-Session liefern, da die Designbemühungen des Tor-Projekts darauf abzielten, Schreibzugriffe auf die Festplatte zu vermeiden.

Herausforderungen von Live-Forensik = Kontaminieren von Beweismitteln [7] Die größten Herausforderungen während des Datenerfassungsprozesses sind: Datenveränderung und Abhängigkeit vom Betriebssystem des verdächtigen Systems; wenn der Erfassungsprozess die Daten verändert, werden die Gerichte die Daten als forensisch untauglich abweisen

Definition Dead Forensik: > [12] ■ Bei „Dead Forensics“ wird der Computer oder das Gerät, das untersucht werden soll, zuerst heruntergefahren, bevor das Speicherabbild erstellt wird. > [11] - Physische Speichererfassung ist nicht übliche Praxis und in den meisten Fällen nicht verfügbar > [9]: TODO! > [13] - Oft einzige Option: Analysen von Festplatten-Images von ausgeschalteten Geräten - Gründe für „einzige Option“: o Verzögerungen bei der Bearbeitung o Personalmangel bei den forensischen Untersuchern - also unrealistisch und unpraktisch, beschlagnahmte Geräte eingeschaltet zu lassen. - Ausschalten eines Geräts reduziert Risiko einer Datenänderung (versehentlich oder absichtlich) - isoliert es vom Netzwerk, um etwaige Versuche, es ferngesteuert zu löschen, zu verhindern, unter anderem. > [12] -> widersprüchlich? ■ System wird heruntergefahren, bevor das Speicherabbild erstellt wird. ■ Volatile Dateien gehen verloren: versteckte Dateien, ausgetauschte Dateien, Web-Aktivitäten, Artefakte und Log-Dateien ■ Das Ziel ist es, eine genaue Kopie des nichtflüchtigen Speichers zu erstellen, bevor das System heruntergefahren wird, um die Originalität der Beweismittel zu erhalten.

Beispiele Dead Forensik: > Stichwortsuche in Festplatten-Images nach herunterfahren [24] > Timestamps von Dateien [24] > SQLite Datenbanken [24] > Unallocated Space [24] > Registry-Hives auf Festplatte, z.B. NTUSER.DAT [24]

Probleme bei Dead Forensik > [7]: TODO!

Wann Live-, wann Dead Forensik? [12] ■ Die Wahl der Methode hängt von der Art der Untersuchung und der verfügbaren Zeit ab. ■ Das Ziel ist es, eine genaue Kopie des Speichers zu erstellen, um die Integrität der Beweise zu bewahren und das Risiko von Veränderungen zu minimieren.

Definition: Darknet Forensik: [20] ■ Motivation Darknet Forensik: o Terroristen, Kriminelle, extremistische Gruppen und Hassorganisationen nutzen das Darknet, um Cybercrime zu begehen. o Die Verwendung von TOR und Bitcoin auf dem Darknet erschwert die Verfolgung von Straftaten durch digitale Forensik-Experten. o Die vorgeschlagenen forensischen Techniken können digitale Forensik-Experten helfen, mit Cybercrime-Fällen im Zusammenhang mit dem Darknet umzugehen. ■

Darknet-Forensik sind in zwei Kategorien unterteilt: 1. TOR-Browser-Forensik: ■ vier Möglichkeiten zur Extraktion von TOR-Browser Artefakten: RAM-Forensik, Registry-Änderungen, Netzwerk-Forensik und Datenbank 2. Bitcoin-Transaktions-Forensik: Extrahieren von forensischen Artefakten aus Bitcoin-Wallet-Anwendung

3 Ziel der Arbeit

Wichtig: White-Box Ansatz gemäß local Attacker in [1] - Das Ziel des Angreifers besteht darin, für eine bestimmte Menge von HTTP-Anfragen, die er wählt, festzustellen, ob der Browser eine dieser Anfragen im privaten Browsing-Modus ausgeführt hat oder nicht. Wenn der lokale Angreifer dieses Ziel nicht erreichen kann, gilt die Implementierung des privaten Browsers als sicher. - Local Attacker weiß, wonach er sucht!

Forensiker müssen Funktionsweise von Private Browsing kennen [11] ■ Die Kenntnis der Erfolgsrate der PB-Technologie unterstützt die Strafverfolgungsbehörden bei digitalen Untersuchungen von Internetinhalten ■ Internetbeweise sind oft entscheidend für Untersuchungen ■ Bestimmung des Umfangs und des Erfolgs von PB-Technologie unterstützt die Strafverfolgungsbehörden bei digitalen Untersuchungen von Internetinhalten ■ Durch die Bestimmung des Umfangs und des Erfolgs von PB-Technologie können sie unnötige Datenverarbeitung und Zeitverschwendung vermeiden, die Untersuchungseffizienz verbessern und sicherstellen, dass keine wichtigen Inhalte übersehen werden. Daher können diese Punkte dazu beitragen, die Effektivität und Effizienz von Untersuchungen zu verbessern, insbesondere in Fällen, in denen Vor-Ort-Triage stattfindet oder in denen eine SHPO angeordnet wurde. Drei Punkte wichtig: ■ Wenn der Verdacht besteht, dass PB stattgefunden hat, hilft es zu wissen, wie erfolgreich die PB-Funktion eines bestimmten Browsers ist, um unnötige Datenverarbeitung (und Zeitverschwendung) zu vermeiden, wenn tatsächlich keine Browserdaten auf einem Gerät vorhanden sind. ■ Die Kenntnis darüber, wo PB möglicherweise Informationen zu Browsing-Sitzungen preisgibt, verbessert die Effizienz von Untersuchungen und verhindert, dass wichtige Inhalte übersehen werden. Dies ist besonders wichtig bei Vor-Ort-Triage, wie sie in einigen Fällen mit einer SHPO angeordnet wird.

Ziel der Arbeit: ===== - Welche Browsing Artefakte werden beim private Browsing auf einem Rechner hinterlassen, welche zeigen, dass eine Browsing Aktion vom Browser durchgeführt wurde? - Das heißt: o Es wird nach Browsing Artefakten gesucht, welche die Zuordnung „Durchgeführte Browsing Aktion“ <-> Browser ermöglichen o Vor, während und nach private Browsing Session nach Browsing Artefakten suchen, welche dem Browser zugeordnet werden können - Negativbeispiel: Suche in Hexdump nach im Browser gesuchtem String nicht als Beweis ausreichend, dass private Browsing Artefakte gefunden wurde. - Kategorisierung nach [18]: > Browsing History > Usernames/Email Accounts > Images

=> Thematisiert in [18]: o It appeared that the overall best way to recover residual data was to obtain the evidence from RAM or working memory, o Kritik: Oft nur String Match in RAM-Hex als Nachweis für PB genannt -> ausreichend? (Evtl. Gegenexperiment mit Editor)

Warum muss String-Artefakt Browser zugeordnet werden können? [12] ■ Die Artefakte, die von den Browsing-Aktivitäten eines Kriminellen zurückgelassen wurden, können mit forensischen Tools extrahiert werden, um die Untersuchung des Ermittlers zu unterstützen. ■ Die erlangten Beweise müssen vor Gericht zugelassen werden, insbesondere digitale Beweise, da sie ohne ordnungsgemäße Verfahren leicht manipuliert werden können. ■ Es gibt bestimmte Merkmale von digitalen Beweisen, die Gerichte

nach folgenden Kriterien akzeptieren: 1. Durchsuchungsbefehle - Beweise, die ohne Genehmigung erlangt wurden, können vor Gericht nicht anerkannt werden. 2. Berichte - Alle Prozesse, Werkzeuge, Methoden, Techniken, spezifischen Zeit- und Datumsangaben sowie die Beweiskette müssen formell dokumentiert werden, um die Authentizität der digitalen Beweise vor Gericht zu demonstrieren und zu unterstützen. 3. Beweisauthentifizierung - Der ursprünglich erhaltene Beweis sollte durch Vergleich der Hash-Werte mit dem Kopiebeweis übereinstimmen. Der erworbene Beweis muss unverändert bleiben, um die Gerichte mit genauen Informationen zu überzeugen. Gerichte akzeptieren Kopien von Beweisen, wenn der ursprüngliche Beweis verloren gegangen oder zerstört wurde, die Kopie jedoch noch intakt ist.

Ziele anderer Arbeiten: ===== > [12] - Die Art der extrahierbaren Daten zu untersuchen - den Unterschied zwischen privatem und normalem Surfen zu vergleichen - zu analysieren, welcher Browser die vollständigeren residualen Daten liefert. > [15] ■ ob bestimmte Arten von Browser-Daten gefunden werden konnten (Webseiten, Verlauf, Download-Verlauf, besuchte URLs und Suchbegriffe) > [21] ■ Das Ziel dieser Studie ist es, eine Rahmenbedingung für die Analysephasen des Webbrowsers im privaten Modus und Anti-Forensik vorzuschlagen, um eine effektive und effiziente forensische Untersuchung zu ermöglichen. ■ Die Studie nutzt Live-Forensik, um detailliertere Informationen über den Computer zu erhalten, während er noch in Betrieb ist, und eignet sich daher besser für die schnelle Datenerfassung in Echtzeit. > [24] ■ umfassende Analyse der privaten Browsing-Funktion in den vier beliebtesten Webbrowsers (IE, Firefox, Chrome und Safari) vorgestellt. > [12] - digitalen Forensikern helfen, Artefakte von Geräten zu verfolgen, die Live-Memory-Erfassung verwenden > [16] - Methodik entwerfen, um folgende Fragen zu beantworten: 1. Kann Tor den Benutzer schützen, indem es Beweise für dessen Nutzung aus dem RAM löscht, wenn die Browsing-Sitzung geschlossen wird? 2. Kann die Tor-Nutzung zu vier Schlüsselmomenten erkannt werden: während das Browser-Fenster geöffnet ist, nach Schließen des Browser-Fensters, nach dem Löschen des Installationsverzeichnis/zugehöriger Dateien und nach dem Ausloggen des Benutzers? 3. Können Dateien aus dem Browsing-Protokoll in der Live-Forensik mit Tor 7.5.2 wiederhergestellt werden, der zum Zeitpunkt der Schreibens aktuellsten Version? - Die Experimente wurden im mobilen Modus mit Tor wiederholt, d.h. von einem USB-Stick ausgeführt. (!!!) zu bestätigen, dass die Existenz und Nutzung des Tor-Browsers in Windows 10 nachweisbar ist. (!!!) nachweisen, dass Artefakte des Tor-Browsing-Protokolls auf dem Zielcomputer wiederhergestellt werden können. > [12] > In dieser Studie werden die residualen Daten zwischen Google Chrome und Mozilla Firefox Webbrowsers im normalen und privaten Browsermodus mithilfe eines forensischen Tools analysiert und verglichen. > [15] ■ In dem Projekt wurden die Effektivität der "privaten"Modus von vier weit verbreiteten Webbrowsers analysiert. > [24] ■ Ziel: Bewertung der Sicherheit des privaten Surfens in den Browsern Chrome, Safari, Firefox und IE ■ Die Autoren haben eine umfassende forensische Analyse durchgeführt, die sowohl Live-Memory-Analyse als auch Post-Mortem-Analyse umfasste. > [15] ■ Vier getestet: Firefox, IE, Safari und Chrome

Keine Ziele der Arbeit: ===== - Private Browsing Indicators": Entering/Leaving Private Browsing [18] - Zeigen, dass ein Browser gestartet/geschlossen wurde - Zeigen, dass ein Browser im privaten Modus gestartet wurde - Zeigen, wann ein Browser gestartet/geschlossen wurde - Browser-Erweiterungen: [24] > Browser-Erweiterungen und ihre Auswirkungen auf das private Surfen wurden in einer Studie von Aggarwal et al. Im Jahr 2010 untersucht. -> Siehe Punkt „Add-Ons als Leck“ > Die Chrome-Erweiterung „Incognito Inspector“ kann im privaten Modus genutzt werden, um detaillierte Informationen über die Nutzeraktivitäten zu sammeln und in Echtzeit an einen Remote-Server zu senden. > Firefox-Erweiterungen sind standardmäßig im privaten Modus aktiviert und können genutzt werden, um Nutzeraktivitäten aufzuzeichnen. > Internet Explorer-Erweiterungen sind in der

Regel deaktiviert und erfordern die manuelle Aktivierung im privaten Modus. Die von den Autoren entwickelte Erweiterung funktionierte jedoch nicht, da sie aufgrund eingeschränkter Privilegien nicht auf die BHO-Klasse zugreifen konnte - [1] > Unterschiedliche Handhabung durch Browser: Gefährliche Leckage für private Browsing Artefakte > Entwickler von Add-Ons haben möglicherweise den privaten Browsing-Modus bei der Entwicklung ihrer Software nicht berücksichtigt, und ihr Quellcode wird nicht derselben rigorosen Überprüfung unterzogen wie die Browser selbst. > Gegenmaßnahme: [1] ■ Es wurde eine Firefox-Erweiterung namens ExtensionBlocker entwickelt, um unsichere Erweiterungen im privaten Modus zu blockieren

4 Methodik

> Validation Stage (= Kapitel „Vergleich der Browser“)

Warum Methodik? > [1] Aufgrund der Komplexität moderner Browser ist eine systematische Methode erforderlich, um zu testen, ob der private Browsing-Modus ausreichend gegen die Bedrohungsmodelle aus Abschnitt 2 verteidigt. > [12] ■ Die Verfahren für die digitale Forensik für Browser-Forensik müssen angemessen befolgt werden, um dem Ermittler bei der Durchführung der Untersuchung zu helfen. Die Verfahren unterscheiden sich je nachdem, wie die Untersuchung durchgeführt werden soll. > [11] ■ Das Fehlen von Klarheit hat einen signifikanten Einfluss auf forensische Untersuchungen von Strafverfolgungsbehörden und deren Ansätze ■ Eine Kette von Beweisführung muss dokumentiert werden, um die Integrität und Zuverlässigkeit der Daten sicherzustellen. ■ Ein formaler forensischer Bericht wird dann vor Gericht präsentiert.

Bekanntes Computer Forensik Vorgehensmodell: [25]: Generic Model Computer Forensics Investigations (GCFIM) -> Daran orientieren sich alle in der Literatur

Phasen nach [15] ■ Die forensische Analyse erfolgt in zwei Phasen. 1. Zunächst wird die Analyse an sowohl "üblichen als auch ungewöhnlichen Speicherorten auf der Festplatte durchgeführt. 2. In der zweiten Phase wird der physische Arbeitsspeicher (RAM) untersucht.

Phasen nach [12]: ■ Es gibt verschiedene Modelle für digitale Forensik, die sich in ihren Phasen unterscheiden können. ■ Fünf Phasen sind besonders wichtig: Identifikation und Sammlung, Bewahrung, Erwerb, Analyse und Prüfung sowie Dokumentation. ■ In der Identifikations- und Sammelphase werden alle potenziellen Beweismittel identifiziert, gekennzeichnet und gesammelt, um sie in der nächsten Phase zu verwenden. ■ Beweismittel können z.B. Log-Dateien, temporäre Dateien, Netzwerkverbindungen, Browserverlauf und Cache sein. > Phasen: Preparation Phase o Versuchsplanung + Konfiguration der HW/SW + Durchführen des Experiments Acquisition Stage o Abbildung von der Festplatte (Static Forensics) und des RAMs (Live Forensics) Analysephase o Bilder der Speicherabbilder mit einem forensischen Tool untersuchen Validierungsphase o gefundenen Artefakte verglichen und dokumentiert

4.1 Preparation Stage

4.1.1 Konfiguration der Versuchsumgebung

VM Konfiguration

RAM: - Kaum Angaben in der Literatur: > [21]: 2 GB > [18]: 4 GB - Hier: 6 GB -> Ausblick: Kritik an Literatur, dass RAM-Größe kaum thematisiert wird, obwohl sie Auswirkungen auf Ergebnisse hat -> Siehe Kapitel X (TODO!)

Netzwerkeinstellungen: - TODO

Windows 10 Installation: - TODO

Tools auf VM: - Process Monitor - Regshot

Konfiguration des Analyse-Rechners

Volatility: Plugins-Liste: (Ähnlich zu [Hariharan] und [4]) - TODO

Autopsy: Evtl. hier Sleuthkit vs Autopsy thematisieren - TODO

Sonstige Tools: WinHex SQLite Viewer etc. - TODO

-> Evtl. am Schluss Tabelle mit allen Tool, Versionen und Plug-Ins

4.1.2 Browserauswahl

> Browserstudie [12] - Die Herstellerangaben unterschiedlicher Browser bzgl. Privatheit untersucht - Firefox 58.02: No Browsing History stored, No Cookies stored, No login Info stored, Tracking Protection Enabled: Disconnect, Download Files not Hidden - Chrome 63.0.3239: No Browsing History stored, No Cookies stored, No login Info stored, Tracking Protection Enabled: No, Download Files not Hidden

> design aim of Tor: [16] - preventing from writing to disk (Perry et al., 2018) - enabling secure deletion of the browser (Sandvik, 2013) (hier nicht relevant)

4.1.3 Browsing Szenario

- Wichtig für White-Box-Ansatz: Browsing Szenario ist bekannt - URL X ... (TODO!)

4.2 Acquisition Stage

> Browsing Szenario durchführen > Zeitpunkte von -> Orientieren an: [16] - RAM-Dumps - VM-Snapshots (nur letzter Snapshot ist Post-Mortem Forensik) - Process Monitor Logfiles - Registry Snapshots

- Warum Process Monitor während Browsing? o Während Browsing Szenario Filechanges untersuchen: DaemonFS set to monitor all activity within local hard drive[18]

- Registry: [21] ■ Das Windows-Registrierungsverzeichnis enthält viele Informationen zur Nutzung des Computers, Benutzerkonfigurationen, Anwendungen und Hardwaregeräte ■ Informationen im Registrierungsverzeichnis werden nach Ausführungsreihenfolge, Suchschlüsselwörtern, zuletzt aufgerufenen Ordnern, Anwendungsprotokollen und anderen Kategorien sortiert.

4.3 Analysis Stage

> Analysis Stage (= Kapitel „Results“) - Analyse der akquirierten Artefakte der vorherigen Phase: VM-Snapshots, RAM-Dumps, Process Monitor Logfiles und Registry Snapshots mit ggf. zusätzlichen Tools - Oberster Leitsatz dabei: gefundenes Artefakt muss eindeutig Browser zugeordnet werden können: Deshalb einfache Stringsuche in RAM mit WinHex ungenügend -> Hier evtl. negatives Beispiel zu Stringsuche einflechten

4.3.1 White-Box Analyse

Whitebox-Analyse: (gezieltes Suchen nach Dateien) [2] Definition: "White-Box"Computer Forensik bezieht sich auf eine forensische Untersuchungsmethode, bei der der forensische Analyst über umfassende Kenntnisse und Zugriff auf das untersuchte System verfügt. Im Kontext der Computerforensik bezieht sich "White-Box"darauf, dass der Analyst über volle Transparenz und Zugriff auf alle Informationen, Ressourcen und Artefakte des Systems verfügt.

Die "White-Box"Forensik kann verschiedene Techniken und Tools umfassen (z.B. Process Monitor, Regshot, Registry Explorer, Dekomprimierungstools), um Daten wiederherzustellen, gelöschte Informationen wiederherzustellen, Metadaten zu analysieren, Netzwerkaktivitäten zu überwachen und weitere forensische Analysen durchzuführen. Der Fokus liegt darauf, das System vollständig zu verstehen und alle relevanten Beweise zu sammeln.

Hier: In Orten gesucht, die 1. Process Monitor ermittelt hat und 2. in der Literatur vorgeschlagen wurden.

Definition: Common Location (= i.d.R. Installationsverzeichnisse der Browser) = „Bekannte Speicherorte“, z.B. bei Firefox - TODO: Quelle > Welche Dateien in Common Locations mit Process Monitor identifiziert > Wie haben sich Dateien verändert in verschiedenen Snapshots? > Was in Dateien gefunden? - Ziel: Befinden sich unter den Dateien, die ein Browser direkt auf die Festplatte schreibt private Browsing Artefakte? - Dateien sind Browserspezifisch, befinden sich in bekannten Pfaden. Beispiele: Datenbank-Dateien, Caches, temporäre Dateien. - String-Suche wäre nicht ausreichend, da Artefakte teilweise komprimiert (siehe .jsonlz4) - Beispiele: > Cache folder, Web history [15]

Schreiboperationen mit Process Monitor verfolgen

- Process Monitor: WriteFile Operationen von Browser - Vorgehen: (Siehe Aktivitätsdiagramm) o Basis = Process Monitor Logfile 1 und 2 o Processmonitor Filter: Browser-Prozess, Dateioperationen, nur WriteFile o Export als CSV o Datenaufbereitung in Excel o Irrelevante Spalten löschen: Time of Day (zeitl. Kontext nicht wichtig), Process Name (Da in Process Monitor bereits nach Namen gefiltert wurde -> Alle Prozesse haben gleichen Namen), Operation (Da in Process Monitor bereits nach Operation gefiltert wurde -> Alle Prozesse haben gleiche Operation „WriteFile“), Result, Detail o Gleiche Operationen (Duplikate) löschen o Neue Spalte mit Dateiendung -> Weiteres gruppieren, sortieren und analysieren ist browserspezifisch o Wenn Daten aufbereitet wurden: 1. Autopsy: Prüfen, ob Dateien noch in Snapshot Image vorhanden 2. Wenn ja, Dateien mit Autopsy extrahieren 3. Wenn nein, prüfen, ob Datei in RAM gecacht -> Hier beschreiben, wie mit Volatility filelist etc. Dateien

aus RAM wiederhergestellt werden können 4. Prüfen ob Browsing Artefakte in Dateien enthalten sind: Stringsuche nach Aktionen des Browsing-Protokolls

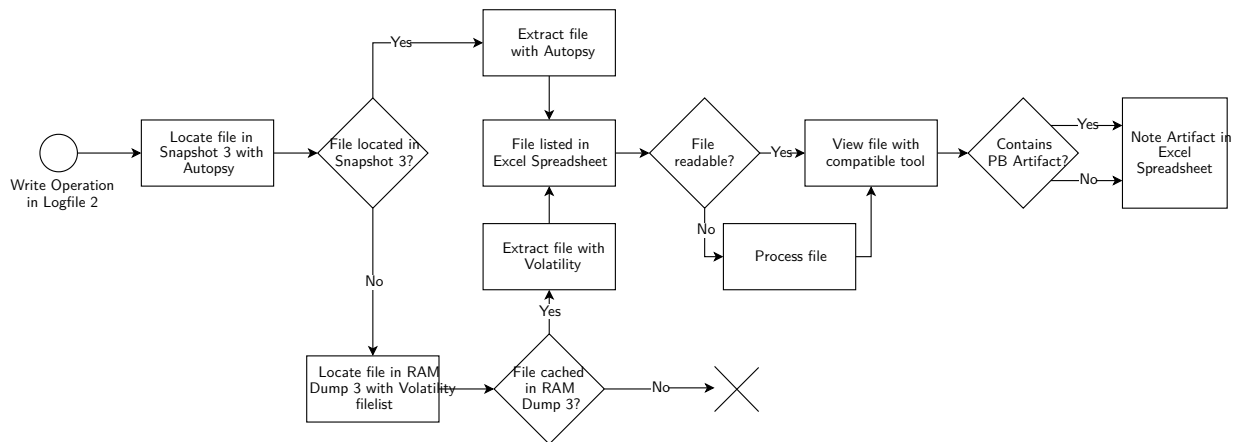


Abbildung 4.1: TODO: Process Monitor Write Operation to Excel Spreadsheet

SQLite-Datenbanken

- Gesondert betrachtet: Zeitlicher Vergleich von SQLite Datenbanken > Begründung: In Literatur ermittelt, dass SQLite DB von zentraler Bedeutung bei Browser History -> Hier wird i.d.R. Suchverlauf gespeichert > Zählt zu den wichtigsten "Common Locations" > Vorgehen: Siehe Aktivitätsdiagramm

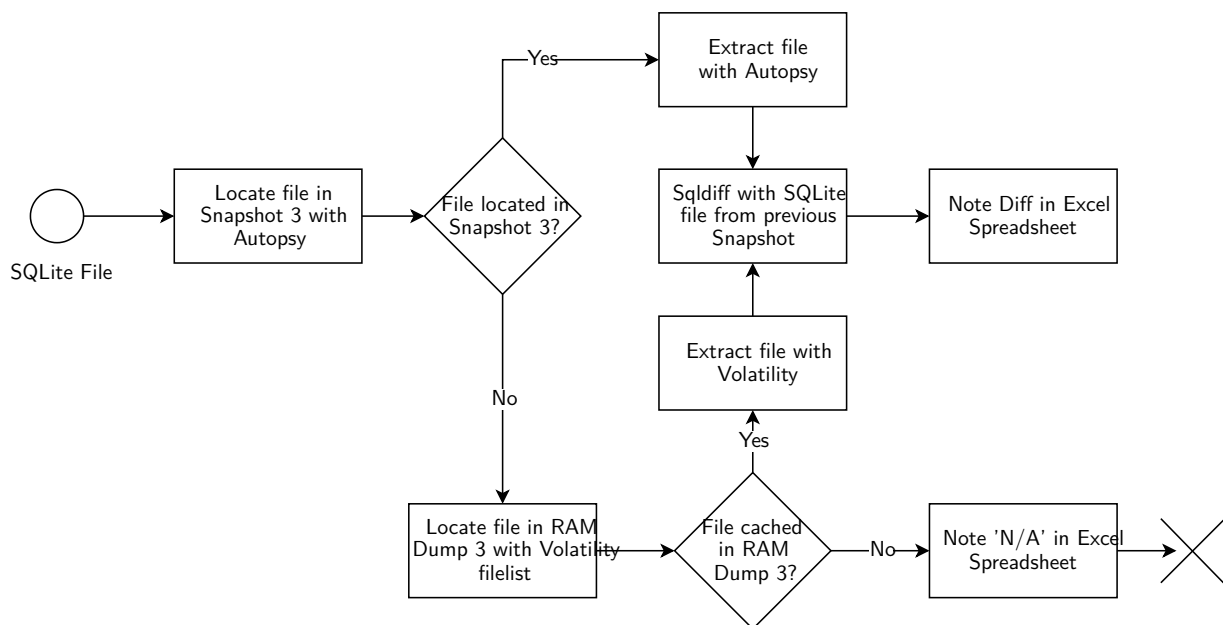


Abbildung 4.2: TODO: Process Monitor Write Operation to Excel Spreadsheet

Registry

- Registry: > Process Monitor: SetValue Operationen von Browser -> Values der Keys untersucht > Stringsuche in Registry Hives mit Registry Explorer (Siehe Liste) > Shellactivities-ähnliche Keys untersucht (Gesondert betrachtet wie SQLite DBs) - TODO: - Aktivitätsdiagramm? - Liste von bekannten Registry Hives - Screenshot Process Monitor? - Screenshot Registry Explorer?

4.3.2 Black-Box Analyse

Blackbox-Analyse: [2] (Stringsuchen im gesamten Image mithilfe von Tool) Definition: Auch "trriage-style keyword search"[11] genannt, = Durchsuchung des Beweismaterials ohne Vorwissen über Browserverhalten (d.h. welche Dateien geschrieben wurden) sowie ohne Vorverarbeitung der Dateien (z.B. Entpacken von Dateien). Stattdessen: Untersuchen der Images nur mittels vordefinierter Funktionen von Forensik-Tools "Triage", da dies schnelles erstes Mittel von Forensikern, um nach Acquisition Phase Ergebnisse zu erhalten

Hier entscheidend "Uncommon Locations": = „Unbekannte Speicherorte“, nur durch tiefgehende forensische Analyse entdeckt

- TODO: Quelle o Registry o Pagefile.sys o Unallocated Disk Space -> Suche nach „obfs4“ deckt Bridging IP-Adressen auf o Windows-Prefetching o Timestamps o \$MFT o \$Unalloc o \$LogFile o Favicons o etilqs o Manifest.json o slack space
- Beispiele in der Literatur: > "\$MFT", "\$LogFile", "Favicons", "etilqs", "Manifest.json", "pagefile.sys.", "unallocated space" and "slack space" [15]
- Ziel: Untypische Orte, wo private Browsing Artefakte gefunden werden können. Im - Unterschied zu Common Locations: Weitergreifendes Konzept, umfasst Dateien, die nicht von Browsern in bekannten Browser-Ordnern gespeichert werden, sondern auch Speicherorte wie RAM, Registry oder Caches des Rechners, wie - In Literatur ermittelt: für private Browsing drei uncommon Locations relevant: o Stichwortsuchen in kompletten Speicherabbildern: Festplatte (Common Location Browser-Pfade ausgenommen) + RAM -> Wichtig: String-Treffer muss Browser zugeordnet werden können -> Negativbeispiele: o [21]: in WinHex: URLs, Passwörter gefunden -> Wie wird URL Browser zugeordnet? Reicht gefundener String in RAM-Hex als Beweis aus? o [14] WinHex: email account can be retrieved, retrieves all URL histories including the directories visited by a user o [15] Firefox: URLs und Keywords als Strings in WinHex gesucht und gefunden o [15] Chrome: URLs und Keywords als Strings in WinHex gesucht und gefunden
- o In Literatur oft verwendet: Stichwortsuchen: > Autopsy Keyword-Suche außerhalb der Common Locations, in allen Partitionen ■ Definition der gesuchten Strings ■ Weiterführend: In Literatur nichts über verwendete Plugins gefunden. Hier: o Automatische Kategorisierung von Dateien o Timeliner-Plugin (Wenn verwendbar?) > RAM: Yarascan Treffer -> String Kontext ■ Definierte Yarasrules - TODO! ■ HTML-Fragmente: [22] We were also able to find blocks of HTML code that constructs Web sites we visited. ■ Image Carving: > Carved from Memdump [18] > Bildsuche mit: Griffeye's DI Analyze Pro with LACE plug-in [11]
- Windows: Prozess-Struktur im RAM: (-> TODO: Wo gefunden?) The EPROCESS data structure contains information about process instances, such as image name and ProcessID, the resources

allocated in terms of memory allocations (how much and where), types (private, mapped, shareable, etc.), memory protections (combinations of read, write, execute, and reserved), modules loaded, and pointers to ETHREADs and the process environment block.

Both EPROCESS and ETHREAD are considered opaque objects by Microsoft [28], inhibiting analysis; fortunately, third-party work has been done to understand these structures [29], [30]. Microsoft does provide symbol files¹, which help communicate the layout of data structures [31]. Indeed, Volatility uses these symbols for its own processing.

Included in EPROCESS, the ETHREAD object is an opaque structure which contains useful information about the stack. We calculated the size of a stack from the difference between its limit and base, both of which are attached to the ETHREAD.

Another member of the EPROCESS structure, the VAD tree, maps out the virtually allocated memory for a process [32]. VAD nodes refer to loaded modules (in the allocations in which they were referenced) and also have unique permission flags per node.

The PEB (process environment block) contains data about the number of heaps, which modules have been loaded into memory, and the command-line string that invoked the process [33]. The module list may not match the VAD tree's list exactly, the difference of these two sets indicating images of interest

In Literatur der Web Browser Forensik vorwiegend verwendet: - Autopsy Stichwort Suche nach PB Artefakten + Indizieren der Dateien durch Autopsy-PlugIns - Stichwortsuche in RAM mit Volatility Yarascan PlugIn. Vertiefende Untersuchung für jeden Yara-Rule-Treffer *** Hier werden Artefakte gefunden *** -> Flussdiagramm

Analyse mit Autopsy

Bei White-Box Analyse: Autopsy nur zur Dateixtraktion genutzt, hier: als konkretes forensisches Werkzeug Wichtig dabei: - Stichwortsuche -> TODO: Screenshot von Suchfunktion -> TODO: Liste von Strings - Nutzen der Plug-Ins

Analyse mit Volatility

Bei White-Box Analyse: RAM nur zur Dateixtraktion genutzt, hier: als konkretes forensisches Werkzeug

Wichtig: Auf Ziel der Arbeit verweisen: gefundenes PB Artefakt muss zwingend Browser zugeordnet werden können -> d.h. gefundener String des Browsing Protocols in Hex des RAM-Dumps reicht nicht als Beweis für gefundenes PB Artefakt aus. Stattdessen: gefundenes PB Artefakt im RAM muss Browser zugeordnet werden können -> Passendes Werkzeug = Volatility PlugIn "Yarascan" TODO: Definition Yarascan -> TODO: Auflistung der Yara-Rules -> Vorgehen: Siehe Baumdiagramm

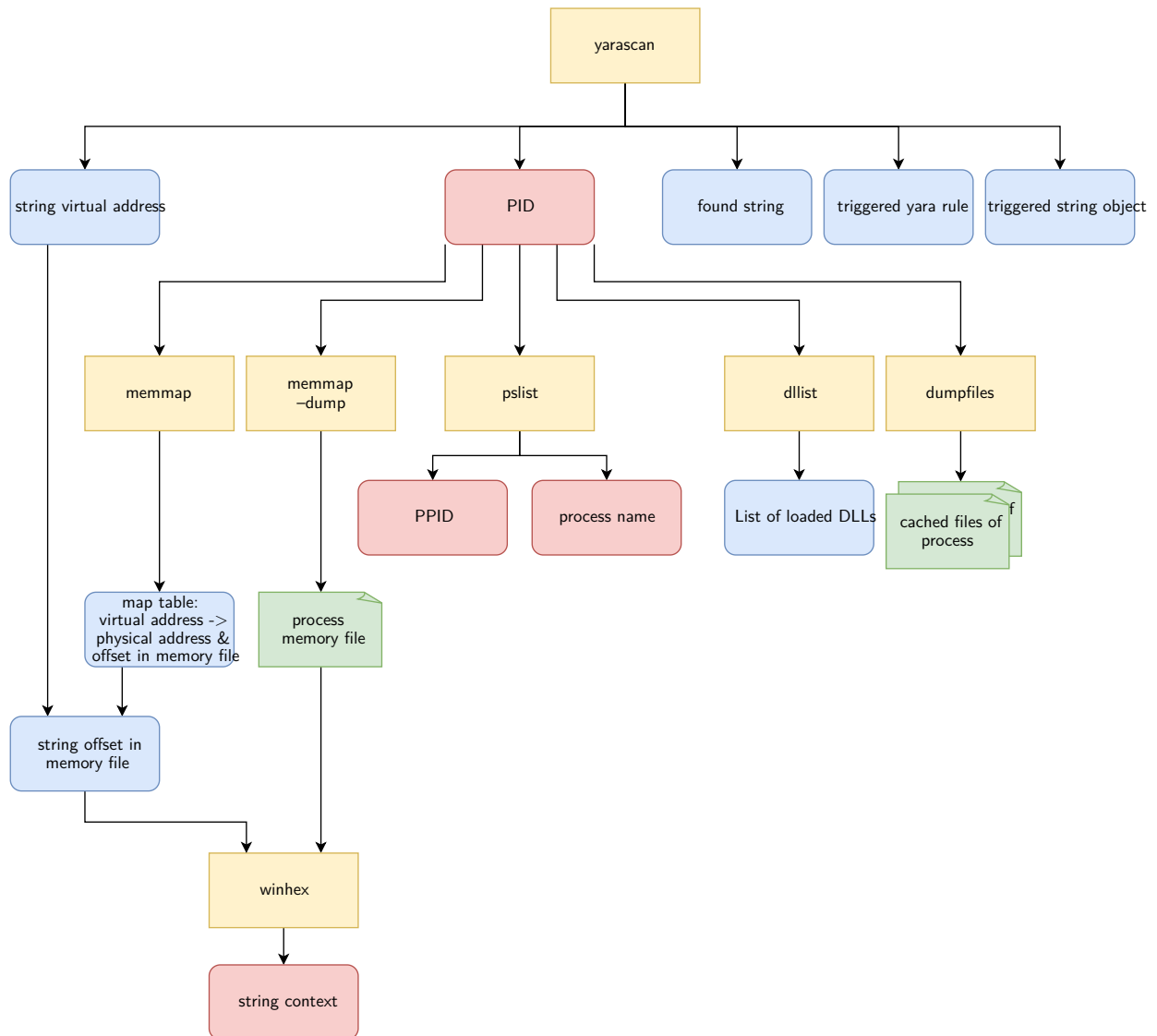


Abbildung 4.3: TODO: Process Monitor Write Operation to Excel Spreadsheet

5 Ergebnisse

= LÄNGSTES/AUSFÜHRLICHSTES KAPITEL!!!

Für jedes Unterkapitel gilt: > Erst allgemeines Vorgehen/Methodik definieren > Danach spezifisch für jeden Browser: Unterschied zwischen Snapshot-Zeitpunkten, insb. zwischen Live- und Dead-Forensik

5.1 Firefox

White-Box Analyse/Common Locations

Schreiboperationen mit Process Monitor verfolgen

Qualitative Analyse: o no traces were found in "common locations" [15] > "places.sqlite", "webappstore.sqlite", "sessionstore.bak", "search.json" and "nssckbi.dll" o Safebrowsing: Alle Dateien in /safebrowsing-updating/ nicht relevant. Dort nur .vlpset und .sbstore Dateien. Speichern 256-Bit Hash von URLs, die auf SafeSearch Blacklist stehen ■ Logfile 1 vs Logfile 2 o Cache-Dateien: drei Caches: startupCache, jumpListCache (beide enthalten Binärdateien ohne Browsing Artefakte) und cache2 (können mit MozillaCacheView untersucht werden, enthalten keine Browsing Artefakte) ■ Logfile 1 vs Logfile 2 o SQLite Datenbanken: Sqlite Dateien erst ohne WAL Dateien untersuchen, Danach mit sqlite3 Konsole: WAL in Datenbank schreiben mit: PRAGMA wal_checkpoint; places.sqlite besonders relevant, da dort Browser in public Modus Browsing URLs verwaltet (Am besten hier vergleich mit Public Browsing machen) > [5] for Mozilla Firefox, 7 database files were recovered: cookies.sqlite-shm, places.sqlite-shm, prefs.js etc. > [16] The two SQLite databases used by Firefox to track cookies and history (cookies.sqlite und places.sqlite) were both recoverable from the file system after deletion Ergebnisse stehen im Gegensatz zu [10] : o Chrome und Firefox: Einträge in places.sqlite + history.sqlite DB gefunden während PB! (Noch aktuell??) Sonderfall: SQLite DB-Crash [10] > WAL Files/Journal Files bei Crash gefunden -> Kann genutzt werden um zu beweisen, dass privater Browser genutzt wurde > Daher: WAL Rollback mit sqlite3 o Jsonlz4 & balkz4: Enthalten komprimierte Firefox-Sessions, jsonlz4 Dateien können mit Tool entkomprimiert werden: <https://www.jeffersonscher.com/ffu/scrounger.html>

Diagramme:

SQLite-Datenbanken

Diagramme:

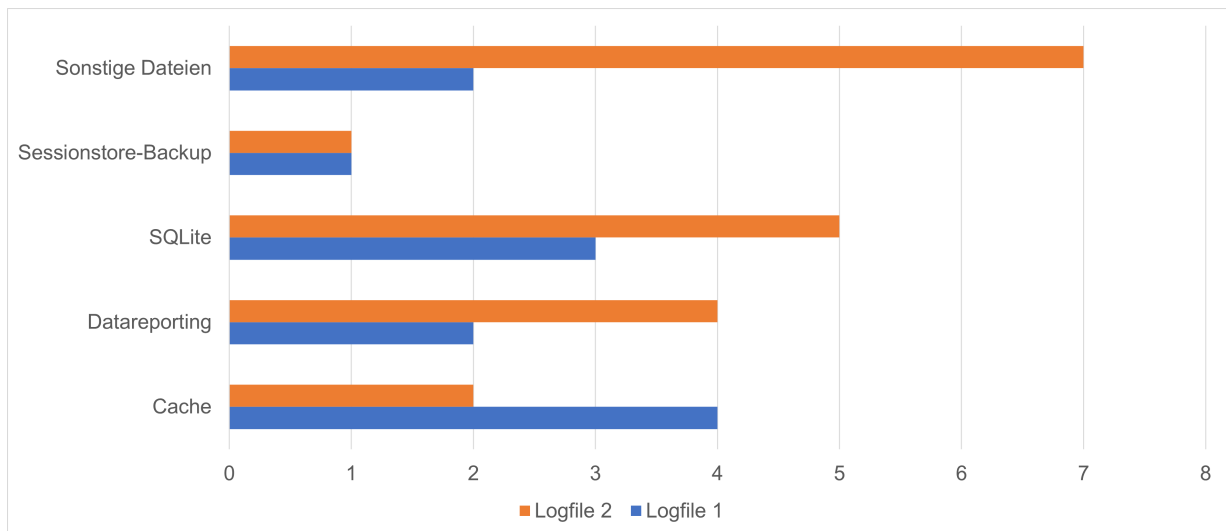


Abbildung 5.1: Comparison of found PB artifacts between RAM Dumps

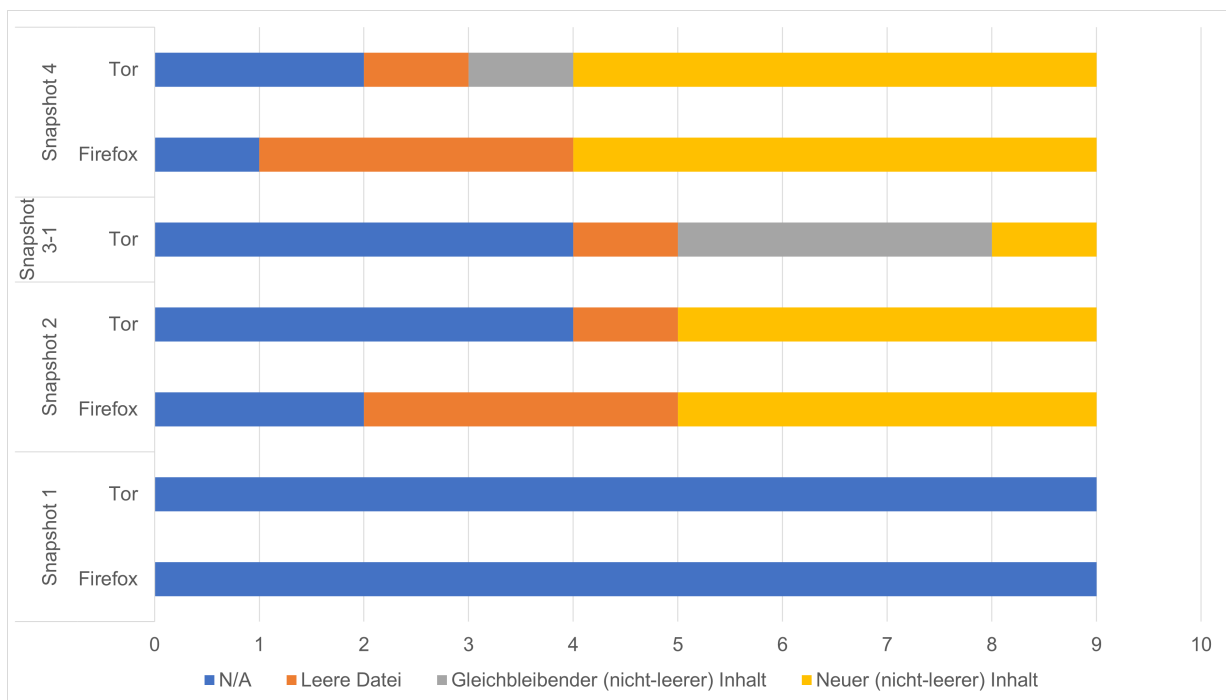


Abbildung 5.2: Comparison of found PB artifacts between RAM Dumps

Registry

> Auf Autor verweisen: angeblich in Shellactivities Ergebnisse. -> Nicht mehr vorhanden in aktueller Version (Verweis auf E-Mail) > Process Monitor/Regshot zeigen keine relevanten Key-Änderungen > [16]:

Autopsy Keyword Suche nach Suchbegriffen: Ergebnisse in %SystemRoot%Minidump NTUSER.DAT, ntuser.dat.LOG1 (a log of changes to NTUSER.DAT) > Zentral: shellactivities Key: NTUSER.DAT -> "shellactivities" key [16] > [21] Detection of registry changes helps to determine what the appropriate plugin is used to search for digital evidence using volatility memory forensic: - RegQueryValue: HKCU/Software/Microsoft/Windows/CurrentVersion/InternetSettings/Connections/DefaultConnectionSettings - RegCloseValue: HKCU/Software/Microsoft/Windows/CurrentVersion/InternetSettings/Connections - IRP_MJ_READ: C:/pagefile.sys

Black-Box Analyse/Uncommon Locations

Analyse mit Autopsy

Qualitative Analyse:

*** Hier Liste mit Suchbegriffen ***

o Autopsy Keywordsuche: > In allen Snapshots ergebnislos (keine Keyword-Hits -> In Literatur: Autoren fanden Ergebnisse in pagefile.sys > Autopsy: websites and some of the keywords found in hidden file called "pagefile.sys" [13] o [15] traces were found in: > However, on investigating the "pagefile.sys", some entries were discovered > Using the "data carving" technique, profile picture was recovered o [22] > Examining pagefile.sys showed some positive hits -> Evtl. hier zeigen, was gefunden werden kann, wenn RAM reduziert -> Aber auf Problem hinweisen, dass gefundener String in pagefile nicht direkt Browser zugeordnet werden kann > [6] Firefox only produced three recoverable artefacts as reported by both tools (FTK, Autopsy) -> Artefakte werden nicht genannt! > [16] Autopsy Keyword Suche nach Suchbegriffen: unallocated space > Autopsy Carving Module (\$Carved): [16] ■ When searching for the string 'clot' from the browsing protocol, six .dll, .edb and .reg files were discovered in unallocated space. ■ Further searching of unallocated space uncovered references to the Tor installation directory and the obfs4 bridging IP addresses ■ browsing data found in NTUSER.DAT was also replicated in unallocated space. o Autopsy PlugIns: > *** TODO: Hier Liste mit PlugIns ***

Analyse mit Volatility

o RAM Yarascan Treffer > Dump 1 vs 2 vs 3 > Im 3. Dump svchost: Evtl. mit Process Explorer VM Snapshot klonen, "auftauen" und zeigen, dass DNS-Cache die Daten speichert. -> Hier DNSList zeigen -> Evtl. 4. Dump nach Beenden/Deaktivieren von DNS-Cache zeigen, dass keine Yarascan Ergebnisse mehr vorhanden

> Diagramme: -

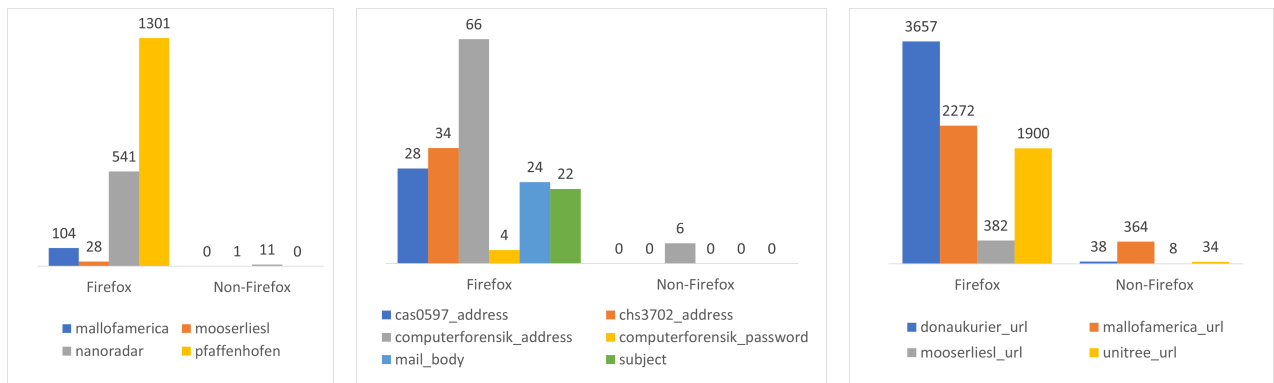


Abbildung 5.3: PB Artifacts found in RAM Dump 1

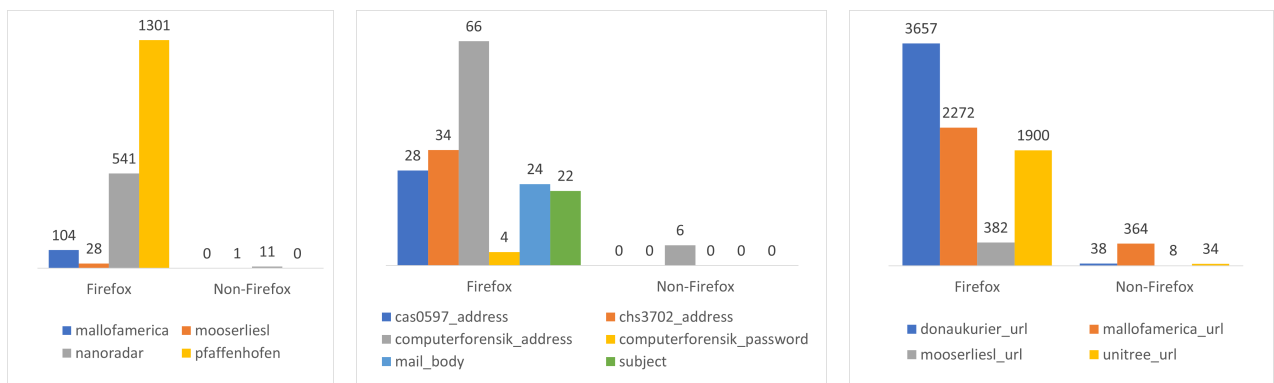


Abbildung 5.4: PB Artifacts found in RAM Dump 2

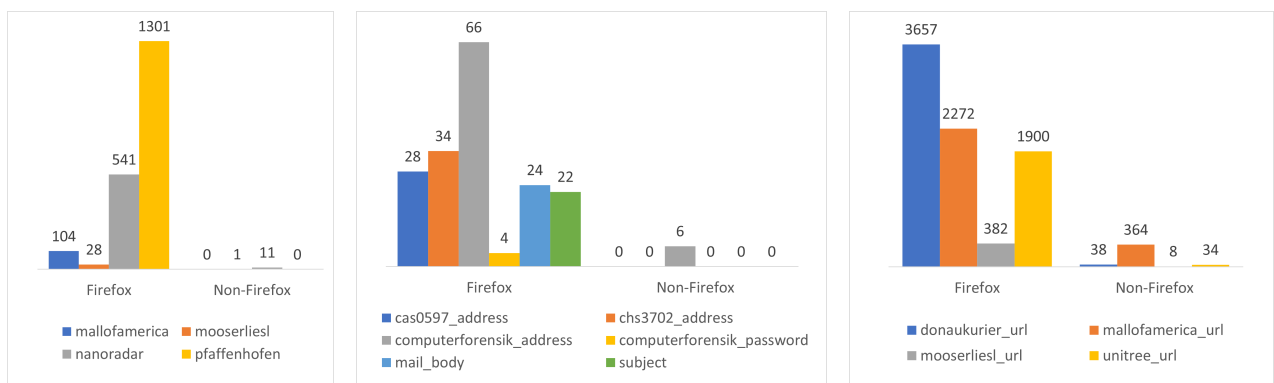


Abbildung 5.5: PB Artifacts found in RAM Dump 3

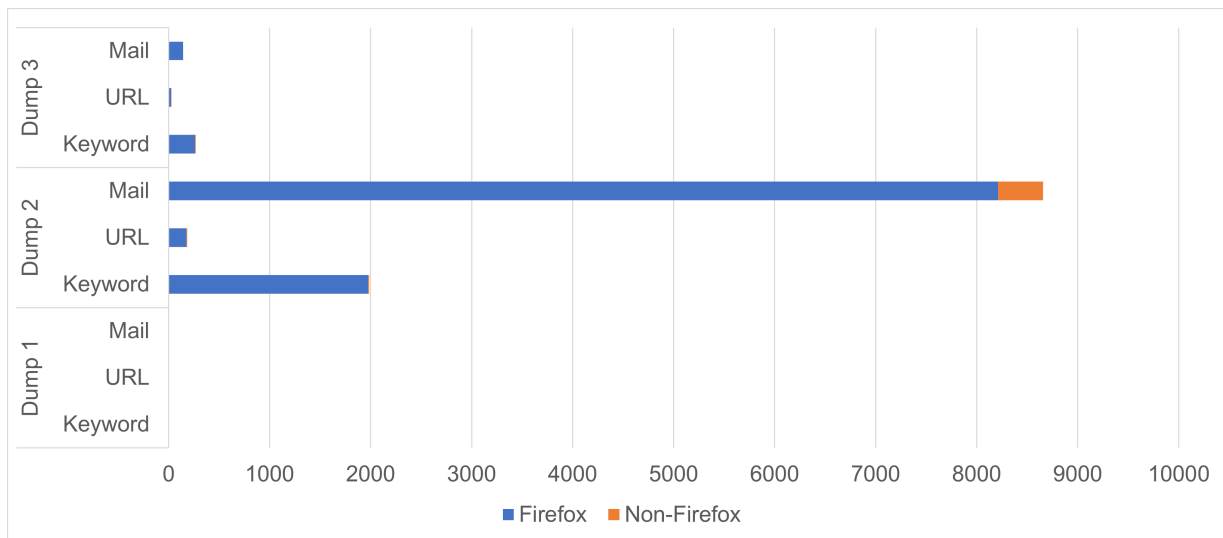


Abbildung 5.6: Comparison of found PB artifacts between RAM Dumps

5.2 Tor

Uncommon Locations

Qualitative Analyse

o Autopsy: [16] ■ Configuration files, downloaded files, and browserrelated data are recoverable from the file system. ■ Significant data-leakage from the browsing session occurred: HTTP header information, titles of web pages and an instance of a URL were found in registry files, system files, and unallocated space.

o RAM-Analyse nach [16]: ■ Live-Analyse identifiziert auch nach dem Schließen und Deinstallieren des Browsers und Abmelden des Benutzers Spuren von Tor-Prozessen, einschließlich des absoluten Pfads zur Browser-Executable, des Benutzernamens und des Geräts, von dem es ausgeführt wurde. ■ The data-leakage contained the German word for 'search' in reference to a Google search. This hints at the locale of the Tor server used to exit the network (exit relay).

o RAM-Analyse nach [8]: o process was found to be firefox.exe o pslist and pstree: parent process was shown o Belkasoft Ram Capturer: retrieve information about facebook o Cmdline: file path of the browser "E:/TorBrowser/Browser/firefox.exe" + name of process tor.exe and firefox.exe o Dlllist: DLL files of the executable files were not captured o Netscan: tor.exe + obfs4proxy.exe -> showed "LISTENING" connections to nonstandardized ports as output. Yarascan: was able to retrieve all the browsing sessions o RAM-Analyse nach [23] mit Volatility ■ process list extracted from the memory ■ registry hives been extracted from the memory dump ■ threads were extracted: "D:/VolatilityWorkbench/volatility.exe"-plugins="D:/VolatilityWorkbench/profiles" pslistfilename="C:/Users/username/Desktop/tor.raw" -profile=Win10x64 17763 -kdbg=0xf807606ac5e0 ■ Handles: resources used by the process 5672 ■ Dlls: These dlls can be found from prefetch file -> Can

be found in “prefetch” file -> Analyzed with “winprefetchview” ■ Places.sqlite: SQLite viewer has been used to recover bookmarks and frequently visited sites even after uninstalling the application ■ Visited Websites: Using keyword search in Dump’s Hex

o Registry: > Shellactivities (siehe Firefox) [16]: instance of a URL were found in registry file > [17] The userassist key is located in the NTUSER.dat hive of the -> Registry and indicates the execution path of the program, as well as the number of times the program was executed

Quantitative Zusammenfassung

5.3 Chrome

Uncommon Locations

o Autopsy Keyword-Suche: > Chrome and Edge produced five artefacts as reported by both tools. (FTK, Autopsy) [6] -> Artefakte werden nicht genannt! > only two temporary files (Figure 7) were recovered with Minitool Power Data Recovery but it was a dead end; Location: appdata/.../Chrome/.../Preferences/RF1533fa.TMP [5] > pagefile.sys file showed no traces at all [22]

5.4 Brave

6 Vergleich der Browser

Einleitend werden Struktur, Motivation und die abgeleiteten Forschungsfragen diskutiert.

7 Diskussion

> Artefakte im DNS Cache: [24] ■ DNS-Caching ist eine Bedrohung für private Browsing ■ Diese Schwachstelle entsteht, weil das Betriebssystem DNS-Anfragen des Browsers im Cache speichert, unabhängig davon, ob der Browser im privaten Modus ist oder nicht ■ Mehrere Jahre nach der Meldung dieser Schwachstelle besteht sie immer noch in allen Browsern fort ■ Es wurden einige Erweiterungen von Drittanbietern entwickelt, um dieses Problem zu beheben, aber keine davon wurde von den Browserherstellern übernommen.

> Viele RAM-Artefakte - Firefox [16] ■ Darcie et al. (2014) fanden Beweise für das Web-Browsing in Form von JPEG- und HTML-Dateien in Live-Forensik, aber eine statische Forensik war erfolglos. ■ Eine vorherige Live-Forensik-Analyse des Firefox-Browsers zeigte, dass Artefakte aus einer privaten Browsing-Sitzung aus dem Speicher wiederhergestellt werden konnten. (Findlay and Leimich, 2014).

> IE hinterlässt viele Spuren im Gegensatz zu Ergebnissen: [14] o hidden folders are usually stored at C:/Users/User/AppData o evidence searches are conducted extensively in the C: partition o bookmarks remain and can be viewed o downloads remain in the downloads folder until the user manually deletes them o CacheView trace entire URL and browsing histories including the temporary files CacheView enables to find the image's URL and from specific website

> Urteil über die Privatheit von Tor nach [16] The design aim of preventing Tor from writing to disk (Perry et al., 2018) is not achieved in this version. ■ Configuration files, downloaded files, and browserrelated data are recoverable from the file system. ■ Significant data-leakage from the browsing session occurred: HTTP header information, titles of web pages and an instance of a URL were found in registry files, system files, and unallocated space. ■ The data-leakage contained the German word for 'search' in reference to a Google search. This hints at the locale of the Tor server used to exit the network (exit relay). The Tor Project's design aim of enabling secure deletion of the browser (Sandvik, 2013) is not achieved in this version. ■ References to: the installation directory, Firefox SQLite files, bridging IPs/ports, default bookmarks, Tor-related DLLs and Tor product information were all recovered after the browser was deleted. ■ In a scenario where the operating system paged memory, an instance

Weiterführende Arbeiten: > Cross-mode interference [10]: o the Chrome://memory page displays all the opened tabs in the browser regardless if they are in the usual or private mode -> Nicht mehr aktuell -> Stattdessen: Chrome Task-manager (Ctrl + Esc), Funktioniert auch bei Firefox

> Für wen wird Browser entwickelt > Warum und für wen wird Private Browsing analysiert? > Ist das Auffinden privater Browsing Artefakte Schuld von Browser Entwicklern? (Oder Schuld des Betriebssystems, wie in (TODO!) erwähnt)

8 Fazit

Einleitend werden Struktur, Motivation und die abgeleiteten Forschungsfragen diskutiert.

Literatur

- [1] Gaurav Aggarwal u. a. "An Analysis of Private Browsing Modes in Modern Browsers." In: *USENIX security symposium*. 2010, S. 79–94.
- [2] Gabriele Bonetti u. a. "Black-box forensic and antifoensic characteristics of solid-state drives". In: *Journal of Computer Virology and Hacking Techniques* 10 (2014), S. 255–271.
- [3] Howard Chivers. "Private browsing: A window of forensic opportunity". In: *Digital Investigation* 11.1 (2014), S. 20–29.
- [4] Divya Dayalamurthy. "Forensic memory dump analysis and recovery of the artefacts of using tor bundle browser–the need". In: (2013).
- [5] Hasan Fayyad-Kazan u. a. "Forensic analysis of private browsing mechanisms: Tracing internet activities". In: (2021).
- [6] Ryan M Gabet, Kathryn C Seigfried-Spellar und Marcus K Rogers. "A comparative forensic analysis of privacy enhanced web browsers and private browsing modes of common web browsers". In: *International Journal of Electronic Security and Digital Forensics* 10.4 (2018), S. 356–371.
- [7] Ms Pooja Gupta. "Capturing Ephemeral Evidence Using Live Forensics". In: *IOSR J. Electron. Commun. Eng* (2013), S. 109–113.
- [8] Meenu Hariharan, Akash Thakar und Parvesh Sharma. "Forensic Analysis of Private Mode Browsing Artifacts in Portable Web Browsers Using Memory Forensics". In: *2022 International Conference on Computing, Communication, Security and Intelligent Systems (IC3SIS)*. IEEE. 2022, S. 1–5.
- [9] Nihad A Hassan. *Digital forensics basics: A practical guide using Windows OS*. Apress, 2019.
- [10] Ashley Hedberg. *The privacy of private browsing*. Techn. Ber. Technical Report, Tufts University, MA, USA, 2013.
- [11] Graeme Horsman u. a. "A forensic examination of web browser privacy-modes". In: *Forensic Science International: Reports* 1 (2019), S. 100036.
- [12] Aina Izzati und Nurul Hidayah Ab Rahman. "A Comparative Analysis of Residual Data Between Private Browsing and Normal Browsing Using Live Memory Acquisition". In: *Applied Information Technology And Computer Science* 3.2 (2022), S. 68–83.
- [13] Ahmed Redha Mahlous und Houssam Mahlous. "Private Browsing Forensic Analysis: A Case Study of Privacy Preservation in the Brave Browser". In: *International Journal of Intelligent Engineering Systems* 13.06 (2020), S. 294–306.
- [14] Raihana Md Saidi u. a. "Analysis of Private Browsing Activities". In: *Regional Conference on Science, Technology and Social Sciences (RCSTSS 2016) Theoretical and Applied Sciences*. Springer. 2018, S. 217–228.

-
- [15] Reza Montasari und Pekka Peltola. "Computer forensic analysis of private browsing modes". In: *Global Security, Safety and Sustainability: Tomorrow's Challenges of Cyber Security: 10th International Conference, ICGS3 2015, London, UK, September 15-17, 2015. Proceedings 10*. Springer. 2015, S. 96–109.
- [16] Matt Muir, Petra Leimich und William J Buchanan. "A forensic audit of the tor browser bundle". In: *Digital Investigation* 29 (2019), S. 118–128.
- [17] Rebecca Nelson, Atul Shukla und Cory Smith. "Web browser forensics in google chrome, mozilla firefox, and the tor browser bundle". In: *Digital Forensic Education: An Experiential Learning Approach* (2020), S. 219–241.
- [18] Donny Jacob Ohana und Narasimha Shashidhar. "Do private and portable web browsers leave incriminating evidence? a forensic analysis of residual artifacts from private and portable web browsing sessions". In: *2013 IEEE Security and Privacy Workshops*. IEEE. 2013, S. 135–142.
- [19] Daniel Perdices u. a. "Web browsing privacy in the deep learning era: Beyond VPNs and encryption". In: *Computer Networks* 220 (2023), S. 109471.
- [20] Digvijaysinh Rathod. "Darknet forensics". In: *future* 11 (2017), S. 12.
- [21] Tri Rochmadi, Imam Riadi und Yudi Prayudi. "Live forensics for anti-forensics analysis on private portable web browser". In: *Int. J. Comput. Appl* 164.8 (2017), S. 31–37.
- [22] Huwida Said u. a. "Forensic analysis of private browsing artifacts". In: *2011 International Conference on Innovations in Information Technology*. IEEE. 2011, S. 197–202.
- [23] Priya P Sajan u. a. "Tor Browser Forensics". In: *Turkish Journal of Computer and Mathematics Education (TURCOMAT)* 12.11 (2021), S. 5599–5608.
- [24] Kiavash Satvat u. a. "On the privacy of private browsing—a forensic approach". In: *Data Privacy Management and Autonomous Spontaneous Security: 8th International Workshop, DPM 2013, and 6th International Workshop, SETOP 2013, Egham, UK, September 12-13, 2013, Revised Selected Papers*. Springer. 2014, S. 380–389.
- [25] Yunus Yusoff, Roslan Ismail und Zainuddin Hassan. "Common phases of computer forensics investigation models". In: *International Journal of Computer Science & Information Technology* 3.3 (2011), S. 17–31.